Estratégia Concursos

Aula 00

Prefeitura de Uberaba-MG (Especialista de Serviços Públicos - Analista de Sistemas) Redes e Segurança - 2024 (Pós-Edital)

Autor:
André Castro

22 de Fevereiro de 2024

Índice

APRESENTAÇÃO

Olá pessoal, como estão? Espero que bem e ansiosos pelo nosso curso. Antes de tudo, gostaria de desejar-lhes boas-vindas ao nosso curso aqui no Estratégia!

Meu nome é André Castro! Sou formado em engenharia de Redes de Comunicação pela Universidade de Brasília – UnB, pós-graduado e mestrando na área de Segurança e Administração de Redes também pela UnB.

Comecei minha jornada em concursos públicos em 2009, ainda no oitavo semestre do curso de graduação, sendo **aprovado e classificado** no concurso para Analista de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão. Agora já temos um novo nome, sendo Ministério do Planejamento, Desenvolvimento e Gestão.

Fui **aprovado** ainda nos concursos de Analista Administrativo da Câmara dos Deputados, realizado em 2011 e **aprovado** no concurso de Analista para o Banco Central do Brasil em 2013.

Exerço ainda atividades de instrução e apoio em alguns cursos na área de Redes e Segurança pela Escola Superior de Redes – ESR, da Rede Nacional de Pesquisa – RNP, além de outros projetos relacionados a concursos públicos, incluindo aulas presenciais.

Possuo também algumas certificações na área de Tecnologia da Informação, como **CCNA, Itil Foundation e Cobit Foundation.**

Para ser aprovado nesses concursos, tive que experimentar a vida de *concurseiro ou concursando, como queiram*. Permaneço nela até hoje com outros objetivos, além da necessidade de sempre se manter atualizado e aprimorando esses anos de experiência.

Acrescido a isso, a experiência que tenho na área acadêmica me trouxe alguma bagagem para aprimorar ainda mais esse curso, **bem como nossa didática de ensino**.

Sei que as dificuldades para o *concursando* são muitas, mas posso afirmar que vale a pena cada esforço, **não só pela remuneração ($$$), mas pelos benefícios e vantagens oferecidos pelo setor público**, além da oportunidade de servir o cidadão brasileiro, em busca de uma máquina pública mais eficaz e eficiente.

Portanto, vamos persistir juntos nessa caminhada e espero poder contribuir bastante em sua jornada. E sempre lembrando que eu gosto bastante de churrasco, principalmente nas comemorações de aprovações!!!

Assim, mãos à obra!!!

Sumário

CRIPTOGRAFIA

Temos agora mais um assunto extremamente bacana. Na verdade, temos aqui uma relação de amor e ódio. Tenho percebido isso em meus alunos. Mas meu papel aqui é tornar o "relacionamento" de vocês com esse assunto bem agradável.

Como já vimos nas outras aulas, a **informação** é um **fator crucial para qualquer organização ou pessoa.** O princípio da confidencialidade fala muito nesse contexto.

Frente a esse cenário, historicamente, sempre se buscou criar formas para "esconder" a informação de terceiros não autorizados. Assim, ainda que estes tivessem acesso à informação, não conseguiriam interpretá-las.

Um filme muito interessante sobre o assunto é "O JOGO DA IMITAÇÃO", o qual eu recomendo pelo conteúdo e qualidade de produção. Fica a dica.

Esse filme nos apresenta um cenário de guerra em que uma nação busca interceptar informações do adversário para obter estratégias de guerra e planos de ataque para ter uma vantagem.

Entretanto, o dado em si era facilmente obtido, porém, não eram capazes de interpretá-los.

Antes de avançarmos, vamos traçar aqui algumas definições e conceitos que aparecem em provas constantemente.

A criptografia é uma ciência que tem como objetivo "embaralhar" as informações. Desse modo, ainda que um atacante obtenha acesso aos dados, este não será capaz de lê-la e em alguns casos, alterá-la.

O termo em análise vem do grego *Kryptós*, que quer dizer "oculto". E grápho, que quer dizer "grafia". Assim, temos que a criptografia corresponde a escrita oculta.

Outros termos gregos que aparecem nesse contexto são:

Análysis = decomposição;

Logo = estudo.

Com isso, temos outros termos fundamentais e presentes no cenário em estudo, que são:

> **Criptoanálise** = Ciência de quebrar códigos e decifrar mensagens. Então o simples fato de você buscar quebrar o código e não somente interpretar a informação já é uma forma de ataque.
>
> **Criptologia** = Ciência que agrega a criptografia e a criptoanálise.
>
> **Cifra** = Método de codificação de mensagens com vista à sua ocultação.

Desse modo, ao codificarmos uma mensagem, podemos utilizar, basicamente, três métodos de cifragem, quais sejam: substituição, transposição e esteganografia.

A combinação desses métodos com fórmulas e funções matemáticas geram os tão conhecidos algoritmos de criptografia.

Substituição

A substituição é um **método de codificação que busca alterar um caractere, símbolo ou dado em algum outro**. É o método mais simples e fácil de executar. Porém, tende a ser o mais fácil de ser quebrado.

O principal exemplo desse método é a CIFRA DE CÉSAR, utilizado ainda no período do Império Romano. A sua rotina era definida de tal modo que cada letra da mensagem original era substituída pelo correspondente a três letras depois no alfabeto. **Trata-se de um método conhecido como Cifra Monoalfabética.**

Assim, temos o exemplo abaixo da utilização dessa codificação:

Texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Texto simples	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Desse modo, como exemplo, ao se escrever a mensagem original, teríamos a mensagem cifrada:

1. Atacar hoje à noite
2. DWDFDU KRMH D QRLWH

Percebam que é um método muito simples de se interpretar e de descobrir a regra utilizada. As vezes temos que abrir mão do acento, certo?

Para os que tiveram alguma infância com brincadeiras bobas iguais a minha, tínhamos aquela brincadeira de "falar em código" em que tínhamos que substituir uma letra sempre por outra específica em nossas frases.

HORA DE PRATICAR!

CESPE / CEBRASPE - 2022 - BANRISUL - Analista de Segurança da Tecnologia da Informação

A cifra de César, que substitui uma letra do alfabeto por outra sem seguir um padrão regular, é um aprimoramento da cifra monoalfabética.

Comentários:

Errado pessoal. Conforme vimos, há um padrão de salto de três posições. Ainda, continua sendo uma cifra mooalfabética.

A evolução da cifra monoalfabética é a cifra polialfabética.

Gabarito: E

CESPE / CEBRASPE - 2021 - MPE-AP - Analista Ministerial

Uma das formas mais antigas de criptografia é a cifra de César, atribuída a Júlio César, da Roma Antiga. Na cifra de César, a se torna D, b se torna E, e assim sucessivamente. Supondo que seja necessário enviar para um amigo que está em outra cidade uma senha criptografada pela cifra de César e que essa senha corresponda à palavra rouxinol, assinale a opção que indica corretamente a palavra criptografada a ser enviada.

A TQWZKPQN

B URXALPRO

C VSYBMRSP

D URXALQRO

E TQWYIQUM

Comentários:

Pessoal, a questão já deu a resposta... A necessidade básica aqui é conhecer o alfabeto, certo? Bastava você exercitar letra a letra, ou tentar ser um pouco mais dinâmico para buscar a resposta.

Basicamente, eu peguei a primeira letra R e vi que vira U. Logo, sombras as alternativas B e D.

Daí, olhando a sequência de ambas, verifica-se que a única diferença é no penúltimo caracter. Na palavra original é a letra O, que passa então a ser R.

Gabarito: D

CESPE – TCE-PR/Analista de Controle – Área TI/2016

Assinale a opção correta, no que concerne a conceitos básicos de criptografia e criptografia simétrica e assimétrica.

a) A principal diferença entre os algoritmos de criptografia simétrica e os algoritmos de criptografia assimétrica consiste no fato de que os primeiros são fundamentados em técnicas de transposição e os segundos em técnicas de substituição.

b) Um esquema de criptografia será considerado computacionalmente seguro se o tempo para se quebrar sua cifra for superior ao tempo de vida útil da informação por ele protegida.

c) Em uma transmissão de dados em que se use criptografia simétrica, as chaves de criptografia e decriptografia têm de ser distintas, embora tenham de ter o mesmo tamanho.

d) O valor da chave de criptografia depende do texto claro a ser criptografado e do algoritmo a ser usado para criptografar esse texto.

e) Em um ataque por força bruta, exploram-se a natureza e as características do algoritmo na tentativa de deduzir as chaves.

Comentários:

Tivemos uma inversão dos conceitos na alternativa "A". Já para a "B", temos exatamente o que se aplica no contexto de Segurança. Se a informação não faz mais sentido, ou seja, se ela não tem mais valor, não há problemas em ela ser violada. Nesse sentido, precisamos garantir que o sistema não seja quebrado enquanto a informação produz algum valor, ou seja, dentro do seu período de vida útil.

Já para a letra "C", temos que a chave deve ser a mesma, certo? Para a "D", não temos relação com o texto em claro em termos da definição da chave.

Por fim, na letra "E", temos a descrição do ataque de criptoanálise e não de força bruta. Este é baseado simplesmente na tentativa e erro.

Gabarito: B

Transposição

Já a transposição foca no simples embaralhamento das letras segundo alguma rotina. Veremos mais à frente que os algoritmos de criptografia geralmente utilizam esse recurso dividindo a mensagem original em blocos de tamanhos iguais. Um exemplo simples seria transpor cada sílaba de cada palavra (bloco) para esquerda, mantendo a rotação de cada bloco. Assim, facilmente lemos:

Você pode ler facilmente esta mensagem?

Já a mensagem transposta abaixo não seria tão simples. Perceba que não há criação de letras ou sílabas novas.

cêVo depo ler cilmentefa taes sagemmen?

CESPE / CEBRASPE - 2019 - TJ-AM - Assistente Judiciário - Suporte ao Usuário de Informática

Empregada na criptografia, a transposição consiste na mudança na posição de letras ou palavras; essa técnica demanda que ambas as partes conheçam a fórmula de transposição utilizada.

Comentários:

Nós veremos mais a seguir que os algoritmos de criptografia incorporam, definitivamente, diversos conceitos e práticas no que tange à substituição e transposição.

O grande destaque da transposição é focar na alteração e embaralhamento da informação, sem incluir novos itens e retirar os existentes. E, obviamente, é necessário que as duas partes saibam e tenham domínio completo do procedimento ou regra estabelecida.

Gabarito: C

Esteganografia

Por último, temos a esteganografia que tem como objetivo esconder uma mensagem dentro de outra. Tipicamente, busca-se enviar uma mensagem de texto embutido no código de uma imagem. Não há muito mais o que falar por aqui, pois as bancas, quando cobra, vem com essa visão simplista e objetiva.

FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação

Anderson quer enviar uma mensagem para sua esposa que está em outra cidade sem que ninguém saiba da existência da mensagem. Então, Anderson inseriu a mensagem em uma foto em que ambos estavam, de forma que fez uma pequena redução na qualidade da imagem e inseriu a mensagem nesses bits sobressalentes.

Para ocultar a mensagem em uma foto, Anderson utilizou a técnica de:

A transposição;

B substituição;

C criptoanálise;

D esteganografia;

E cifração polialfabética.

Comentários:

Vejam que mais que o conceito da esteganografia no sentido de se esconder uma mensagem dentro de outra, temos o contexto prático da consequência de se alterar a estrutura original do documento, gerando uma perde de qualidade, nesse caso. Em outros, pode haver perda parcial da informação original.

Gabarito: D

CESPE / CEBRASPE - 2020 - Ministério da Economia - Tecnologia da Informação

Esteganografia é uma técnica que consiste em ocultar uma mensagem dentro da outra, enquanto a criptografia é uma técnica que codifica o conteúdo da mensagem.

Comentários:

Conforme nós vimos pessoal. Não há muito que variar no conceito.

Gabarito: C

Cifragem de Bloco – Cipher Block

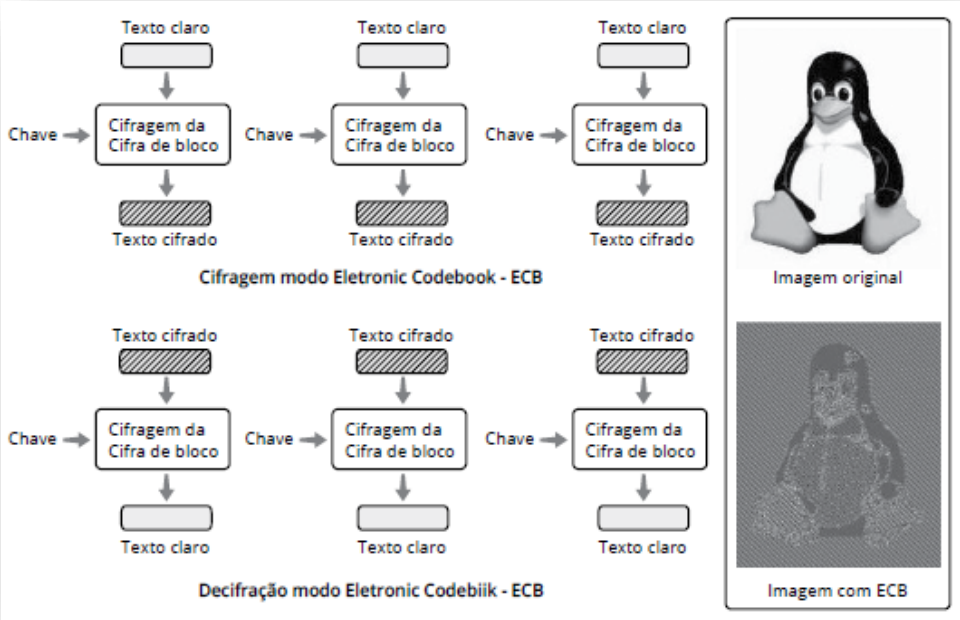
Antes de conversamos a respeito dos algoritmos de criptografia, vamos conhecer as diferentes técnicas de cifragem utilizadas pelos diversos algoritmos de criptografia.

Como o próprio nome já diz, **a ideia é quebrar a mensagem a ser enviada em blocos de tamanho fixo** antes de se aplicar as diversas operações matemáticas de determinado algoritmo.

Em regra, temos que todos os modos buscam garantir aspectos de confidencialidade. Alguns deles são capazes de tratar aspectos de autenticidade e integridade, ou seja, não podemos generalizar e afirmar que a cifragem por bloco garante os princípios de segurança de forma geral.

Eletronic Code Book – ECB

É o método mais simples que utiliza como conceito a independência dos blocos sendo aplicada a mesma chave. É uma técnica não randômica pela simples concatenação dos blocos resultado da fragmentação da mensagem original.

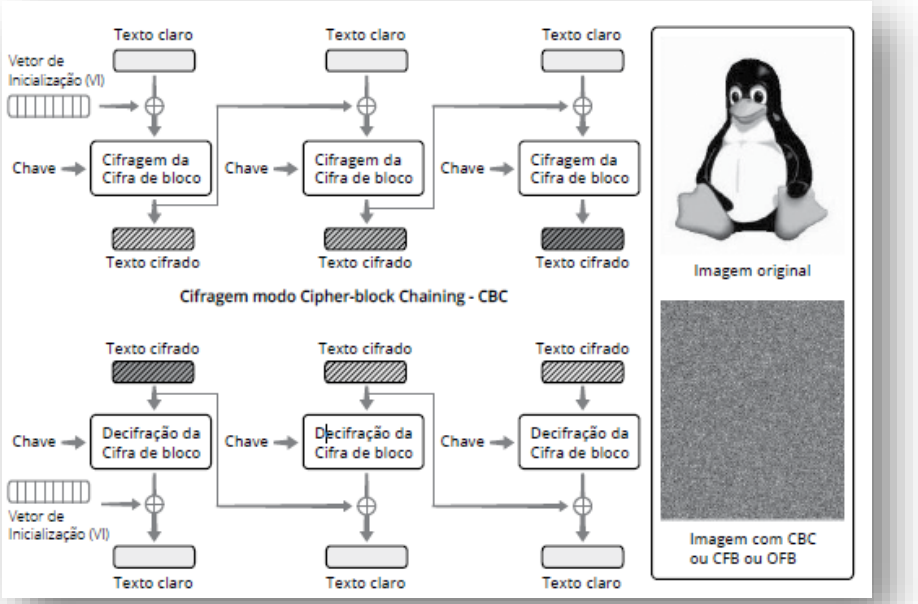


O ECB utilizada como tamanho padrão 64 bits por bloco. Não é considerado um mecanismo seguro devido à repetição dos dados e resultado de cifragem idêntico. Assim, blocos de entrada iguais, produzem blocos cifrados iguais, não escondendo, portanto, algum padrão dos dados. Por isso, é conhecido por ter transmissão segura de valores únicos.

Como vantagem podemos citar o fato de que o erro de um bit causará prejuízo apenas no bloco o qual ele pertence, devido à independência dos blocos.

Cipher Block Chaining – CBC

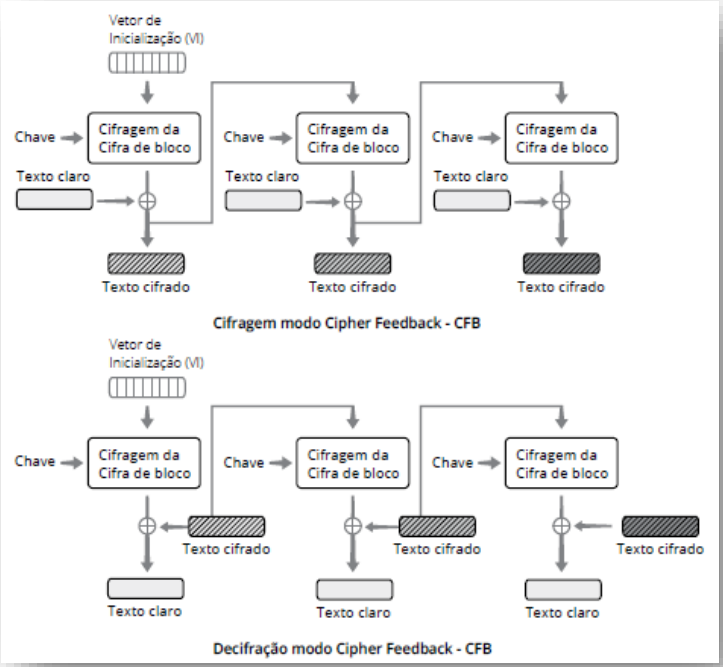
É o método mais utilizado. Utiliza a operação XOR devidamente representada na imagem a seguir pelo círculo em volta do sinal de "+". A cifragem de cada bloco depende da cifragem de todos os blocos anteriores.



Percebam que o bloco cifrado é utilizado para "embaralhar" os blocos subsequentes. Depende que os blocos cheguem de forma sequencial para que não haja problema na decifração, perdendo no aspecto de desempenho quando comparado ao ECB. Além disso, um erro em qualquer bit ou bloco, gera prejuízo em todos os blocos subsequentes.

- **Cipher FeedBack - CFB**

Suporta qualquer tamanho de entrada, independentemente do bloco. Por esse motivo, se torna útil para aplicações que dependem de transmissão imediata.



Percebam que o bloco cifrado é utilizado para "embaralhar" os blocos subsequentes. Depende que os blocos cheguem de forma sequencial para que não haja problema na decifração, perdendo no aspecto de desempenho quando comparado ao ECB. Além disso, um erro em qualquer bit ou bloco, gera prejuízo em todos os blocos subsequentes.

A diferença básica para o CBC é o ponto de junção entre o texto cifrado anterior e o novo texto.

ESCLARECENDO!

Destaco ainda a existência do modo OFB (Output Feedback), que segue o mesmo princípio do CFB, com a diferença de que a realimentação é feita pela saída do algoritmo e não das parcelas de texto cifrado.

Um outro modo existente, é o CTR (Counter). O modelo é mais simplista em que cada bloco de texto em claro é submetido a um XOR com um contador criptográfico. O referido contador é incrementado para cada bloco subsequente para não ser o mesmo aplicado todas as vezes. Mais uma vez, é comparado ao OFB, porém, a realimentação é o contador e não a saída do algoritmo.

Uma vez que a realimentação não depende do algoritmo, tem-se um modo muito mais rápido em termos de desempenho.

CESPE / CEBRASPE - 2022 - BANRISUL - Analista de Segurança da Tecnologia da Informação

A cifra de bloco é uma das classes gerais de técnicas de criptografia simétrica utilizada em muitos protocolos seguros da Internet, como o PGP e o SSL.

Comentários:

Essa é a ideia pessoal. Talvez nesse ponto você tenha ficado em dúvida sobre os protocolos citados... Mas ambos são ancorados em criptografias simétricas que utilizam cifra de bloco.

Só aproveitando para deixar o registro:

O PGP (Pretty Good Privacy), destina-se a comunicação segura via e-mail, para isto utiliza-se de criptografia de chave pública. A mensagem enviada é criptografada com a chave pública do destinatário. Para que o usuário possa decifrar a mensagem ele decifra com a sua chave secreta a qual somente ele possui. Desta forma, qualquer pessoa que intercepte esta comunicação não conseguirá decifrar a mensagem.

No PGP temos também a facilidade de poder assinar uma mensagem, assim a mensagem vai cifrada com a chave secreta do remetente e o destinatário decifra com a chave pública do remetente. Uma mensagem pode ir cifrada e assinada.

Gabarito: C

Cifragem de Fluxo – Stream Cipher

Diferentemente da cifra de bloco, a cifra de fluxo não necessita aguardar o processamento de toda a mensagem para se aplicar o algoritmo. Como o próprio nome nos remete, a ideia **é ser algo mais dinâmico e ágil de tal forma que, à medida que os dados vão chegando, vai se aplicando o algoritmo de forma contínua**.

Podemos perceber claramente que este é um modelo amplamente difundido em cenário de transmissão de mídias, onde há um streaming de dados a serem criptografados.

O parâmetro para se aplicar a técnica pode ser bit a bit, byte a byte ou até em intervalos de tempo específicos.

Identificação de Dados Criptografados

Antes de avançarmos em nossas discussões, é importante destacarmos que bons algoritmos de criptografia buscam gerar criptogramas que se confundem com os dados aleatórios, justamente para dificultar a análise. Isso é bom na perspectiva de evitar ataques de criptoanálise, entretanto, dificulta o trabalho de responsáveis por realizar auditorias em dados criptografados, como é o caso de peritos em forense computacional.

Podemos observar três contextos básicos para dados criptografados, quais sejam: arquivos criptografados, discos virtuais criptografados e discos complemente criptografados.

Arquivos Criptografados

Nesse primeiro contexto, tem-se a criptografia aplicada somente ao conteúdo de determinado arquivos. Isso implica dizer que as características do arquivo se mantêm decifrados, ou seja, é possível verificar facilmente a sua assinatura e metadados (nome, tamanho, datas de criação, entre outros).

Existem duas formas básicas de geração desses arquivos criptografados. A primeira é por intermédio dos próprios programas que geraram os arquivos (excel, doc, pdf, zip, rar). A segunda alternativa, é a utilização de programas específicos em que é possível selecionar diversos arquivos para que estes tenham seus conteúdos criptografados a partir de uma única senha. Alguns exemplos desses aplicativos são: eCryptFS e EncFS para ambientes LINUX e o EFS para Windows.

Para se identificar arquivos criptografados pode-se utilizar testes de entropia (medida de aleatoriedade) ou ainda assinaturas e marcados específicos no cabeçalho desses arquivos.

Discos Virtuais Criptografados

Nesse contexto, utiliza-se um arquivo-contêiner devidamente criptografado em que, a partir da sua decriptação, gera-se um disco virtual com sistema de arquivos próprio. Basicamente cria-se uma nova unidade de disco acessível no sistema de arquivos.

Isso implica dizer que todo o sistema de arquivos do sistema operacional hospedeiro não é afetado, ou seja, permanecendo em claro.

Assim, todas as alterações no referido disco virtual serão salvas no arquivo a ser posteriormente criptografado no momento de sua desmontagem, zelando-se pela integridade e confidencialidade dos dados. Diversos são as aplicações capazes de criar os arquivos-contêiner: bitlocker, apple disk image, LUKS, truecrypt, entre outros.

Mais uma vez, os testes de entropia ajudam a identificar arquivos-contêiner. Por ser um disco virtual próprio, geralmente possuem tamanhos consideráveis, na ordem de gigabytes, e com conteúdo ininteligível por causa da criptografia.

Discos Completamente Criptografados

Quando assistimos filmes em geral que abordam essa temática, nos deparamos por diversas vezes em que policiais recuperam computadores de criminosos e quando vão acessas os dados, se deparam com o disco criptografado. Começa então um processo custoso para decriptação.

Esse cenário é conhecido também como Full Disk Encryption ou Whole Disk Encryption. Nesse caso, diferentemente dos outros dois contextos, todo o sistema de arquivos e sistema operacional estão devidamente criptografados.

O que se mantém em claro nesse contexto são os primeiros setores do disco (geralmente a partição de boot), permitindo a inicialização do SO. As ferramentas mencionadas anteriormente também são capazes de criptografar todo o disco.

Ao se iniciar um disco criptografado, será solicitada uma senha logo na inicialização do SO. A chamada geralmente é feita pela aplicação responsável pelo processo de criptografia.

Para a detecção de discos criptografados, geralmente cada aplicação utiliza um marcador próprio (código identificador) nos primeiros setores do disco, que permitem a sua identificação, possibilitando saber também qual programa foi utilizado.

Importante destacar que os conceitos vistos para discos se aplicam também a mídias externas, como pendrives ou HD's externos.

1. a) Criptoanálise

Como já mencionamos, a criptoanálise tem foco no entendimento de como funciona o algoritmo de criptografia. Desse modo, a realização da criptanálise depende da quantidade de informações que se tem à disposição e quão possível é manipulá-las.

A partir daí, podemos elencar cincos tipos de ataques, que recorrentemente caem em provas, quais sejam:

- **Apenas Texto Cifrado – CypherText-Only**
- **Texto Claro Conhecido – Known-plaintext**
- **Texto Claro Escolhido – Choosen-Plaintext**
- **Texto Cifrado Escolhido – Choosen-CypherText**
- **Texto Escolhido – Choosen-Text**

Apenas Texto Cifrado – CypherText-Only: Nesse contexto, há conhecimento apenas do algoritmo de criptografia utilizado e do próprio texto cifrado;

Texto Claro Conhecido – Known-plaintext: Além dos itens acima, o atacante tem a informação dos pares de texto claro de entrada e seu respectivo texto cifrado de saída;

Texto Claro Escolhido – Choosen-Plaintext: Agora o atacante não se restringe apenas a saber o par de entrada e saída, mas ele é capaz de manipular a entrada e avaliar a sua respectiva saída;

Texto Cifrado Escolhido – Choosen-CypherText: Agora o atacante é capaz de fazer o caminho reverso, onde a partir de um texto cifrado escolhido, ele é capaz de verificar qual o texto em claro correspondendo;

Texto Escolhido – Choosen-Text – Há plena capacidade de manipulação dos textos de entrada e saída, e vice-versa;

2. b) Métodos de Decifragem de Dados

Conforme já mencionamos ao longo do curso, há diversas técnicas que podem ser utilizadas com a finalidade de se decifrar mensagens criptografadas.

Nesta etapa, comentaremos a respeito de algumas técnicas. Devemos lembrar que um primeiro ponto a ser observado, é o algoritmo utilizado. Este algoritmo, por si só, pode ser vulnerável a determinados tipos de ataques. Desse modo, entender o contexto é fundamental.

Método da Recuperação Direta

Pessoal, como o próprio nome já diz, **o intuito desse método é conseguir obter a senha de maneira direta, ou seja, a partir de algum ponto de armazenamento ou a chave utilizada como referência para armazenar o dado criptografado**.

Então busca-se ter a ciência de algoritmos frágeis em sua implementação, regras de armazenamento simples com repositório conhecido, chaves padrões utilizadas para guardar as senhas criptografadas.

Um exemplo seria acessar, por exemplo, um repositório comum de alguma ferramenta utilizada para criação de sites. Nesse caso, o repositório é conhecido e armazena as senhas em texto claro. Ou seja, se for possível acessar o repositório, é possível obter a senha.

Método Pré-Computado

Neste método, busca-se criar uma lista, bem extensa por sinal (aumentando a chance de quebra), **que correlaciona, para um determinado algoritmo, os textos em claro e os resultados gerados**. Por isso o termo "pré-computado".

Desse modo, a partir de um determinado resultado, é possível realizar pesquisa na tabela e verificar qual o texto em claro correspondente àquele texto criptografado.

Importante destacar que, quando maior o tamanho das chaves utilizadas, mais custoso é a criação e armazenamento da tabela pré-computadas. Assim, sistemas mais antigos, por utilizarem chaves com quantidade de bits baixa, ficam muito suscetíveis a esse tipo de ataque.

Há de se mencionar também que há serviços online que já disponibilizam aplicativos e bases pré-computadas para diversos tipos de algoritmos de criptografia e funções HASH, e, em muitos casos, tais bases são comercializadas, até porque o maior custo é de construção da base... posteriormente, basta realizar a comparação.

Para os novos algoritmos, com chaves maiores, usa-se o conceito de bases parciais. Ou seja, não há garantia de que o objeto será quebrado, uma vez que poderá não constar no rol da tabela. Isso acontece justamente porque para se criar uma tabela com todas as possibilidades possíveis dadas o tamanho da chave se torna inviável.

Método da Força Bruta

De maneira descontraída, podemos dizer que a "ignorância" é o ponto forte desse método. Aqui, busca-se, a partir de um grande poder computacional, processar todas as possibilidades de senhas para determinado ambiente ou algoritmos.

Matematicamente, é um método infalível, pois, justamente por exaurir as possibilidades, em algum momento será encontrada a chave almejada.

Entretanto, no mundo prático, o negócio não é tão simples. Processas as informações e testar possibilidades demanda tempo, e o tanto de tempo depende do poder de processamento disponível para realizar a quebra.

Por esse motivo, a relação (tamanho da chave e tempo) para quebra é um fator crítico. Assim, o método em questão se torna extremamente eficiente para senhas curtas.

Método de Dicionário

Sem dúvida, no contexto atual, é uma das técnicas mais utilizadas. O procedimento a ser realizado é muito semelhante com o método da Força Bruta. Entretanto, a invés de se testar todas as possibilidades possíveis dentro de uma quantidade limitada de caracteres, testa-se as senhas conforme uma lista pré-definida de "possíveis senhas" para o contexto em análise.

Desse modo, busca-se construir um dicionário que contemple senhas muito utilizadas por usuários como: 123456, 12345seis, senha, password, entre outros...

A grande vantagem do dicionário é que este pode ser construído a partir de diversas bases, inclusive a partir da integração destas. Uma ferramenta amplamente utilizada é o "John, the ripper".

Entretanto, uma forma de se otimizar ainda mais o ataque, é utilizar dicionários personalizados para determinado ambiente ou vítima. Assim, a partir da simples obtenção de dados pessoas, dados biográficos, engenharia social, entre outros, pode-se inserir possíveis senhas que contemplem datas específicas, nomes de parentes, combinações de datas e iniciais de nomes, entre muitos outros.

Para aumentar ainda mais a probabilidade de acerto, é interessante gerar variações dos textos criados na base, substituindo letras por números (como é o caso do "S" pelo "5"), além de inserir caracteres especiais e variações de letras maiúsculas e minúsculas.

Pode-se também se valer da inversão de letras ou sílabas, sempre na perspectiva de que o usuário tentará tornar uma senha comum para ele, em algo um pouco mais difícil de ser obtido indevidamente.

Método Probabilístico

Por fim, temos o método probabilístico. Como o nome já diz, busca-se por intermédio de algoritmos e análises estatísticas, aquelas sequências de caracteres que possuem maior probabilidade de ocorrência dado um contexto.

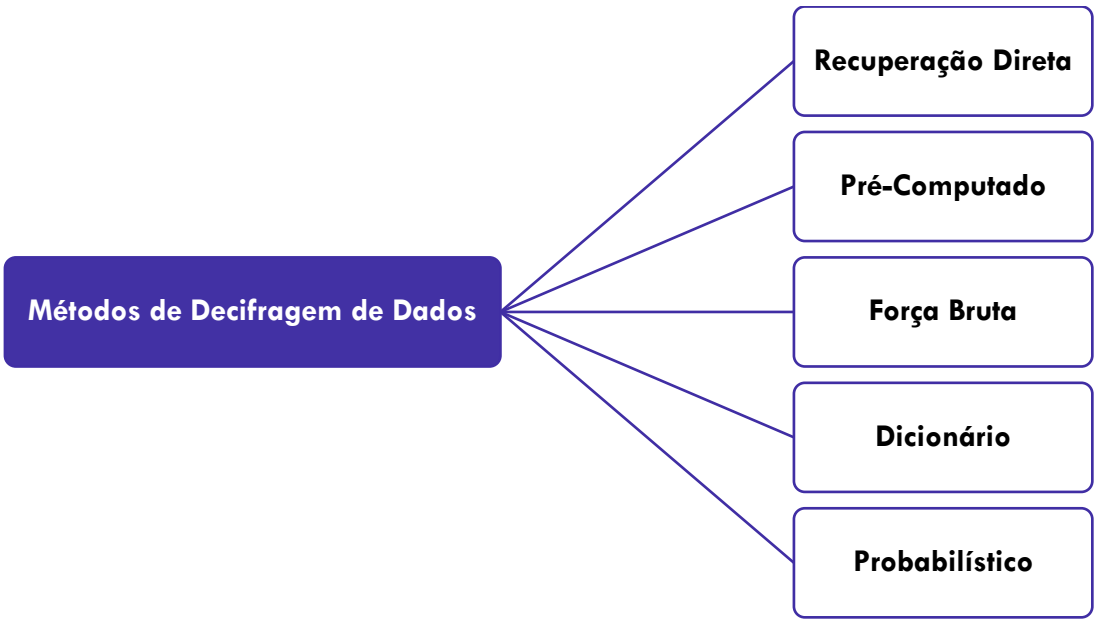
Este método pode ser derivado em duas subespécies, quais sejam: **probabilidade condicional e gramática especializada**.

A primeira contempla gerar vocábulos a partir de um idioma específico. Um exemplo clássico é o fato de que letras "h" têm a probabilidade de serem antecedidas por "c" ou "l", formando "ch" ou "lh" do que qualquer outra letra. Portanto, os algoritmos estatísticos buscam correlacionar esses aspectos para obter resultados satisfatórios.

Teoricamente falando, tais probabilidades condicionais, considerando suas frequências de ocorrência, são conhecidas como cadeias de MARKOV.

No segundo caso, **a gramática especializada**, busca-se criar um padrão de comportamento das senhas geradas para determinada gramática. Assim, a partir de um dicionário bem-sucedido, pode-se extrapolar o perfil das senhas, como, por exemplo, a utilização de 5 letras, 3 números e 1 caractere especial.

A partir de tal conclusão, busca-se gerar novas senhas que terão maior probabilidade de ocorrência, sem deixar de lado o fator personalizado já mencionado no método do dicionário.



Importante destacar a eficiência de cada um dos métodos. No caso da **Força Bruta** sendo eficiente **contra as senhas pequenas e homogêneas**, já o dicionário para senhas comuns que ainda possuem alguma regra de alteração e a probabilística para os casos mais complexos a serem tratados.

Destaca-se que, na maioria das vezes, bons resultados de decifragem são alcançados pela combinação dos métodos já mencionados com vistas a potencializar ainda mais o ataque, decifrando o conteúdo desejado na menor parcela de tempo.

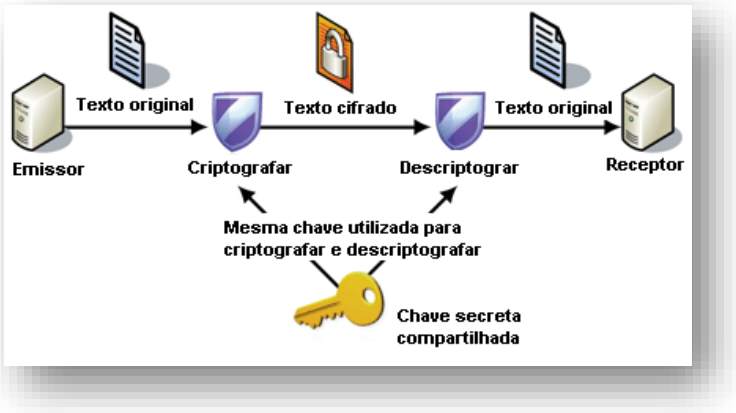
CRIPTOGRAFIA SIMÉTRICA

A criptografia simétrica possui como princípio o fato de se utilizar a mesma chave para o procedimento de criptografia e descriptografia.

Desse modo, a ideia é pegar um texto em claro que se deseja enviar a um destinatário e aplicar um algoritmo de criptografia simétrica sobre ele. Esse algoritmo depende da inserção de uma chave que será utilizada nos cálculos matemáticos para gerar uma mensagem que não seja interpretada facilmente.

No destinatário, deve-se aplicar o algoritmo com vistas a descriptografar a mensagem, ou seja, a partir da mensagem criptografada, busca-se obter a mensagem original. **Esse processo depende da inserção da MESMA CHAVE utilizada no processo de criptografia**.

A imagem a seguir nos apresenta o modelo:



Percebam que para o perfeito funcionamento do algoritmo, tanto o emissor quanto o receptor necessitam conhecer a chave simétrica utilizada e isso gera um problema na utilização do algoritmo. Como trocar as informações da chave de um modo seguro? Veremos logo mais!

A criptografia simétrica visa garantir apenas o princípio da confidencialidade. Os demais não podem ser garantidos, pois não há mecanismo que garanta que a mensagem não será alterada no caminho, podendo gerar um resultado de decriptação diferente da mensagem original. Não há como garantir de que a pessoa que aplicou a chave simétrica no processo de encriptação é quem ela diz ser. Veremos com detalhes cada um dos principais algoritmos de criptografia simétrica.

FGV - 2022 - TJ-TO - Técnico Judiciário – Informática

Em segurança da informação, a criptografia de chave simétrica é utilizada para garantir o requisito básico de segurança:

A confidencialidade;

B disponibilidade;

C integridade;

D autenticidade;

E não repúdio.

Comentários:

Na linha do que acabamos de ver pessoal, temos que o princípio chave da criptografia simétrica é a confidencialidade.

Gabarito: A

Entretanto pessoal, temos um entendimento do CESPE contrário ao que preconiza a maioria da bibliografia. Vejamos:

Ano: 2018 Banca: CESPE Órgão: STJ - Técnico Judiciário - Desenvolvimento de Sistemas

Na troca de mensagens entre duas empresas parceiras, a autenticidade e o sigilo das informações trocadas podem ser garantidos com o uso de criptografia simétrica.

Comentários:

O Cespe deu essa questão como correta. Alguns autores assumem que o fato de apenas os envolvidos na comunicação terem acesso à chave, vale o princípio da autenticidade. Ainda não identifiquei esse tipo de questão em outras bancas, entretanto, é importante ficarmos atentos.

Gabarito: C

Uma boa prática em qualquer processo de criptografia **é realizar a compressão dos dados antes da encriptação.** Tal procedimento tem como objetivo reduzir a ocorrência de dados repetidos ou redundantes em uma sequência de dados. Desse modo, **com uma menor quantidade de dados redundantes, dificulta-se o processo de criptoanálise** de um eventual atacante. Vale mencionar, **que a compressão também reduz o tamanho dos dados de entrada, aumentando o desempenho** da aplicação ou sistema.

Antes de avançarmos para os principais algoritmos de criptografia simétrica, gostaria de registrar alguns pontos. Primeiro, veremos claramente que os tamanhos das chaves simétricas são muito menores que os algoritmos de chaves assimétricas, o que implica em um processamento mais rápido do primeiro em relação em segundo.

Por esse motivo, na prática, utiliza-se o algoritmo de chave assimétrica como forma de trocar as chaves simétricas de modo seguro e posteriormente, toda a comunicação se dá utilizando o algoritmo de chave simétrica.

Outro ponto é que a robustez de segurança dos algoritmos de chave simétrica se encontra no segredo da chave, enquanto nos algoritmos de chave assimétrica, está no algoritmo. Entretanto, não quer dizer que isso basta, pois ambos são importantes para os dois modelos.

CESPE / CEBRASPE - 2021 - PG-DF - Analista Jurídico - Analista de Sistema - Suporte e Infraestrutura

No processamento de grandes volumes de dados, as chaves assimétricas são uma opção mais rápida que as simétricas para garantir a confidencialidade dos dados.

Comentário:

Justamente ao contrário. A opção mais rápida é a simétrica, e ela é utilizada na prática. O seu desafio é sempre o processo de troca de chaves... E aí neste processo entra a criptografia assimétrica para preencher e resolver essa situação.

Gabarito: E

Vamos conhecer agora os **principais algoritmos de criptografia simétrica**.

DES

Durante muitos anos o DES foi o algoritmo padrão utilizado na criptografia simétrica. Foi criado pela IBM em 1977 com tamanho de chaves relativamente pequenas, quando comparada com as demais.

Utiliza chaves de 64 bits, dos quais 56 bits são randômicos e os 8 restantes são de paridade para garantir a integridade da chave. E aqui temos uma primeira observação. **Apesar do tamanho da chave ser de 64 bits, a robustez para efeito de quebra de chave era de 56 bits, uma vez que os 8 são derivados dos 56 bits.** Assim, para efeito de prova, devemos considerar, quando abordado em um caráter genérico, que o DES utiliza chave de 56 bits.

CESPE - 2019 - TJ-AM - Assistente Judiciário – Programador

O DES (data encryption standard) é um sistema de codificação simétrico por blocos de 64 bits, dos quais 8 bits (1 byte) servem de teste de paridade.

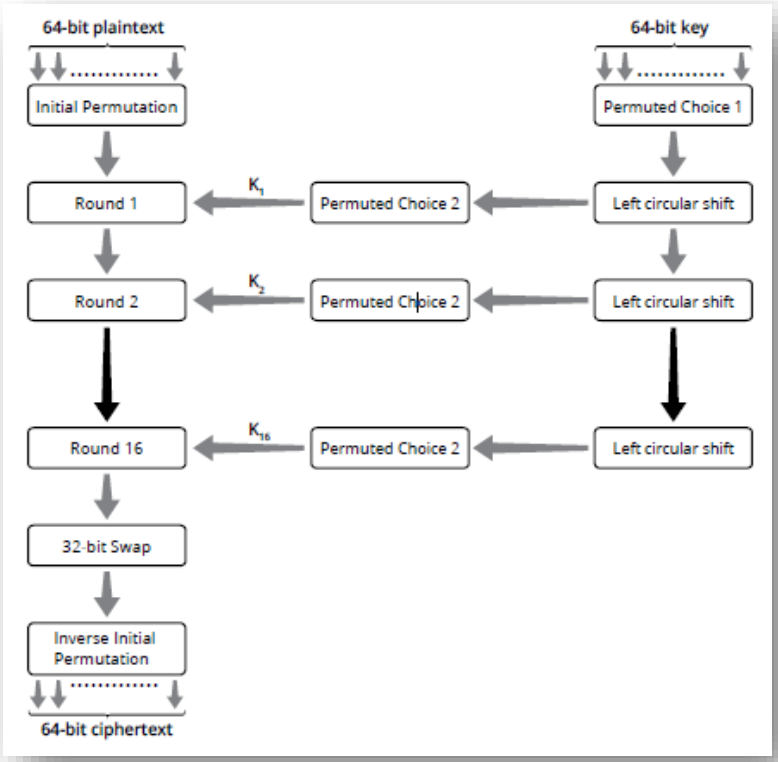
Comentários:

Simples e direto, conforme já conversamos.

Gabarito: C

Através da utilização do ataque de força bruta, foi quebrado em desafio lançado pelo NIST em 1997. Entretanto, é utilizado para efeito de estudo até os dias de hoje.

A imagem a seguir retrata o fluxo de operações do algoritmo:



Por utilizar cifra de bloco, o DES pode utilizar quaisquer das técnicas anteriormente mencionadas. Analisando a figura, podemos perceber que o algoritmo se utiliza de 16 rodadas envolvendo ainda técnicas de permutação e substituição.

Utiliza também o conceito de S-BOXES em processos de substituição de bits. A NSA era constantemente acusada de ter um backdoor nessas S-BOXES uma vez que seu funcionamento não era divulgado.

Essa organização é conhecida como rede de Feistel, ou também cifra de Feistel.

A estrutura de FEISTEL opera nas metades dos blocos (32 bits) de cada vez e consiste em 4 estágios (apresentados no diagrama abaixo):

Expansão - o bloco de 32 bits (metade do bloco) é expandido para 48 bits usando a permutação expansiva, representada pelo E no diagrama, através da duplicação de alguns bits.

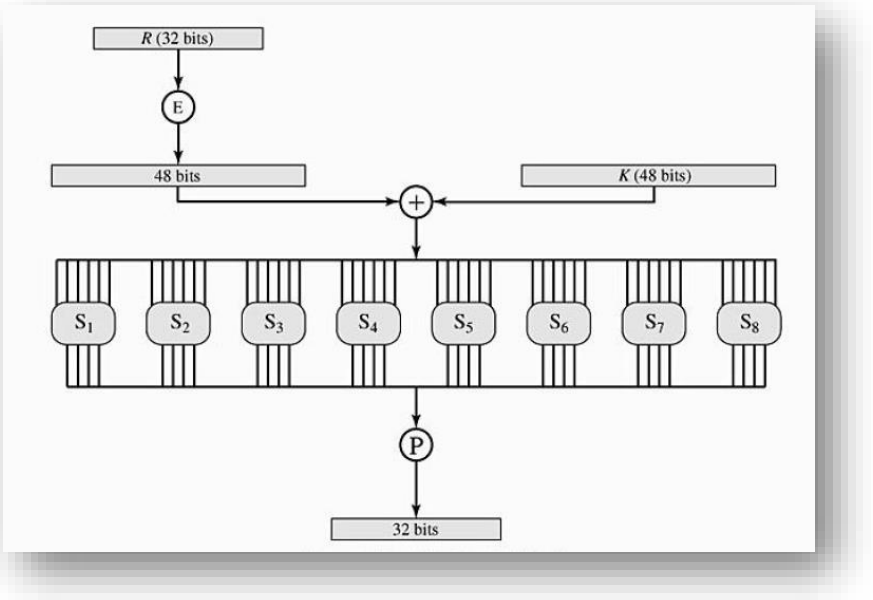
Mistura de chaves - o resultado é combinado com uma subchave usando uma operação XOR. Dezesseis subchaves de 48 bits - uma para cada round - são derivadas da chave principal utilizando o escalonamento de chaves (descrito abaixo).

Substituição - após trocar a subchave, o bloco é dividido em oito pedaços de 6 bits antes do processamento pelo box de substituição ou S-box. Cada um dos oito S-boxes substitui os seis bits de entrada por quatro bits de saída de acordo com uma transformação não-linear, fornecida por uma lookup table. Os s-boxes fornecem o núcleo da segurança do DES - sem eles, a cifra seria linear e quebrada de forma trivial.

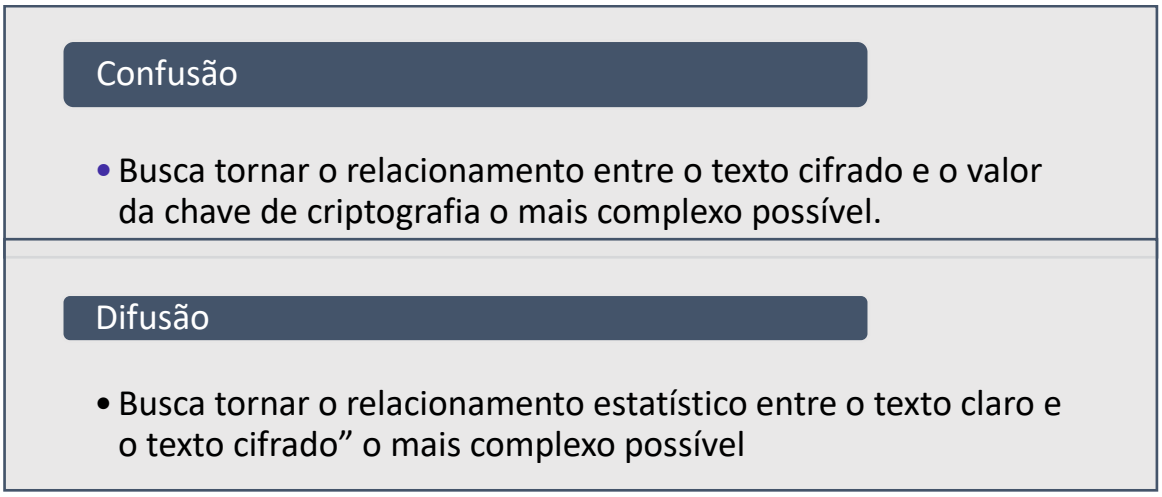
Permutação - finalmente, as 32 saídas das S-boxes são rearranjadas de acordo com uma permutação fixa, o P-box.

ESCLARECENDO!

A figura abaixo representa essas etapas:



A substituição ocorrida nos S-boxes, a permutação de bits nos P-boxes e a expansão fornecem a chamada "confusão e difusão", respectivamente, um conceito identificado por Claude Shannon nos anos 1940 como uma condição necessária para uma cifragem prática e segura.



Ainda, aproveitando o bloco para essa complementação, cabe citar também o princípio de *Kerckhoff*, que foca em dois pilares básicos, vejamos:

--> **Algoritmos** = Devem ser **Públicos** e de amplo conhecimento para gerar resiliência e robustez frente à comunidade.

--> **Chaves** = **Secreta,** partindo do pressuposto que deve ser de conhecimento privativo.

CESPE / CEBRASPE - 2020 - Ministério da Economia - Tecnologia da Informação

Apesar de a criptografia moderna estar presente no cotidiano dos usuários, a implantação de mecanismos criptográficos requer diversos cuidados, como a utilização de algoritmos e protocolos conhecidos e extensivamente analisados e o uso de primitivas criptográficas adequadas para cada situação.

Comentários:

Aproveitando esse bloco para trazer uma complementação... Algoritmos seguros sem dúvida são aqueles que têm a oportunidade de serem amplamente testados e conhecidos em termos de sua estrutura e processo.

Ou seja, a segurança maior não tá no algoritmo em si, mas a chave. Mas é importante que a comunidade tenha essa percepção de que o algoritmo é seguro, frente a múltiplas interações com o código.

Além disso, as primitivas criptográficas também trazem à baila a escolha de entradas no algoritmos, padrões de chaves e outras derivações que são necessários para que a criptografia funcione da forma adequada.

Gabarito: C

CESPE - 2019 - TJ-AM - Assistente Judiciário – Programador

Segundo o princípio de Kerckhoffs, a capacidade de proteger mensagens se torna mais forte quando se utilizam chaves públicas no processo.

Comentários:

Conforme seu princípio, as chaves têm que ser secretas.

Gabarito: E

CESPE - 2019 - TJ-AM - Assistente Judiciário – Programador

A segurança de um sistema criptográfico simétrico deve estar na chave e no tamanho dessa chave, e não nos detalhes do algoritmo.

Comentários:

Derivado do mesmo princípio de Kerckhoff. Como os algoritmos é público, não faz sentido ancorar sua segurança nos detalhes do algoritmo. Já a chave, tem-se o tamanho e privacidade que contribuem diretamente no processo.

Gabarito: C

CESPE / CEBRASPE - 2022 - BANRISUL - Analista de Segurança da Tecnologia da Informação

DES (data encryption standard) e AES (advanced encryption standard) são exemplos de cifras de blocos em que as mensagens a serem criptografadas são processadas em blocos de kilobits (Kb).

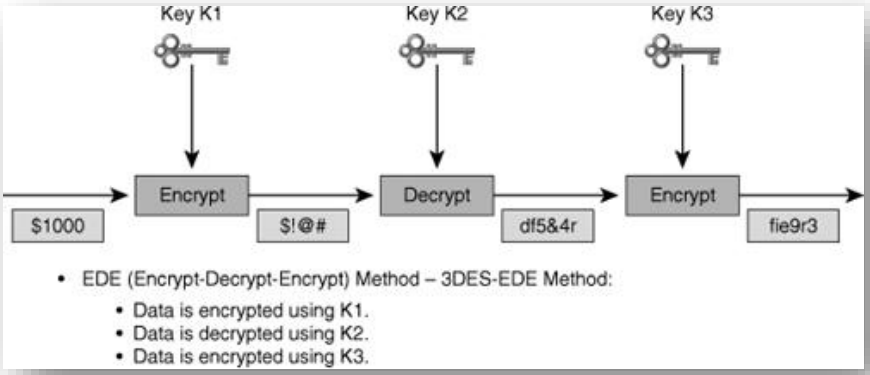
Comentários:

Pessoal, ainda que não tenhamos visto o AES, que seguirá o mesmo padrão do DES em termos do processamento de blocos, mudando tão somente seu tamanho, tem-se que ambos processam em blocos de BITS.

Gabarito: E

3DES

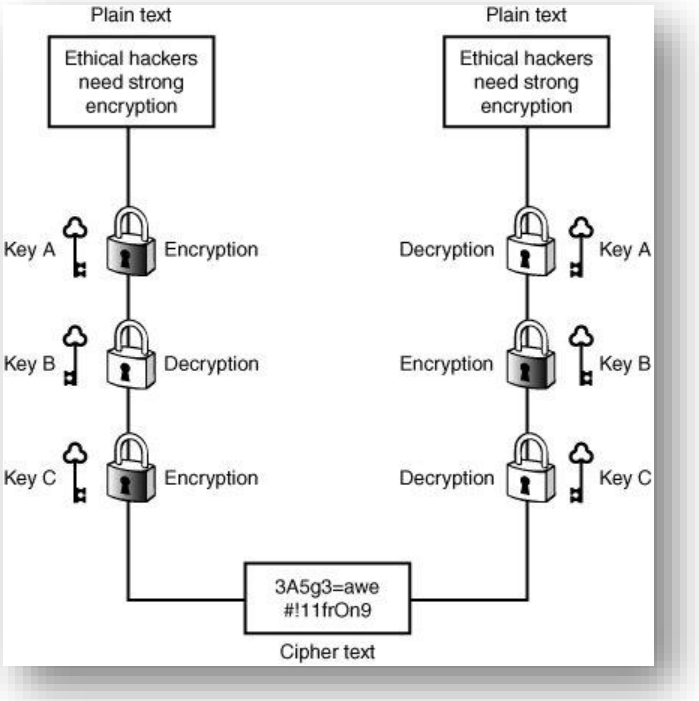
Na tentativa de dar uma sobrevida ao DES, criou-se o 3DES, que nada **mais é do que a aplicação do DES três vezes, com o detalhe de que na segunda vez, faz-se o processo de decriptação**.



Desso modo, **ao se utilizar três chaves distintas, tem-se uma robustez de 56 bits por chave, totalizando 168 bits de tamanho de chave**.

Entretanto, o 3DES suporta a utilização de apenas duas chaves, assumindo que a primeira e a terceira sejam iguais. Nesse caso, a robustez da chave se restringiria a 112 bits.

No processo de decriptação, basta inverter o sentido da operação, conforme figura a seguir:



RC – Rivest Cipher

O RC possui três versões que usualmente aparecem em provas, quais sejam: 4, 5 e 6.

É um algoritmo desenvolvido pela RSA.

O RC4 é orientado a byte e possui tamanho de chave variável até 2048 bits, com algoritmo baseado em permutação randômica. **Possui como principal característica a utilização de cifras de fluxo**. É um algoritmo bastante utilizado no TLS.

O RC4 é muito simples e sua força se concentra no mecanismo de geração de uma sequência pseudoaleatória. A chave desse algoritmo é usada para inicializar um vetor interno.

O RC5 é um algoritmo parametrizado que utiliza **cifra de bloco de tamanho variável (32, 64 e 128 bits), tamanho de chave variável (0 a 2048) e quantidade variável de rodadas (0 a 255)** de processamento. Utiliza três rotinas padrões: expansão, encriptação e decriptação.

Já o RC6, sendo baseado no RC5, também utiliza cifra de bloco. Acrescenta recursos de inclusão de multiplicação de inteiros e registradores de 4 bits, enquanto o RC5 utilizava de 2 bits.

AES – Advanced Encryption Standard

Foi desenvolvido para substituir o DES como padrão do governo americano. Suporta tamanhos de chaves variáveis. Entretanto, por padrão, **utiliza-se o tamanho de bloco fixo de 128 bits, podendo ser utilizado chaves de 128, 192 e 256 bits.** Não utiliza a tão conhecida rede de Feistel disseminada pelo DES, mas sim o algoritmo de Rjindael.

Importante você já tomar nota que o AES também trabalha com rodadas ou interações. Entretanto, diferentemente do DES que possuía 16 rodadas fixas, o AES trabalhar com 10, 12 ou 14 rodadas, a depender do tamanho da chave utilizada, sendo 128, 192 ou 256, respectivamente.

E nesse ponto, faço um destaque rápido a respeito de algumas referências de algoritmos seguros hoje tomando como referência seus tamanhos de chaves.

- **64 bits = chave fraca**
- **128= segurança de rotina**
- **256= considerado seguro**

Assim, vejamos, inclusive, a questão...

CESPE / CEBRASPE - 2021 - SERPRO - Analista - Especialização: Desenvolvimento de Sistemas

Para arquivos criptografados com algoritmos que utilizam chaves de até 256 bits, é viável realizar ataques de força bruta no espaço de chaves, com real possibilidade de sucesso em tempo aceitável.

Comentários:

Na linha do que acabamos de comentar. Vejam que com 128, ainda é considerado um modelo de segurança de rotina. Isso quer dizer que depende do contexto de aplicação, mas ainda tem um nível aceitável.

Gabarito: E

Seu funcionamento pode ser resumido em quatro estágios, quais sejam:

SubBytes – Utiliza uma caixa-S para substituição operada byte a byte de acordo com uma tabela

ShiftRows – Permutação Simples

MixColumns – Uma combinação linear que utiliza aritmética sobre corpo finito.

AddRoundKey – Um XOR bit a bit simples do bloco atual com uma parte da chave expandida.

Portanto, **temos três estágios de substituição (Subbytes, MixColumns e AddRoundKey) e um de permutação (shiftRows).** É sempre importante lembrar que todos os estágios são reversíveis, até porque será necessário realizar a decriptação dos dados.

FGV - 2022 - TJ-DFT - Analista Judiciário - Suporte em Tecnologia da Informação

Caio recebeu a tarefa de melhorar a segurança da rede local do Tribunal de Justiça. A demanda solicitada foi a implementação de um sistema de criptografia que atenda aos requisitos a seguir.

1. receber como entrada um bloco de texto sem formatação;

2. trabalhar com tamanhos de chaves diferentes;

3. movimentar o bloco para uma matriz quadrada onde são executadas suas operações;

4. relacionar o número de rodadas do algoritmo com o tamanho da chave.

Para cifrar as mensagens e atender aos critérios determinados, Caio deve utilizar o algoritmo criptográfico:

A RSA;

B AES;

C DES;

D 3DES;

E ELGAMAL.

Comentários:

Vejam que a questão traz um breve resumo de características, exatamente, do AES. O destaque sem dúvida fica por conta do número de rodadas variável com o tamanho da chave. Indo de 10, 12 e 14 rodadas para as chaves 128, 192 e 256, respectivamente.

Além disso, conforme nós vimos, todas as operações são realizadas sobre matrizes quadradas.

Gabarito: B

FGV – 2022 – TRT – 13ª Região (PB) – Analista Judiciário – Tecnologia da Informação

Com relação ao padrão criptográfico AES, assinale V para afirmativa verdadeira e F para a falsa.

I. É uma cifra de bloco cujo objetivo é substituir o DES em aplicações comerciais. Usa um tamanho de bloco de 128 bits e um tamanho de chave de 128, 192 ou 256 bits.

II. Usa uma estrutura de Feistel a cada rodada completa que consiste em quatro funções distintas: substituição de bytes, permutação, operações aritméticas sobre um corpo finito e operação XOR com uma chave.

III. Comparada a cifras de chave pública, como o RSA, a estrutura do AES, e da maioria das cifras simétricas, é muito complexa e não pode ser explicada tão facilmente quanto o RSA e os algoritmos semelhantes.

As afirmativas são, respectivamente,

A V, V e V.

B V, F e V.

C V, V e F.

D F, F e V.

E F, V e V.

Comentários:

Vamos aos itens:

I – Temos aí as principais características do AES. Importante sempre reforçar a característica do bloco padrão de 128 bits, enquanto as chaves, de fato, podem variar nas três versões. **CORRETO**

II – A estrutura de Feistel é usada no DES e 3-DES. **INCORRETO**

III – Ainda não vimos o RSA e os algoritmos de criptografia assimétrico, mas adianto que o modelo matemático destes é, de fato, mais simples em termos de sua compreensão. **CORRETO**

Gabarito: B

Outros exemplos de algoritmos de criptografia simétrica são:

Blowfish, Twofish e IDEA

FGV – 2022 – SEAD-AP – Perito Criminal – Ciência da Computação – Analista de Sistema

Aline deseja enviar uma mensagem cifrada para Marcos usando um esquema de cifra de chave simétrica. Portanto, para encriptar sua mensagem Aline deve usar o algoritmo

A AES.

B Diffie-Helman.

C MD5.

D RSA.

E SHA-1.

Comentários:

Pessoal, diante dos algoritmos que vimos até agora, temos que o AES é nossa opção, certo?

Veremos os demais mais à frente, mas já adianto:

b) Assimétrico

c) Função HASH

d) Assimétrico

e) Função HASH

Gabarito: A

CESPE – 2019 – MPC-PA – Analista Ministerial – Tecnologia da Informação

Assinale a opção que corresponde ao algoritmo criptográfico conceitualmente menos resistente a ataques de força bruta.

A Twofish

B DES

C AES

D ECC

E RSA

Comentários:

Pessoal, sem dúvida, temos o DES como a maior fragilidade, dadas suas características de tamanho de chave. Lembrando que o DES foi de suma importância no processo de geração dos primeiros resultados efetivos em termos de criptografia. Entretanto, é antigo e já está defasado.

Gabarito: B

FGV – 2022 – TRT – 13ª Região (PB) – Técnico Judiciário – Tecnologia da Informação

João quer enviar uma mensagem cifrada para Maria e escolheu um algoritmo no qual seja possível usar a mesma chave criptográfica para encriptação do texto puro e decriptação do texto cifrado.

Para isso, João pode utilizar o algoritmo

A Blowfish.

B ECC.

C MD5.

D SHA-1.

E RSA.

Comentários:

O conhecimento desses algoritmos de menor expressão se restringem à sua categorização. Esse é o caso do Blowfish como algoritmo simétrico.

Gabarito: A

CESPE / CEBRASPE – 2019 – TJ-AM – Analista Judiciário – Analista de Sistemas

A segurança de um sistema criptográfico simétrico tem como características básicas a força do algoritmo e o comprimento da chave.

Comentários:

Essa é a ideia pessoal. Quanto ao comprimento da chave, já estamos cansados de reforçar a importância, certo? E quanto à força do algoritmo, temos o aspecto da sua resiliência, no sentido de não ser fragilizado frente a ataques de criptoanálise.

Gabarito: C

FGV/TJDFT/Suporte em TI/2022

Sobre criptografia, analise as afirmativas a seguir.

I. O algoritmo AES é um exemplo de algoritmo criptográfico que utiliza cifra de bloco simétrico e chave de criptografia com 128, 192 ou 256 bits.

II. A cifra de Vigenère é um exemplo de cifra de transposição polialfabética.

III. As cifras de substituição rearranjam os caracteres de uma mensagem segundo um algoritmo especifico, de forma a embaralhar os caracteres do texto.

Está correto o que se afirma em

A I, apenas.

B II, apenas.

C III, apenas.

D I e II, apenas.

E I e III, apenas.

Comentários:

Questão mais ampla que aborda vários conceitos. Vamos entendê-la.

I – O primeiro item é bem tranquilo, certo pessoal? Já vimos reiteradas vezes. CORRETO

II – Pessoal, um item para trabalharmos um novo conhecimento. A cifra de Vigenère é basicamente uma cifra de SUBSTITUIÇÃO POLIALFABÉTICA. A sua ideia base nada mais é do que a aplicação sucessiva da cifra de Cesar com variação na quantidade de letras para subtituição. Utiliza ainda um conceito de "palavra-chave" que vai ditar a regra desses deslocamentos. INCORRETO

III - A referida descrição está para a transposição pessoal, no sentido de haver o embaralhamento. INCORRETO

Gabarito: A

CRIPTOGRAFIA ASSIMÉTRICA

A criptografia Assimétrica, também conhecida como criptografia de chaves públicas é caracterizada **pelo fato de se utilizar duas chaves no processo criptográfico, ou seja, caso seja utilizada uma para criptografar os dados, deve-se, necessariamente, usar a outra para descriptografar**. As duas chaves utilizadas são conhecidas como privada e pública.

A primeira é de conhecimento exclusivo do dono da chave, enquanto a segunda, como o próprio nome diz, é de conhecimento público. *Como assim André? Todos conhecem a chave pública? Isso não é inseguro?* Calma meus caros. É isso mesmo, todos conhecem a chave pública. E não, não é inseguro. Elas possuem propósitos distintos em suas formas de utilização. Veremos a seguir.

Agora pessoal, um detalhe importante que já foi cobrado em prova. **O processo de criptografia de chave pública não se restringe a uma única sequência, isto é, não necessariamente se criptografa com a chave privada e decriptografa com a pública.** Por este motivo, não podemos dizer que essa é uma característica que define o modelo de criptografia assimétrica.

Outro ponto importante é que o surgimento desse tipo de técnica possibilitou a troca de chaves simétrica de uma forma segura. Ou seja, agora é possível usar algoritmos de criptografia assimétrica para trocar informações de chaves simétricas.

Essa característica é a base das soluções de certificação digital.

Avançando um pouco mais na nossa conversa, vamos diferenciar agora a sequência de utilização das chaves. Isso é muito importante e prestem bastante atenção.

Se o objetivo é garantir a **confidencialidade**, deve-se cifrar com a chave pública do **RECEPTOR e decifrar com a chave privada do RECEPTOR!**

Se o objetivo é garantir a **autenticidade**, deve-se cifrar com a chave privada do **EMISSOR e decifrar com a chave pública do EMISSOR!**

CESPE / CEBRASPE – 2021 – SEFAZ-AL – Auditor Fiscal de Finanças e Controle de Arrecadação da Fazenda Estadual

A criptografia assimétrica utiliza duas chaves, uma pública e outra privada, para cifrar e decifrar mensagens.

Comentários:

Simples assim pessoal. Essa característica é justamente o que define a criptografia assimétrica.

Gabarito: C

CESPE / CEBRASPE – 2021 – PG-DF – Técnico Jurídico – Tecnologia e Informação

O sistema criptográfico pode usualmente alterar a chave privada de um usuário, gerando uma nova chave pública correspondente.

Comentários:

Lembremos sempre que o par de chaves é gerado de forma conjugada, onde uma chave é derivada da outra. Logo, sempre que é gerado uma nova chave privada, ainda que em regime de alteração, tem-se, necessariamente, que se gerar uma nova chave pública correspondente.

Gabarito: C

CESPE – TCE-SC/AFCE – Área TI/2016

Os algoritmos de criptografia de chave pública devem ser computacionalmente fáceis, a fim de que o receptor de uma mensagem cifrada com uma chave pública a decriptografe utilizando sua chave privada para recuperar a mensagem original.

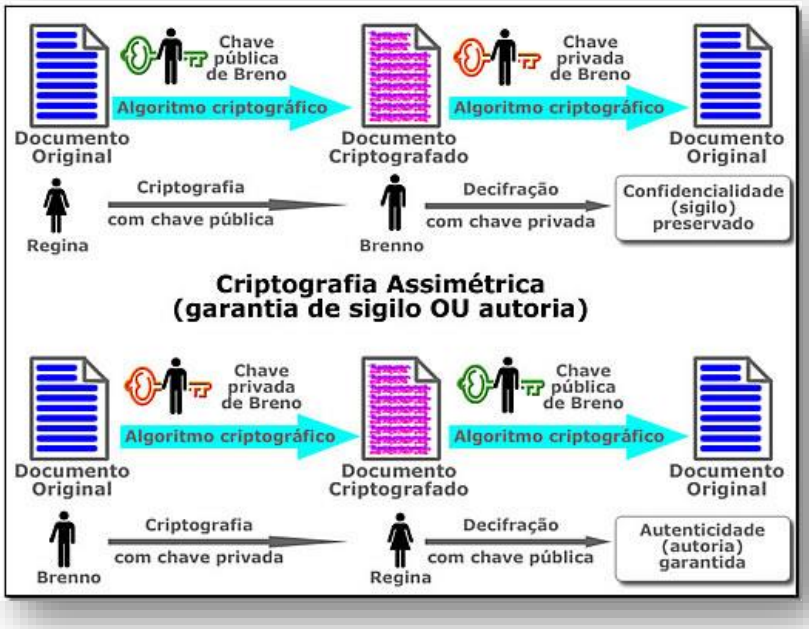
Comentários:

Pessoal, no primeiro momento que li essa alternativa, fiz a interpretação a seguir: "Dizer que o algoritmo de criptografia de chave pública deve ser computacionalmente fácil é um problema pessoal. O que deve ser computacionalmente fácil é a geração do par de chaves, o que é bem diferente. A robustez do algoritmo está na dificuldade de se achar ou definir a chave privada a partir da chave pública e vice-versa. Inclusive, há uma grande complexidade do algoritmo RSA, que é assimétrico. "

Entretanto, com uma leitura mais cautelosa, perceba o detalhe da abordagem. A facilidade computacional do algoritmo está atrelado ao processo adequado de descriptografia, ou seja, uma vez que eu insiro a chave correta, ele facilmente realiza o processo. Isso é uma verdade.

Gabarito: C

Conseguiram entender? Bom, vamos explicar agora. Vamos usar a figura abaixo:



Vamos lembrar que a chave pública é de conhecimento público, ou seja, na figura em análise, a REGINA, que é a emissora da mensagem, conhece a chave pública do Breno. Portanto, quando REGINA cifra a mensagem com a chave pública de Brenno, qual a única chave capaz de decifrar a mensagem? Exato, a chave privada de Breno! E quem é a única pessoa que conhece a chave privada do Brenno? O próprio Brenno!!!

Logo, o único que será capaz de interpretar a mensagem enviada será o Breno. Temos aí a garantia da confidencialidade.

E agora, o segundo cenário. Somente Brenno conhece sua chave privada. Logo, ele criptografa com sua chave privada. Qual a única chave capaz de decifrar essa mensagem? Exato! A chave pública de Brenno. Ou seja, se eu pegar a chave pública de qualquer outra pessoa e tentar decifrar a mensagem, provavelmente a mensagem não fará nenhum sentido, ou seja, não será decifrada corretamente. Agora, se eu usar a chave Pública de Brenno, terei a mensagem correta. Logo, posso afirmar, pelo princípio do par de chaves assimétricas, que a pessoa que cifrou o texto é o Brenno.

Tranquilo pessoal? Busquem entender esses conceitos e não decorar. Eles são extremamente importantes. Caso não tenha ficado claro, volte e leia de novo com mais calma.

CESPE / CEBRASPE – 2021 – SEFAZ-AL – Auditor Fiscal de Finanças e Controle de Arrecadação da Fazenda Estadual

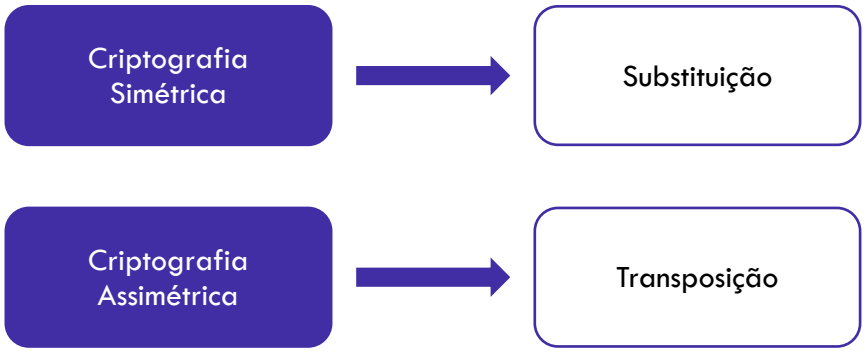
Na criptografia assimétrica, é necessário que remetente e destinatário de uma mensagem tenham, cada um, uma das chaves do par (chave pública, chave privada) para que a mensagem seja corretamente cifrada na origem e decifrada no destino.

Comentários:

Ainda que a questão não tenha sido explícita no sentido de indicar qual chave deve ficar com quem, não há espaço para invalidação do item, ao meu ver. Assumindo que a chave privada sempre ficará com o dono, naturalmente, o seu respectivo par de chave (pública nesse caso) deve ser compartilhado.

Gabarito: C

Gostaria de acrescentar ainda um aspecto que tem aparecido em algumas questões. Vimos as técnicas de substituição e transposição. **Desse modo, a criptografia Simétrica está fundamentada na técnica de SUBSTITUIÇÃO, enquanto a Assimétrica, na técnica de TRANSPOSIÇÃO.** Isso não quer dizer que possa, em alguns casos, usar outras técnicas, ok?



Vamos conhecer agora os principais algoritmos de criptografia assimétrica e como eles funcionam.

FGV – Professor de Informática (SEAD-AP)/2022

Com relação aos métodos de criptografia de chave pública, considere as afirmativas a seguir.

III. Cada participante em um sistema de chave pública possui um par de chaves, uma pública e outra, privada.

II. Qualquer participante pode criptografar e decriptografar uma mensagem usando a própria chave privada.

III. Quando o participante P1 envia uma mensagem criptografada para P2, é preciso que P2 conheça a chave privada de P1.

É correto somente o que se afirma em

a) I.

b) II.

c) III.

d) I e II.

e) II e III.

Comentários:

Vamos lá pessoal... Questão que traz o resumo da introdução de criptografia assimétrica.

I – Nosso princípio da criptografia assimétrica. Sem dúvida, cada participante tem o par de chaves. E sempre importante lembrar que uma chave deriva da outra, ou seja, só funcionam conjuntamente. Esse processo de geração de chaves é de suma importância, pois é nele que se garante a vinculação das chaves, e os processos de criptografia e descriptografia futuros. Portanto, correto o item.

II – Na linha do que adiantamos no item anterior, as chaves se complementam. Logo, para os processos onde são geradas as criptografias a partir das chaves públicas, somente as respectivas chaves privadas que compõem os seus pares, ou ainda, que pertencem ao respectivo dono da chave que será capaz de descriptografar. Logo, item Errado.

III – Errado pessoal. Vejam que a questão coloca o contexto de que um outro participante, no caso P2, precisa conhecer a chave privada do participante P1. Isso jamais deve acontecer. A chave privada é de conhecimento única e exclusiva do dono. Somente a chave pública é de conhecimento amplo.

Gabarito: A

CESPE – ANATEL/Analista – Suporte e Infraestrutura de Tecnologia da Informação/2014

Para que a criptografia de chave pública seja considerada segura, uma das premissas é que o conhecimento do algoritmo, o conhecimento de uma das chaves e a disponibilidade de amostras de texto cifrado sejam, em conjunto, insuficientes para determinar a outra chave.

Comentários:

Questão bem bacana da ANATEL. De fato, os três pontos apresentados são características desses algoritmos. Há o conhecimento público da chave pública e do algoritmo utilizado. Além disso, caso o usuário intercepte a mensagem cifrada, isso, por si só, não permite que ele obtenha informações da chave privada.

Gabarito: C

FGV – Auditor de Controle Externo – Tecnologia da Informação (TCE-TO)/2022

Bernardo e João são auditores recém-concursados no TCE/TO.

Bernardo precisa enviar documentos sigilosos para João e vice-versa, contudo, nenhum deles utilizou ainda a ferramenta de criptografia disponível na instituição.

Sabendo-se que é utilizada a criptografia por chave pública, o procedimento que deve ser seguido por cada auditor antes de tramitar os documentos é:

a) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; guardar a chave privada; e encriptar os documentos utilizando a chave pública do destinatário;

b) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; enviar a chave privada para o destinatário; e encriptar um documento utilizando a chave privada enviada;

c) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; guardar a chave privada; e encriptar os documentos utilizando a chave privada do remetente;

d) gerar a chave pública para encriptação e decriptação dos documentos; enviar a chave pública para o destinatário; e encriptar os documentos utilizando a chave pública enviada;

e) combinar uma senha entre eles; encriptar e decriptar os documentos utilizando a senha combinada..

Comentários:

Vamos lá pessoal. Trata-se de uma questão conceitual. Sem dúvida, o início passa pela geração do par de chaves de qualquer participante no processo. Em seguida, deve-se tornar a chave pública conhecida para que seja possível a interação com outros participantes no processo, enquanto a chave privada deve permanecer restrita e em sigilo de posse do dono.

Por fim, como o objetivo é garantir a confidencialidade, deve-se criptografar com a chave pública do destinatário. Assim, somente a respectiva chave privada será possível de descriptografar. Lembrando que a posse da chave privada é do dono, ou seja, somente o próprio destinatário terá condições de abrir.

Gabarito: A

Diffie-Hellman – DH

Principal algoritmo quando se fala **no propósito de troca de chaves simétricas em um meio inseguro sem conhecimento prévio do segredo**. Há de se destacar desde já que o DH por si só não garante autenticidade e, portanto, está sujeito a ataques de interceptação, como o Man-in-the-middle, conforme veremos à frente.

O protocolo VPN IPSec, por exemplo, utiliza o DH para tal finalidade. Esse algoritmo não é utilizado para cifrar e decifrar mensagens, mas tão somente providenciar um meio seguro o suficiente para troca de chaves através de um canal seguro.

Na sua versão mais atual o DH pode ser utilizado conjuntamente com algoritmos de curva elíptica criando um processo chamado Perfect Forward Secrecy (PFS), otimizando a resistência contra-ataques que visam obter chaves de sessão, principalmente em cenário de navegação WEB segura através do HTTPS.

A sua estrutura e robustez reside na complexidade e problema do logaritmo discreto.

CESPE / CEBRASPE – 2022 – BANRISUL – Analista de Segurança da Tecnologia da Informação

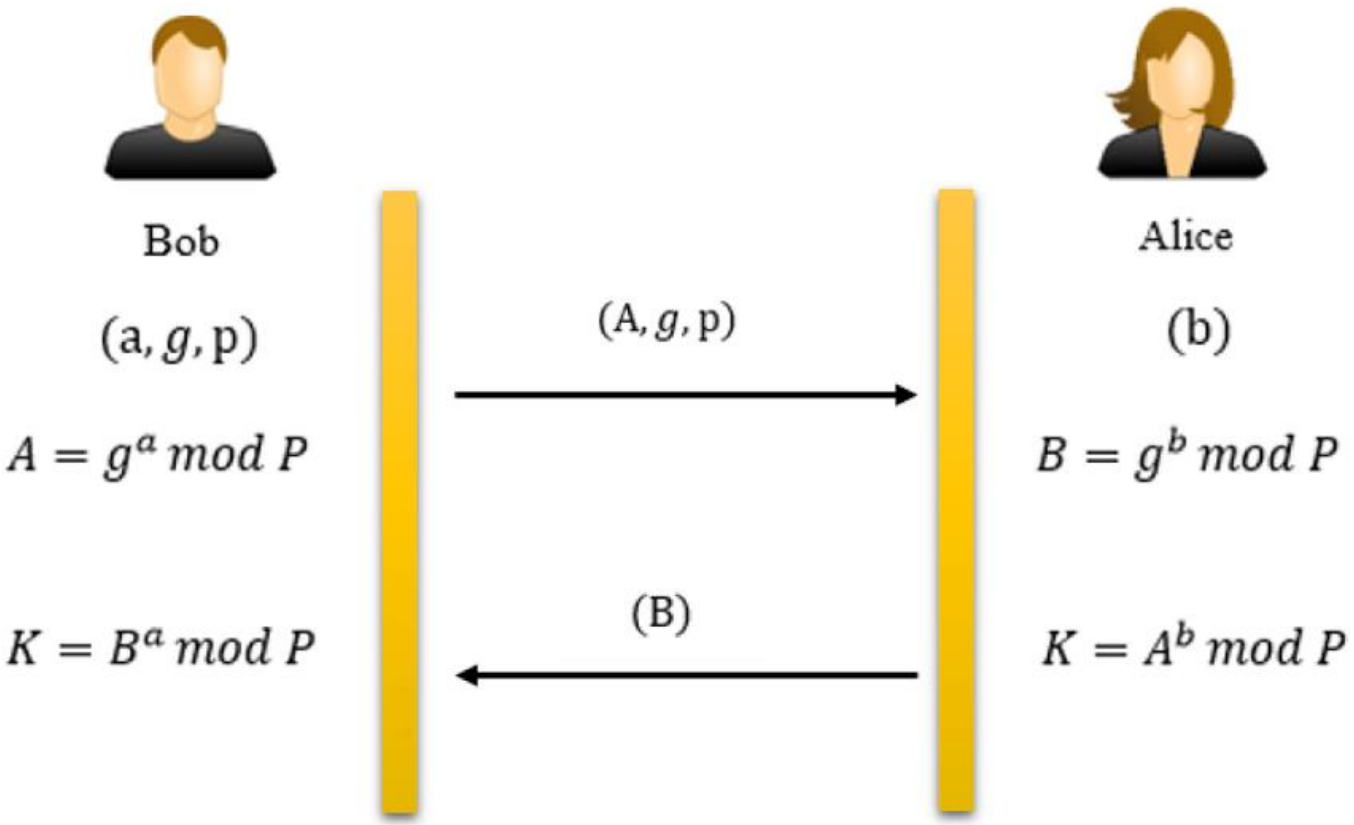
Algoritmos de chaves assimétricas dispensam a necessidade de um canal seguro para o compartilhamento de chaves.

Comentários:

Sem dúvida pessoal, esse foi o principal valor gerado por parte da criptografia assimétrica, que possibilitou, inclusive a resolução do problema de troca de chaves da criptografia simétrica.

Gabarito: C

A seguir, algumas imagens que representam seu fluxo de operação:

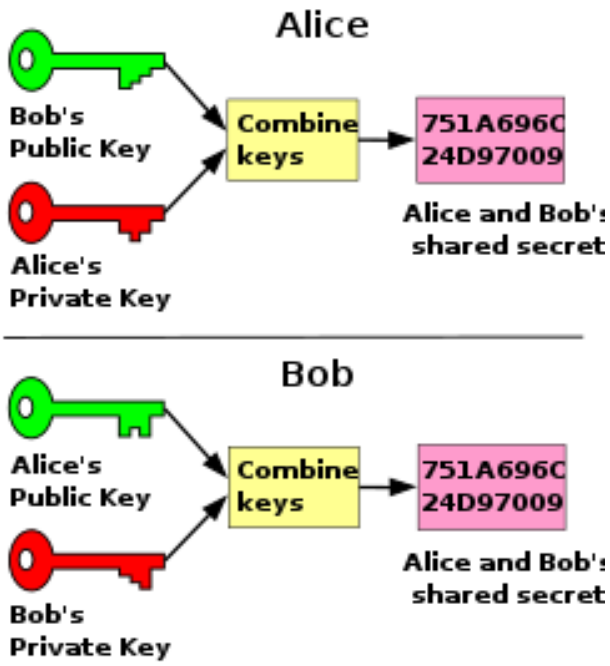


Importante ter no radar a passagem dos parâmetros, e quais são escolhidos diretamente e quais são derivados. Vejam que BOB escolhe os parâmetros (a,g,p). Em seguida, calcula-se "A", a partir desses parâmetros, para posterior troca de alguns parâmetros escolhidos e outros derivados. O mesmo procedimento é feito por Alice, que devolve o parâmetro "B" calculado a partir do parâmetro "b" escolhidos e operacionalizado com "g" e "p".

Dessa forma, no final, gera-se a chave "K", que utiliza em suas operações os parâmetros derivados "A" e "B" em cada lado de forma invertida. Vejam que, na prática, é possível que ambos calculem a parâmetro "K", sem precisar que essa informação seja trafegada no processo.

Importante que vocês percebam ainda que, na prática, "A" e "B" são justamente as chaves públicas e, portanto, podem ser compartilhadas e acessadas sem prejuízo para a segurança do sistema.

Ainda, em uma outra perspectiva, podemos entender, de forma didática, a partir da lógica de cores.



Há de se destacar ainda as diferentes implementações a partir dos tipos de chaves utilizadas. Assim surgem os **termos anônimo, estático ou efêmero.**

Vamos dar uma olhada em cada um desses métodos:

- **Anônimo Diffie-Hellman:** Neste método, as chaves públicas utilizadas na troca de chaves Diffie-Hellman não são autenticadas, ou seja, não estão associadas a uma identidade específica nem são assinadas por uma autoridade de certificação. Isso resulta em comunicações anônimas, uma vez que a identidade das partes envolvidas não é verificada. No entanto, essa abordagem é suscetível a ataques man-in-the-middle (MITM), pois um atacante pode se passar por uma das partes envolvidas na comunicação e interceptar ou modificar as mensagens trocadas.

- **Estático Diffie-Hellman:** Neste método, as chaves públicas utilizadas na troca de chaves Diffie-Hellman são estáticas, ou seja, são de longa duração e podem ser reutilizadas em várias sessões de comunicação. As chaves públicas são normalmente autenticadas, seja por assinaturas digitais ou certificados digitais emitidos por uma autoridade de certificação confiável. Isso fornece maior segurança em comparação com o método anônimo, pois a identidade das partes envolvidas é verificada. No entanto, o uso de chaves estáticas pode comprometer a privacidade futura das comunicações, caso a chave privada seja comprometida em algum momento.

- **Efêmero Diffie-Hellman:** Neste método, as chaves públicas utilizadas na troca de chaves Diffie-Hellman são efêmeras, o que significa que são geradas para cada sessão de comunicação e descartadas após o uso. Isso fornece um nível adicional de segurança conhecido como Perfect Forward Secrecy (PFS), que garante que, mesmo se uma chave privada for comprometida no futuro, as comunicações anteriores permanecerão seguras. No entanto, isso requer a geração e a autenticação de novas chaves públicas

para cada sessão, o que pode aumentar a complexidade computacional e a carga na rede. Efêmero Diffie-Hellman é frequentemente combinado com chaves estáticas para autenticar as partes envolvidas.

Em resumo, os métodos anônimo, estático e efêmero do Diffie-Hellman representam diferentes abordagens de implementação com diferentes níveis de segurança e privacidade.

O método anônimo não autentica as partes envolvidas e é suscetível a ataques MITM.

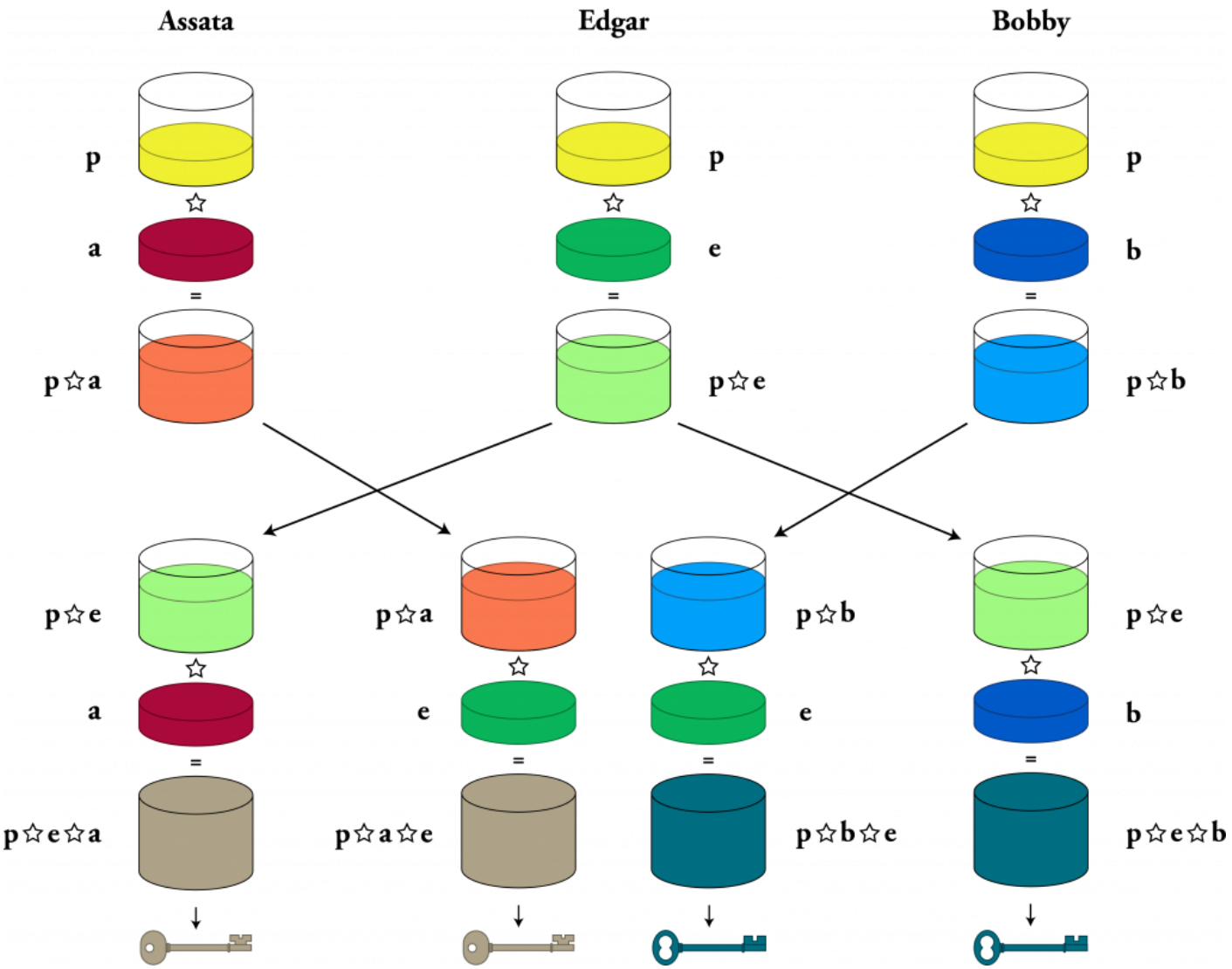
O método estático autentica as partes envolvidas e usa chaves de longa duração, mas não fornece Perfect Forward Secrecy.

O método efêmero fornece Perfect Forward Secrecy, mas exige a geração e a autenticação de novas chaves públicas para cada sessão de comunicação.

Bom, como mencionamos anteriormente, nem tudo funciona sem riscos. Há o caso de vulnerabilidade do tipo Man-in-the-midlle – MITM, principalmente associado aos processos de ausência de autenticação, como o caso de DH no tipo anônimo. Ele ocorre da seguinte forma:

1. **Alice e Bob concordam em usar um número primo grande (p) e uma base (g), que são conhecidos publicamente.**
2. **Um atacante, Mallory, intercepta a comunicação entre Alice e Bob.**
3. **Alice seleciona um número privado (a) e calcula A = g^a mod p. Alice envia A para Bob, mas Mallory intercepta e armazena A.**
4. **Mallory cria um novo número privado (m1) e calcula M1 = g^m1 mod p. Mallory envia M1 para Bob, fazendo-o acreditar que é A.**
5. **Mallory cria um novo número privado (m2) e calcula M2 = g^m2 mod p. Mallory envia M2 para Alice, fazendo-a acreditar que é B.**
6. **Bob seleciona um número privado (b) e calcula B = g^b mod p. Bob envia B para Alice, mas Mallory intercepta e armazena B.**
7. **Alice calcula a chave secreta compartilhada como K_A = M2^a mod p.**
8. **Bob calcula a chave secreta compartilhada como K_B = M1^b mod p.**
9. **Mallory pode calcular a chave secreta compartilhada entre Alice e Mallory como K_AM = A^m2 mod p e a chave secreta compartilhada entre Bob e Mallory como K_BM = B^m1 mod p.**
10. **Agora, Mallory pode interceptar e decifrar as mensagens criptografadas entre Alice e Bob usando as chaves secretas compartilhadas K_AM e K_BM. Além disso, Mallory pode modificar as mensagens antes de recriptografá-las e enviá-las aos destinatários originais.**

Esse processo é descrito na imagem abaixo, caso queiram acompanhar o fluxo a partir da didática das cores:


Assata
Edgar
Bobby
p
a
p☆a
p
e
p☆e
p
b
p☆b
p☆e
a
p☆e☆a
p☆a
e
p☆a☆e
p☆b
e
p☆b☆e
p☆e
b
p☆e☆b

RSA – Rivest, Shamir and Adelman

O RSA foi um algoritmo publicado no ano de 1977. Possui a característica de ser utilizado tanto para processos de cifragem como para produzir hashes. Foi baseado na proposta apresentada pelo algoritmo DH.

É amplamente utilizado por diversas aplicações como SSL e TLS, além de fazer parte da estrutura PKI – Public Key Infrastructure, que veremos com mais detalhes posteriormente, mas, adianto as características de geração de par de chaves, criptografia e descriptografia dos dados e assinatura digital.

Sua robustez reside na dificuldade de se fatorar números extensos. Sugere-se, atualmente, que sejam utilizadas chaves de 2048 a 4096 bits para aumentar a robustez contra ataques de força bruta. Entretanto, diversas aplicações utilizam chaves de 1024, até porque, quanto maior a chave, maior o processamento do algoritmo.

Vamos verificar o funcionamento do RSA pois algumas bancas acabam cobrando a rotina e algumas características dela.

No RSA as chaves são geradas desta maneira:

Escolha de forma aleatória dois números primos grandes “p” e “q”, da ordem de 10^{100} no mínimo.

Compute n = p.q

Compute a função totiente em n:phi(n) = (p-1)(q-1)

Escolha um inteiro “e” tal que 1 < e < phi(n), de forma que “e” e phi (n), sejam primos entre si.

Compute “d” de forma que d.e ≡ 1 mod {phi(n)} , ou seja, “d” seja o inverso multiplicativo de “e” em mod {phi(n)}.

No passo 1, os números podem ser testados probabilisticamente para primalidade.

No passo 5, é usado o algoritmo de Euclides estendido, e o conceito de inverso multiplicativo que vem da aritmética modular

Por final temos:

A chave pública: o par (n,e).

A chave privada: a tripla (p,q,d). De fato, para desencriptar, basta guardar “d” como chave privada, mas os primos “p” e “q” são usados para acelerar os cálculos.

Cifragem

Para transformar uma mensagem “m”, onde 0 < m < n, numa mensagem “c” cifrada usando a chave pública do destinatário “n” e “e”, basta fazer uma potenciação modular:

$c = m^e \ mod(n)$

A mensagem então pode ser transmitida em canal inseguro para o receptor. Há um algoritmo para realizar esta potência rapidamente.

Decifragem

Para recuperar a mensagem “m” da mensagem cifrada “c” usando a respectiva chave privada do receptor “n” e “d”, basta fazer outra potenciação modular:

$m = c^d \ mod(n)$

Todo o processo é feito a partir da divisão de blocos de tamanhos limitados.

FGV – 2022 – SEFAZ-BA – Agente de Tributos Estaduais – Administração Tributária

Os métodos criptográficos, de acordo com a chave utilizada, podem ser classificados em duas categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Assinale a opção que indica um exemplo de método criptográfico da categoria que utiliza chaves assimétricas.

A Blowflish.

B RSA.

C 3DES.

D IDEA.

E AES.

Comentário:

Questão bem simples pessoal, com mera associação e categorização, no caso, dos algoritmos. Então, conforme vimos, o RSA está ancorado na criptografia Assimétrica.

Gabarito: B

FGV – 2022 – SEFAZ-BA – Agente de Tributos Estaduais

A equipe de segurança de um órgão público está em busca de um algoritmo de criptografia que possua as seguintes características:

(III) duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono; e

(ii) quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la.

De acordo com as características desejadas pela equipe de segurança, o algoritmo de criptografia que deve ser usado é o:

A RC4;

B DES triplo;

C SHA-256;

D Twofish;

E RSA.

Comentário:

Novamente, temos as características primárias descritas no enunciado, remetendo para a cripgrafia assimétrica. No caso, o algoritmo representante da criptografia assimétrica é o RSA.

Gabarito: E

FCC – TJ-AP/Analista Judiciário – TI/2014

Um Analista de TI do Tribunal de Justiça recebeu a incumbência de planejar e implementar um esquema de criptografia de Chave Pública para a troca de informações entre as duas comarcas de Macapá. Dentre os diferentes algoritmos existentes, ele deve escolher o

a) AES.

b) RC6.

c) DES.

d) IDEA.

e) RSA

Comentário:

Vejamos o tanto de questões que resolveríamos por simplesmente lembrar que o RSA é um algoritmo de criptografia assimétrica.

Gabarito: E

El Gamal

O El Gamal possui **como segurança de seu sistema a dificuldade do cálculo de logaritmos discretos em um corpo finito**.

Sua principal aplicação é na transferência de assinaturas digitais e trocas de chaves no estabelecimento de comunicações. Possui três componentes básicos: gerador de chaves, algoritmo de cifragem e algoritmo decifragem.

Possui um processo similar ao Diffie-Hellman. Um grande exemplo de utilização do El Gamal é no PGP (Pretty Good Privacy).

É importante destacar que o El Gamal possui algumas características de algoritmos de criptografia simétrica.

One-Time Pad – OTP

É uma técnica de criptografia que, se utilizada da forma correta, é considerada inquebrável, ou incondicionalmente seguro.

Utiliza a combinação caractere por caractere com uma chave secreta aleatória, que deve ter, necessariamente, o mesmo tamanho da mensagem em claro. Esse é limitador de implementação do OTP. A chave deverá ser usada uma única vez e destruída após o uso.

Aproveito ainda para diferenciar o termo incondicionalmente seguro, conforme já vimos, de computacionalmente seguro. Este último está relacionado ao fato de que o custo de quebrar a cifra é superior ao valor da informação codificada ou que o tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação.

CESPE / CEBRASPE – 2021 – PG-DF – Analista Jurídico – Analista de Sistema – Suporte e Infraestrutura

Considerando-se os algoritmos de criptografia tradicionais (RSA, por exemplo), tem-se a garantia que é impossível determinar a chave privada a partir do conhecimento da chave pública.

Comentário:

Muito cuidado pessoal. Essa questão de ser incondicionalmente seguro não existe, conforme comentamos. Na prática, temos os conceitos de computacionalmente seguro. Vejam o que o CESPE colocou de justificativa para esse item, uma vez que ele teve seu gabarito alterado, ficando em ERRADO.

"Os algoritmos não garantem que seja impossível, a garantia é que seja computacionalmente inviável que um invasor determine a chave privada caso conheça a chave pública. Uma forma de ataque aos sistemas de chave pública é, portanto, tentar calcular a chave privada, dada a chave pública. A tentativa faz sentido, pois a história da criptoanálise mostra que um problema que parece insolúvel de um ponto de vista pode ter uma solução se for visto de uma maneira inteiramente diferente."

Gabarito: Errado

FUNÇÕES HASH

As funções HASH **são algoritmos criptográficos unidirecionais**. Utiliza-se funções matemáticas que permitem **gerar um resultado de tamanho fixo independentemente do tamanho do conteúdo de entrada**.

Desse modo, por ser unidirecional, isso quer dizer que, a partir de um resultado, não há algoritmos ou chave que retorne à mensagem original.

Para se ter uma ideia, podemos aplicar um algoritmo HASH (MD5) a uma sequência como "123456" e teremos como resultado o texto "e10adc3949ba59abbe56e057f20f883e". Mesmo que alguém tenha acesso ao último conteúdo, não há como saber que foi a mensagem "123456" que gerou tal resultado.

Mas então como poderíamos, por exemplo, tentar descobrir a mensagem original? Bom, como a função utilizada pelo algoritmo é conhecida, poderíamos pegar uma sequência de diversos valores e aplicar o algoritmo com vistas a identificar um resultado igual. Um exemplo seria a análise a partir da tabela abaixo:

Original	MD5	Valor procurado	Igual ?
123450	149787a6b7986f31b3dcc0e4e857cd2a	e10adc3949ba59abbe56e057f20f883e	Não
123451	078563f337ec6d6fedf131ddc857db19	e10adc3949ba59abbe56e057f20f883e	Não
123452	7692dcdc19e41e66c6ae2de54a696b25	e10adc3949ba59abbe56e057f20f883e	Não
123453	0f3e84acb19dff22f695f31dbe3e972a	e10adc3949ba59abbe56e057f20f883e	Não
123454	268e27056a3e52cf3755d193cbeb0594	e10adc3949ba59abbe56e057f20f883e	Não
123455	00c66aaf5f2c3f49946f15c1ad2ea0d3	e10adc3949ba59abbe56e057f20f883e	Não
123456	e10adc3949ba59abbe56e057f20f883e	e10adc3949ba59abbe56e057f20f883e	SIM

A referida técnica é conhecida como ataque de força bruta em funções HASH. Assim, busca-se montar um banco de dados grande e variado o suficiente que permita consultas posteriores em busca de igualdade de resultados.

Essas funções também são conhecidas como Funções HASH ONE-WAY. *Mas André, se eu não consigo saber o valor original, para que serve o HASH?*

Pessoal, as principais aplicações das funções HASH são para garantir os princípios de integridade, autenticidade e confidencialidade. Vamos citar alguns exemplos.

EXEMPLIFICANDO

Para fins de confidencialidade e autenticidade, podemos citar o logins com a utilização de senhas que fazemos em sites. Os servidores de dados que armazenam as informações de LOGIN e SENHAS não armazenam os dados diretamente. Eles armazenam o resultado do HASH das senhas. Isto é, vamos supor que eu tenha uma senha do tipo “senhapadrão”.

O valor HASH MD5 desse texto é “aa52af9c01caa48a0d2958c961112b5b”. Assim, o valor que o servidor armazenará é o HASH. Na próxima vez que eu fizer o login, digitarei meu nome de usuário e senha normalmente. Porém, para verificar se minha senha é válida, o servidor calculará novamente o HASH da senha digitada e comparará com o valor HASH armazenado. Como o algoritmo é padrão, logo, teremos sempre o mesmo valor HASH para a mesma entrada.

A confidencialidade pode ser garantida nesse caso na hipótese de violação da base de dados do servidor. Assim, caso as mensagens em claro fossem armazenadas, o atacante teria obtido facilmente todas essas informações. Mas, como o que está armazenado é somente o valor do HASH, isso dificultará o processo de obtenção das senhas por parte do atacante.

Para fins de integridade, temos uma mensagem que deve ser enviada a um destinatário. Desse modo, envia-se a mensagem e o resultado do HASH da referida mensagem. Quando o destinatário receber essas duas informações, ele pegará o texto em claro e fará o cálculo da função HASH dessa mensagem e comparará com a outra mensagem recebida. Caso sejam idênticas, quer dizer que, de fato, não houve alteração na

mensagem recebida. Caso seja diferente, assume-se que houve uma violação à integridade dos dados. Esse modelo é muito utilizado na assinatura digital e certificado digital.

Outras características que surgem nas funções de HASH é que estas devem apresentar **modelos matemáticos e cálculos simples que exijam pouco processamento das informações**. Além disso, **o conceito de difusão diz que deve ser impossível modificar a mensagem original sem modificar o resultado do HASH desta mensagem**.

O **resultado de um cálculo de uma função HASH também é bastante referenciada como "message digest"**.

CESPE / CEBRASPE – 2021 – SERPRO – Analista – Especialização: Desenvolvimento de Sistemas

Dados sobre os quais tenha sido calculado um valor de hash criptográfico com determinado algoritmo têm garantia de sua integridade sempre que, em qualquer tempo, um novo cálculo de hash desses dados com emprego do mesmo algoritmo resultar idêntico ao valor inicialmente calculado.

Comentário:

Essa é a ideia por trás do HASH pessoal, bastante associado ao princípio da integridade, com sua perenidade no regime de cálculo do HASH a partir de uma mesma entrada de informação.

Gabarito: Certo

Ataques de Colisão

Uma das formas de se promover ataques em algoritmos HASH é através da obtenção de valores de entrada distintos que produzem o mesmo resultado de saída. Por ter um tamanho fixo, obviamente haverá casos em que isso ocorrerá. Uma maneira de se amenizar esse problema é através do aumento do tamanho em bits das *messages digests*.

Ataque de Aniversário

Um outro tipo de ataque baseado em probabilidade, vinculando ao paradoxo do aniversário. Assumindo que eu tenha uma mensagem original "TESTE". Para se entender esse ataque, fica muito claro quando estamos em sala de aula. A ideia é simples. O professor pergunta, existe algum aluno que faça aniversário na mesma data que eu, que é, por exemplo, 30 de julho? Teremos uma probabilidade de que isso ocorra.

Agora a pergunta é diferente. Existe dois de vocês, quaisquer que sejam, que fazem aniversário no mesmo dia? **Um cálculo matemático simples mostra que a probabilidade de ocorrência do primeiro caso, para uma sala de 30 alunos é de 7,9%, enquanto, no segundo, é de 70%.**

Esse tipo de ataque possibilita a criação de um modelo que otimiza de forma considerável o ataque de colisão. Além disso, por causa desse ataque, o esforço computacional para quebra é considerado igual $2^{k/2}$ onde k representa o tamanho do digest.

Esses dois cenários representam a robustez de um algoritmo em termos de colisão. Assim, um algoritmo assegura a colisão simples caso seja computacionalmente impossível, conhecendo uma mensagem M, achar uma outra mensagem M' que produza o mesmo HASH. E o algoritmo será robusto à colisão forte caso seja computacionalmente difícil encontrar um par de mensagens (M,M') que produzam o mesmo HASH.

FGV – Auditor de Controle Externo – Tecnologia da Informação (TCE-TO)/2022

As funções de hash são comumente empregadas nos mecanismos de segurança da informação.

Quanto às suas propriedades básicas, para que o algoritmo de hash seja considerado forte, é correto afirmar que:

a) a mesma entrada deve produzir saídas diferentes;

b) deve ser difícil encontrar duas entradas que produzam o mesmo hash;

c) deve ser possível produzir a entrada original a partir do hash resultante;

d) pequenas mudanças na entrada devem produzir pequenas mudanças no hash resultante;

e) mesmo que as entradas possuam o mesmo tamanho, os resultados de hash terão tamanhos diferentes..

Comentários:

Vimos que uma das principais características das funções HASH é justamente que cada entrada gere uma saída diferente. Entretanto, isso nem sempre é possível devido ao espaço amostral e a fixação da quantidade de bits de saída recepcionando quaisquer quantidades de bits de entrada. Assim, em algum momento, teremos problemas de colisão, onde entradas diferentes produzem resultados iguais. E é nesse ponto onde vemos a robustez da função HASH.

Logo, temos como gabarito a alternativa B.

Vamos aos outros itens:

a) A mesma entrada deve sempre produzir a mesma saída. Esse é um princípio básico. INCORRETO

c) A função HASH é de via única, de tal modo que não é possível voltar à mensagem orginal a partir da saída produzida por ela. INCORRETO

d) Não há uma relação de mudança "pequena" ou "grande". Naturalmente, mudanças na entrada devem produzir mudanças na saída. INCORRETO

e) Ao contrátio pessoal. Mesmo que a entrada varie de tamanho, a saída sempre terá tamanho fixo. INCORRETO

Gabarito: B

TJ-RO Prova: FGV – 2021 – TJ-RO – Analista Judiciário – Analista de Sistema – Desenvolvimento de Sistema

Na implementação de tabelas Hash, quando as chaves não são perfeitamente distribuídas, é preciso lidar com as potenciais colisões que ocorrem quando:

a) o espaço de endereçamento é superior ao número de chaves armazenadas;

b) duas ou mais chaves têm o mesmo índice na tabela;

c) as chaves são exclusivamente numéricas;

d) as chaves são exclusivamente alfanuméricas;

e) há duplicação de chaves.

Comentários:

Pessoal, conforme vimos, o tamanho HASH de saída é único, independentemente do tamanho da mensagem de entrada. Por esse motivo, é natural que haja dois ou mais resultados iguais, a partir de diferentes entradas. Trata-se de uma questão de espaço amostral. Caso o tamanho das mensagens de entrada não tenha o máximo do tamanho sendo equivalente à saída, sempre teremos algum tipo de duplicação.

Stallings, em uma visão matemática, nos traz o seguinte: "Para um valor de hash h = H(x), dizemos que x é a pré-imagem de h."

Assim, justamente, a partir de $x \neq y$ e $H(x) = H(y)$, teremos uma colisão.

Gabarito: B

VUNESP – 2019 – Câmara de Piracicaba – SP – Administrador de RedeUm sistema utiliza como hash criptográfico a soma do valor numérico de cada caractere da mensagem. O algoritmo de hash é frágil, pois

A não é possível determinar uma função inversa.

B produz o efeito avalanche.

C possui baixa resistência a colisões.

D o código hash gerado é único

E demanda um elevado poder computacional para ser calculado.

Comentários:

A ideia por trás dessa questão é fazer com que vocês percebam que, caso seja utilizado a técnica de soma dos caracteres, você pode ter diferentes entradas produzindo o mesmo HASH, uma vez que há diferentes palavras que possuem a mesma composição de caracteres.

Então, claramente, tem-se uma questão de aumento de probabilidade de colisão, e consequentemente, podemos dizer que esse algoritmo possui baixa resistência a colisões.

Gabarito: B

As bancas têm cobrado ainda as características dos diversos algoritmos de HASH. Portanto, vamos falar um pouco sobre cada um deles.

MD5

Foi criado para substituir o algoritmo MD4. **Esse algoritmo produz um tamanho de HASH de 128 bits.** Em 2008 já foram identificadas algumas colisões nesse algoritmo, passando a ser considerado algumas fragilidades. Já em 2013, por exemplo, a MICROSOFT lançou uma atualização que desabilita a aplicação do MD5 às suas autoridades certificadoras.

Possui um tamanho de entrada de múltiplos de 128 bits.

Um dos problemas que existe no MD5 está relacionado à colisão de prefixos de uma mensagem, gerando uma probabilidade alta de se compor sufixos que também produzam colisões.

SALT

Esse é um recurso que surgiu para amenizar o problema de prefixo. A ideia aqui é sempre acrescentar um valor fixo padrão a ser definido pelo sistema ou servidor para compor a mensagem original.

Assim, se a mensagem original for “123456”, determinada empresa acrescentaria um nome fixo, por exemplo, “nomedaempresa” antes de cada mensagem antes de calcular o HASH, gerando-se uma pseudo-mensagem “estrategia123456”.

Esse recurso é utilizado pelos sistemas LINUX.

MD4

O MD4 produz HASH de tamanho de 128 bits, dependendo de entradas de tamanho múltiplos de 512 bits. Caso a entrada não tenha esse tamanho, acrescenta-se um bit adicional de valor “1” e sucessivos “0’s” até completar o múltiplo.

SHA

O algoritmo SHA possui diversas versões de implementação que produzem resultados distintos. Foi criado pela agência de segurança do governo norte-americano – NSA.

Atualmente, temos os algoritmos abaixo e seus respectivos tamanhos de HASH:

SHA1 – 160 bits de HASH;

SHA-224 – 224 bits de HASH. É uma versão truncada do SHA-256;

SHA-256 – 256 bits de HASH, com palavras de entrada de 256 bits;

SHA-384 – 384 bits de HASH. É uma versão truncada do SHA-512;

SHA-512 – 512 bits de HASH, com palavras de entrada de 512 bits;

Divide-se ainda as versões do SHA em 1, 2 e 3. Atualmente, devido à sua robustez, utiliza-se o SHA3 nas mesmas proporções da análise acima.

CESPE / CEBRASPE – 2021 – PG-DF – Analista Jurídico – Analista de Sistema – Suporte e Infraestrutura

O resultado e o tamanho do método criptográfico hash variam de acordo com o tamanho da informação à qual ele seja aplicado.

Comentários:

Jamais pessoal. Conforme nós vimos, o HASH de saída, ou seja, a mensagem resumida é sempre fixa, de acordo com a função estabelecida.

Gabarito: E

CESPE / CEBRASPE – 2020 – Ministério da Economia – Tecnologia da Informação

A função hash, utilizada para garantir integridade e autenticidade dos dados, gera, a partir de uma entrada de qualquer tamanho, uma saída de tamanho fixo; caso dois arquivos tenham o mesmo conteúdo, mas nomes diferentes, os valores do hash MD5 serão diferentes.

Comentários:

Pessoal, o nome do arquivo em nada influencia aqui. O HASH é sempre aplicado sobre o arquivo, ou seja, sobre o conteúdo. Então, não basta o nome ser diferente, o conteúdo que precisa ser diferente para gerar a variação da saída da função HASH.

Gabarito: E

CESPE – TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013

A função de *hashing*, por apresentar utilidade criptográfica, caracteriza-se por bidirecionalidade, compressão, tamanho variável, facilidade de cálculo, difusão, colisão simples e colisão forte.

Comentários:

Houve a inversão de duas características das funções HASH na assertiva. A primeira é o caráter de unidirecionalidade (e não bidirecionalidade), e o segundo de tamanho fixo (e não tamanho variável).

Gabarito: E

QUESTÕES COMENTADAS

1. **(CESPE – SE-DF/Analista de Redes/2017) No contexto de uma infraestrutura de chaves públicas, um documento eletrônico assinado digitalmente com a chave pública do remetente falhará na verificação de integridade e autoria pelo destinatário, caso essa verificação seja realizada com a aplicação da mesma chave pública do remetente.**

Comentários:

Duas observações aqui pessoal. Primeiramente em relação ao conceito de chaves públicas. Esses algoritmos trabalham com um par de chaves, ou seja, um é utilizado para cifrar e o outro para decifrar. Lembrando que podem ser usados da forma inversa também. Essas chaves são conhecidas como públicas e privadas. Logo, de fato, não será possível decifrar a mensagem do cenário apresentado no enunciado. O segundo ponto a ser mencionado é que para tratar aspectos de autenticidade e integridade, princípios garantidos pela assinatura digital, deve-se usar para o processo de cifragem a chave privada do remetente e não a chave pública. Então realmente não será possível aferir a integridade dos dados.

Gabarito: C

---

2. **(CESPE – TCE-PR/Analista de Controle – Área TI/2016) Assinale a opção correta, no que concerne a conceitos básicos de criptografia e criptografia simétrica e assimétrica.**

a) A principal diferença entre os algoritmos de criptografia simétrica e os algoritmos de criptografia assimétrica consiste no fato de que os primeiros são fundamentados em técnicas de transposição e os segundos em técnicas de substituição.

b) Um esquema de criptografia será considerado computacionalmente seguro se o tempo para se quebrar sua cifra for superior ao tempo de vida útil da informação por ele protegida.

c) Em uma transmissão de dados em que se use criptografia simétrica, as chaves de criptografia e decriptografia têm de ser distintas, embora tenham de ter o mesmo tamanho.

d) O valor da chave de criptografia depende do texto claro a ser criptografado e do algoritmo a ser usado para criptografar esse texto.

e) Em um ataque por força bruta, exploram-se a natureza e as características do algoritmo na tentativa de deduzir as chaves

Comentários:

Tivemos uma inversão dos conceitos na alternativa "A". Já para a "B", temos exatamente o que se aplica no contexto de Segurança. Se a informação não faz mais sentido, ou seja, se ela não tem mais valor, não há problemas em ela ser violada. Nesse sentido, precisamos garantir que o sistema não seja quebrado enquanto a informação produz algum valor, ou seja, dentro do seu período de vida útil.

Já para a letra "C", temos que a chave deve ser a mesma, certo? Para a "D", não temos relação com o texto em claro em termos da definição da chave.

Por fim, na letra "E", temos a descrição do ataque de criptoanálise e não de força bruta. Este é baseado simplesmente na tentativa e erro.

Gabarito: B

(CESPE – TCE-PR/Analista de Controle – Área TI/2016) Em um esquema de criptografia de chaves públicas, caso um sistema participante opte por alterar sua chave privada, para que seja mantida a comunicação, será necessário

a) gerar uma nova chave privada a partir da chave pública existente e substituir a chave pública pela nova chave.

b) gerar uma nova chave privada e publicar essa nova chave privada.

c) gerar um novo par de chaves e publicar as duas novas chaves — pública e privada.

d) gerar um novo par de chaves e publicar a nova chave pública.

e) gerar um novo par de chaves, substituir a chave privada e, consequentemente, descartar a nova chave pública gerada.

Comentários:

Os algoritmos de criptografia de chaves públicas são baseados em fórmulas matemáticas que, a partir de determinados valores de entrada, geram um par de chaves como resultado (chave privada e pública). Essas chaves só fazem sentido juntas... Não há como combinar com outras chaves privadas e públicas de outros algoritmos. Desse modo, para se alterar a chave privada, deve-se gerar um novo par de chaves, procedimento este descrito na alternativa "D". Lembrando que das duas chaves, como o próprio nome diz, deve-se dar publicidade à chave pública.

Gabarito: D

---

3. **(CESPE – TCE-PR/Analista de Controle – Área TI/2016) Acerca da criptografia, assinale a opção correta.**

a) O algoritmo DES utilizado para chaves simétricas é imune a ataques do tipo meet-in-the-middle (encontro no meio).

b) Em um esquema de criptografia simétrica, a chave secreta, além de ser a saída para o algoritmo de criptografia, é também a chave para decriptografar e depende do texto claro e do algoritmo.

c) O algoritmo Diffie-Hellman é utilizado para criptografia com chave pública e pode ser utilizado tanto para assinatura digital quanto para decriptografia.

d) O algoritmo RSA é imune a ataques matemáticos, mas suscetível a ataques do tipo força bruta.

e) O algoritmo RSA permite que o emissor criptografe uma mensagem com a chave pública do destinatário ou, ainda, que assine uma mensagem com sua chave privada.

Comentários:

Como sabemos, o RSA é um algoritmo de chave pública. Isso implica dizer que este algoritmo pode ser utilizado para garantir dois princípios distintos a depender da sequência de utilização das chaves:

Se criptografar com a chave privada do emissor, garante-se a autenticidade.

Se criptografar com a chave pública do receptor, garante-se a confidencialidade.

Esse cenário está representado na alternativa "E".

Algumas observações é que o RSA não é imune a ataques matemáticos. Já o algoritmo DH é utilizado para troca de chaves.

Gabarito: C

---

4. CESPE – TCE-SC/AFCE – Área TI/2016

Os algoritmos de criptografia de chave pública devem ser computacionalmente fáceis, a fim de que o receptor de uma mensagem cifrada com uma chave pública a decriptografe utilizando sua chave privada para recuperar a mensagem original.

Comentários:

Pessoal, no primeiro momento que li essa alternativa, fiz a interpretação a seguir: "Dizer que o algoritmo de criptografia de chave pública deve ser computacionalmente fácil é um problema pessoal. O que deve ser computacionalmente fácil é a geração do par de chaves, o que é bem diferente. A robustez do algoritmo está na dificuldade de se achar ou definir a chave privada a partir da chave pública e vice-versa. Inclusive, há uma grande complexidade do algoritmo RSA, que é assimétrico. "

Entretanto, com uma leitura mais cautelosa, perceba o detalhe da abordagem. A facilidade computacional do algoritmo está atrelado ao processo adequado de descriptografia, ou seja, uma vez que eu insiro a chave correta, ele facilmente realiza o processo. Isso é uma verdade.

Gabarito: C

5. **(CESPE - –J STF/Apoio Especializado/Tecnologia da Informação/2013) A criptologia incorpora estudos e conhecimentos das áreas de criptografia e criptoanálise.**

Comentários:

Vimos exatamente isso, não é pessoal? Criptologia é a ciência que agrega a criptografia e criptoanálise.

Gabarito: C

---

6. **(CESPE - –J TRT10/Apoio Especializado/Tecnologia da Informação/2013) Na criptografia de chave pública assimétrica, são utilizadas duas chaves diferentes: uma chave privada confidencial, para criptografar os dados, e outra chave pública, para decriptografar os dados, a qual é distribuída para os destinatários.**

Comentários:

Pessoal, comentei lá na nossa teoria a respeito do fato de que não podemos restringir a criptografia assimétrica no quesito de que a privada necessariamente será utilizada para criptografar e a pública para decriptografar. Como vimos, depende do propósito da aplicação.

Gabarito: E

---

7. **(CESPE - –CF/Área 2/2013) A compressão de dados antes da encriptação geralmente aumenta a segurança do sistema, por reduzir a redundância na mensagem, dificultando a criptoanálise.**

Comentários:

Exatamente como vimos na teoria. Lembrando que tal processo também possibilita ganhos de desempenho.

Gabarito: C

---

8. **(CESPE - –CF/Área 2/2013) Esquemas de criptografia de chave pública também são conhecidos como de criptografia simétrica, pois possuem apenas uma chave, tanto para encriptação quanto para desencriptação.**

Comentários:

Questão bem tranquila, certo pessoal? Criptografia de chave pública está relacionada ao processo de criptografia assimétrica que utiliza duas chaves distintas no processo.

Uma observação é em relação à variação de nomenclatura para o processo de decriptação. Nesse caso, tivemos a desencriptação. Em outros, teremos a descriptação. Não se espantem.

Gabarito: E

---

9. **(CESPE - –CF/Área 3/2013) Um aplicativo que utiliza recursos biométricos para a criptografia de arquivos, como a impressão digital de um indivíduo tanto para encriptar quanto decriptar, assemelha-se a um sistema criptográfico simétrico.**

Comentários:

Mais uma questão tranquila e bem conceitual. Como vimos, de fato, a criptografia simétrica utiliza uma mesma chave para criptografar e descriptografar. Nesse caso, a chave utilizada é a impressão digital do usuário.

Gabarito: C

---

10. **(CESPE - –CF/Área 3/2013) Modos de operação de cifra de bloco permitem cifrar mensagens de tamanhos arbitrários com a utilização de algoritmos de cifragem de blocos, que trabalham com blocos de tamanho fixo. Os modos de operação existentes asseguram a confidencialidade e a integridade da mensagem cifrada, embora nem todos possam ser utilizados para autenticação.**

Comentários:

Comentamos na teoria que a técnica de cifragem por bloco não pode ser generalizada no sentido de garantir os princípios de segurança.

Gabarito: E

---

11. **(CESPE - –CF/Área 3/2013) A confidencialidade e a integridade de uma comunicação são garantidas com o uso de criptografia tanto simétrica quanto assimétrica. No entanto, para garantir autenticidade e irretratabilidade, é necessário o uso combinado desses dois tipos de criptografia**

Comentários:

A criptografia simétrica visa garantir tão somente o princípio da confidencialidade.

Gabarito: E

---

12. (CESPE - –A (TCE-ES)/Informática/2013) Criptografia é uma técnica matemática capaz de transformar uma informação da sua forma original para outra forma totalmente ilegível, a partir da qual um processo inverso pode voltar a recuperar a informação para seu formato original. Acerca dessas informações, assinale a opção correta.

a) A técnica criptográfica garante os atributos de autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação.

b) Os algoritmos de chaves simétricas e assimétricas são as categorias básicas de algoritmos criptográficos, sendo os de chaves assimétricas a base conceitual da certificação digital.

c) Os algoritmos RSA e as curvas elípticas são exemplos de algoritmos criptográficos com base em chaves simétricas.

d) Os algoritmos DES e AES são exemplos de algoritmos criptográficos com base em chaves assimétricas.

e) Quando criptografada, a informação passa a ter a garantia de nível máximo de proteção.

Comentários:

Vamos aos itens:

A criptografia surgiu com o intuito de garantir a confidencialidade apenas. **INCORRETO**
Exatamente como vimos na nossa teoria. **CORRETO**
RSA é algoritmo assimétrico. Além disso, utiliza como base de modelo matemático o cálculo de números primos extremamente grandes. **INCORRETO**
Ambos são algoritmos de criptografia simétrica. **INCORRETO**
Dizer que a informação tem nível máximo é um pouco demais, certo? **INCORRETO**

Gabarito: B

---

13. (CESPE - –na Info (TCE-RO)/2013) Na criptografia simétrica, são geradas duas chaves criptográficas, uma privada e outra pública, para que um arquivo seja transferido, entre dois computadores, de forma criptografada.

Comentários:

Não né pessoal? Isso seria a criptografia assimétrica.

Gabarito: E

---

14. (CESPE - –J (STF)/Apoio Especializado/Análise de Sistemas de Informação /2013) Criptografia de chave simétrica, que também é conhecida como criptografia de chave pública, utiliza chaves distintas para codificar e decodificar as informações. Uma dessas chaves é pública e a outra é do gerador da criptografia.

Comentários:

Mais uma vez, a mistura de conceitos. Percebam quão recorrente isso é.

Gabarito: E

---

15. (CESPE - –na Sist (SUFRAMA)/2014) Para averiguar a integridade de um arquivo de computador a ser transmitido por um meio inseguro, pode-se gerar um hash antes da transmissão e verificar o hash após a transmissão.

Comentários:

Pessoal, vimos exatamente esse exemplo como um dos benefícios a serem extraídos da utilização das funções HASH, certo? De fato, a integridade pode ser garantida conforme descrição da assertiva.

Gabarito: C

---

16. (CESPE - –J TRT17/Apoio Especializado/Tecnologia da Informação/2013) Para evitar o acesso de terceiros não confiáveis aos dados, pode-se utilizar a criptografia simétrica, técnica que confere confidencialidade às informações.

Comentários:

Lembrando que também poderia ser utilizado a criptografia assimétrica sem problema algum.

Gabarito: C

---

17. (CESPE - –J TRT17/Apoio Especializado/Tecnologia da Informação/2013) A função de hashing, por apresentar utilidade criptográfica, caracteriza-se por bidirecionalidade, compressão, tamanho variável, facilidade de cálculo, difusão, colisão simples e colisão forte.

Comentários:

Houve a inversão de duas características das funções HASH na assertiva. A primeira é o caráter de unidirecionalidade (e não bidirecionalidade), e o segundo de tamanho fixo (e não tamanho variável).

Gabarito: E

---

18. (CESPE - –ud Gov (CGE PI)/Tecnologia da Informação/2015) Se, em um esquema de criptografia de chave pública, o emissor E criptografar uma mensagem M utilizando a chave pública do receptor R, então, nesse esquema, é oferecida confidencialidade, mas não autenticação.

Comentários:

Exatamente isso pessoal. Se usou-se a chave pública do receptor, a única chave possível que poderá descriptografar essa mensagem é a chave privada do recepto, que é de conhecimento único deste.

Gabarito: C

---

19. (CESPE - –CF/Área 3/2013) AES é uma cifra de bloco, enquanto o RC4 é uma cifra de fluxo. Apesar dessa diferença, ambos têm em comum a utilização de um tamanho de chave de 128, 192 ou 256 bits.

Comentários:

O primeiro trecho da assertiva está tudo certo. Entretanto, o segundo gerou ambiguidade. O AES, como vimos, suporta esses três tamanhos de chaves. Já o RC4, suporta esses três e muitos outros.

Desse modo, a banca apresentou a seguinte justificativa para anulação:

" O enunciado do item não deixa claro se são apenas os tamanhos de chave de 128, 192 e 256 bits que podem ser utilizados. Por esse motivo, o item deve ser anulado. "

Gabarito: ANULADA

---

20. (CESPE - –NTAQ/TI - –nalista de Infraestrutura/2014) Na criptografia simétrica, a mesma chave compartilhada entre emissor e receptor é utilizada tanto para cifrar quanto para decifrar um documento. Na criptografia assimétrica, utiliza-se um par de chaves distintas, sendo a chave

pública do receptor utilizada pelo emissor para cifrar o documento a ser enviado; posteriormente, o receptor utiliza sua chave privada para decifrar o documento.

Comentários:

Temos aqui uma questão problemática em relação a um tópico que já comentamos. Dizer que será necessariamente essa sequência na criptografia assimétrica é um erro, conforme inclusive já vimos gabarito de outra questão.

Gabarito: C (Gabarito do Professor: ERRADO)

---

21. **(CESPE - –na MPU/Tecnologia da Informação e Comunicação/Desenvolvimento de Sistemas/2013) Em uma troca de dados, via Internet, entre dois computadores que estejam utilizando um algoritmo de criptografia assimétrica, antes de trocarem os dados, os usuários deverão compartilhar entre eles a chave, já que ela deve ser a mesma para os dois usuários.**

Comentários:

Não né pessoal? Uma das vantagens do algoritmo de criptografia assimétrica é justamente não haver a necessidade de troca de chaves e a utilização de uma única chave.

Gabarito: E

---

22. **(CESPE -ANATEL/Analista - –uporte e Infraestrutura de Tecnologia da Informação/2014) Uma das propriedades de uma função de hash, conhecida como resistência à primeira inversão ou propriedade unidirecional, garante que, dada uma mensagem, não é possível encontrar uma mensagem alternativa que gere o mesmo valor de hash da mensagem original.**

Comentários:

Temos aqui a descrição da característica de difusão e não de unidirecionalidade. Esta última diz respeito a incapacidade de se voltar à mensagem original a partir do valor de HASH obtido.

Gabarito: E

---

23. **(CESPE - –NATEL/Analista - –uporte e Infraestrutura de Tecnologia da Informação/2014) Para que a criptografia de chave pública seja considerada segura, uma das premissas é que o conhecimento do algoritmo, o conhecimento de uma das chaves e a disponibilidade de amostras de texto cifrado sejam, em conjunto, insuficientes para determinar a outra chave.**

Comentários:

Questão bem bacana da ANATEL. De fato, os três pontos apresentados são características desses algoritmos. Há o conhecimento público da chave pública e do algoritmo utilizado. Além disso, caso o usuário intercepte a mensagem cifrada, isso, por si só, não permite que ele obtenha informações da chave privada.

Gabarito: C

---

24. (CESPE - –NATEL/Analista - –esenvolvimento de Sistemas de Informação/2014) Nos métodos mais seguros de criptografia, a função e a chave utilizadas na encriptação devem ser de conhecimento exclusivo do remetente da mensagem.

Comentários:

Ao contrário pessoal. Métodos de criptografia são considerados mais robustos quando seus algoritmos e funções são de conhecimento público. A chave, caso seja pública, também.

Gabarito: E

---

25. (CESPE - –ec MPU/Técnico Administrativo/Tecnologia da Informação e Comunicação/2013) Se um usuário cifra uma mensagem com a chave pública do destinatário e depois cifra novamente com sua própria chave privada, apenas o destinatário será capaz de recuperar a mensagem em claro.

Comentários:

Pessoal, tivemos dois processos de cifragem.

Utilizou-se a chave pública do destinatário e;
Em seguida, a chave privada do emissor.

Para revertermos o processo, devemos desfazer na sequência correta.

Assim, primeiro devemos decifrar a mensagem com a chave pública do emissor. Até então, qualquer um pode fazer esse procedimento pois a chave é pública.

Em seguida, deve-se utilizar a chave privada do destinatário e nesse caso, somente o destinatário tem conhecimento dessa chave. Logo, de fato, somente ele será capaz de recuperar a mensagem original.

Gabarito: C

26. (CESPE - –ec MPU/Técnico Administrativo/Tecnologia da Informação) Em sistemas de criptografia assimétrica existem duas chaves com funções complementares que devem ser mantidas em segredo.

Comentários:

Somente uma chave precisa ser mantida em segredo, que é a privada, certo pessoal?

Gabarito: E

---

27. (CESPE - –CF/Área 3/2013) SHA-1 e MD-5 são exemplos de hashes criptográficos largamente utilizados na Internet. O MD-5 tem sido substituído pelo SHA-1 pelo fato de este gerar um hash maior e ser o único à prova de colisões.

Comentários:

De fato, o HASH do SHA-1 (160 bits) é maior que o MD5 (128 bits). Entretanto, não podemos dizer que há alguma função de HASH à prova de colisões.

Gabarito: E

---

28. (CESPE - –CF/Área 3/2013) O SHA-1, comumente usado em protocolos de segurança, como TLS, SSH e IPSec, também é utilizado por alguns sistemas de controle de versão como Git e Mercurial para garantir a integridade das revisões.

Comentários:

Inevitavelmente, ao ser falar de funções de HASH, elas estarão vinculadas a diversos serviços agregando princípios de integridade e autenticidade. A assertiva nos apresenta alguns exemplos válidos de sua utilização.

O TLS1.0 e TLS1.1 usam SHA-1 em conjunto com MD5 para a produção de códigos de autenticação de mensagens (Message authentication Code – MAC). Na versão 1.2, passou-se a utilizar o SHA-256. O IPSeC segue o mesmo modelo do TLS1.0.

O Git é um sistema de repositório para desenvolvimento de sistemas e aplicações que utiliza o SHA-1 para indexar os arquivos e códigos gerados e armazenados em seu repositório. Desse modo, é capaz de tratar aspectos de integridade do arquivo nos procedimentos de download e upload.

E por último, temos o Mercurial, que também é um sistema de repositório que utiliza SHA-1 para tratar a integridade dos dados, porém, de uma maneira diferente. Para cada arquivo armazenado no sistema, cria-

se um registro, denominado REVLOG. Isso permite tratar as revisões de cada arquivo e o SHA-1 é capaz de tratar a integridade de cada revisão.

Gabarito: C

---

29. (CESPE - –na Info (TCE-RO)/2013) O hash poderá auxiliar na verificação da integridade de um arquivo transferido de um computador para outro.

Comentários:

Reforçando o que já vimos.

Gabarito: C

---

30. (CESPE - –J STF/Apoio Especializado/Tecnologia da Informação/2013) Os algoritmos de criptografia simétricos apresentam menor desempenho que os algoritmos assimétricos.

Comentários:

Exatamente ao contrário pessoal. Para começar, basta lembrar dos tamanhos das chaves.

Gabarito: E

---

31. (CESPE - –J STF/Apoio Especializado/Tecnologia da Informação/2013) No RSA (Rivest-Shamir-Adleman), o texto claro é criptografado em blocos com valor binário limitado.

Comentários:

Vimos na nossa teoria que o tamanho dos blocos é limitado.

Gabarito: C

---

32. (CESPE - –J (STF)/Apoio Especializado/Análise de Sistemas de Informação /2013) O algoritmo de criptografia MD5 (Message-Digest Algorithm 5) é um método que transforma uma palavra em um código criptografado único, ou seja, não é possível que duas strings diferentes produzam o mesmo hash.

Comentários:

Afirmar categoricamente que não é possível é uma inverdade.

Gabarito: E

---

33. **(CESPE - –J (STF)/Apoio Especializado/Suporte em Tecnologia da Informação/2013) O algoritmo RSA gera chaves públicas de tamanho fixo e limitado a 2.048 bits.**

Comentários:

Além de não ser fixa, também não é limitada a 2048 bits.

Gabarito: E

---

34. **(CESPE - –A (ANATEL)/Desenvolvimento de Sistemas de Informação/2014) O texto cifrado F é obtido a partir do texto aberto C, utilizando-se o método monoalfabético de criptografia com chave igual a 3.**

Comentários:

Temos aqui a descrição técnica da cifra de César.

Gabarito: C

---

35. **(CESPE - –A (ANATEL)/Suporte e Infraestrutura de Tecnologia da Informação/2014) O algoritmo de criptografia AES (advanced encryption standard) opera em quatro estágios: um de permutação e três de substituição. O estágio de permutação ShiftRows é reversível e os estágios de substituição SubBytes, MixColumns e AddRoundKey são não-reversíveis.**

Comentários:

Com certeza você deve estar se perguntando: cobraram isso mesmo? Bom pessoal, aparentemente sim. Porém, há um detalhe que torna a questão simples.

O AES é um algoritmo de criptografia que utiliza a decriptação para retornar à mensagem anterior. Para isso, ele basicamente usa o processo inversos da encriptação. Assim, não há o que se falar de estágios irreversíveis.

Gabarito: E

36. (CESPE - –UFC/Controle Externo/Auditoria de Tecnologia da Informação/2015) No algoritmo AES, a cifra de decriptografia é idêntica à cifra de criptografia, assim como a sequência de transformações para a decriptografia é a mesma para a criptografia, o que pode ser considerado uma vantagem, já que apenas um único módulo de software ou firmware é necessário para aplicações que exigem tanto criptografia quanto decriptografia.

Comentários:

Pessoal, dizer que essa característica é uma vantagem é um problema quando tratado de forma generalizada. Na prática, pode ser vantajoso no aspecto de custo operacional, tempo de processamento ou até investimento de recursos. Entretanto, sob a ótica da segurança, isso acaba se tornando uma vulnerabilidade.

Além disso, devemos observar a sequência mencionada na assertiva. Na prática, no processo de decriptação, utiliza-se a sequência e operações invertidas quando comparada com o processo de encriptação.

Gabarito: E

---

37. (CESPE – TRE/RS / Analista Judiciário/2015) Assinale a opção correta relativamente a criptografia.

a) O algoritmo de criptografia AES utiliza quatro estágios diferentes, dois de permutação e dois de substituição.

b) No modo de operação de cifra de bloco cipher block chaining, o texto claro é tratado em blocos — um bloco por vez — e cada bloco de texto claro é criptografado mediante o uso de uma mesma chave.

c) Um código gerado por uma função hash para um conjunto de dados pode garantir a sua integridade porque, ao ser calculado novamente sobre o mesmo conjunto de dados, a qualquer tempo, pode determinar, inequivocadamente, se esse conjunto foi alterado ou não.

d) Esquema de criptografia incondicionalmente seguro significa que o custo para quebrar a cifra é superior ao valor da informação codificada ou que o tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação.

e) A criptoanálise, técnica para ataque a um esquema de criptografia convencional, caracteriza-se pela experimentação de cada chave possível em um trecho do texto cifrado, até que se obtenha uma tradução inteligível para texto claro.

Comentários:

Vamos aos itens:

a) No AES de fato são 4 estágios. Entretanto, temos a seguinte distribuição: três estágios de substituição (Subbytes, MixColmns e AddRoundKey) e um de permutação (shiftRows). **INCORRETO**.

b) Temos aqui a descrição mais próxima do EBC (não depende que seja um bloco por vez, pode ser de forma paralela) e não do CBC como afirma a questão. No CBC, a chave não é a mesma, pois depende a cifragem do bloco anterior. **INCORRETO**

c) Exatamente! A mesma mensagem sempre gerará o mesmo HASH, considerando que a mesma função seja gerada. **CORRETO**

d) O conceito de incondicionalmente seguro está relacionado ao fato de ser inquebrável, como o One-Time-Pad. O conceito de tempo e custo está relacionado ao termo computacionalmente seguro. **INCORRETO**

e) A criptoanálise é a ciência de quebrar códigos e decifrar mensagens. Então o simples fato de você buscar quebrar o código e não somente interpretar a informação já é uma forma de ataque. **INCORRETO**

Gabarito: C

---

38. (CESPE – TRE/RS / Técnico Judiciário/2015) A propósito de criptografia, assinale a opção correta.

a) Há, no envio de email com o hash, garantia de autenticidade, pois ele criptografa a mensagem enviada.

b) Na criptografia de chave pública, ou assimétrica, a chave utilizada para encriptar mensagens é distribuída livremente, ao passo que a chave privada decripta a mensagem.

c) São utilizadas, na criptografia simétrica, duas chaves: uma para encriptar e outra para decriptar.

d) O AES é um algoritmo de criptografia simétrica que usa chaves de 168 bites.

e) A criptografia, simétrica além de garantir a integridade dos dados, atende plenamente aos demais princípios de segurança como a integridade e a autenticidade, por exemplo.

Comentários:

Temos aqui uma questão problemática da qual eu discordo do gabarito e entendo que deveria ter sido anulada. Vamos aos itens:

a) O Hash puramente é utilizado para fins de integridade. **INCORRETO**.

b) Depende do modelo de utilização. Pode-se utilizar tanto a chave privada quanto a pública para encriptação, sempre utilizando a chave oposta para decriptação. Desse modo, caso se busque autenticidade, será usada a chave privada na encriptação e, esta, não deve ser distribuída. Por esse motivo, entendo que o item esteja incompleto. Ele estaria correto se informasse que o modelo utilizado teria como propósito a confidencialidade, e, nesse caso, vale o que está descrito no item. **INCORRETO**

c) Na criptografia simétrica, utiliza-se uma única chave. **INCORRETO**

d) O AES suporta chaves de 128, 192 ou 256 bits. **INCORRETO**

e) A criptografia simétrica por si só garantirá apenas a confidencialidade. **INCORRETO**

Gabarito: B (Gabarito do Professor: Anulação)

---

39. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) O protocolo 3DES possui três chaves criptográficas: a primeira e a segunda criptografam informações; a terceira é usada para descriptografar aquelas.

Comentários:

Uma bagunça, certo pessoal? Primeiro, que o 3DES não necessariamente utiliza 3 chaves, uma vez que podem ser utilizadas apenas duas chaves. Além disso, as mesmas chaves utilizadas no processo de cifragem serão utilizadas no processo de reversão, ou seja, de decifragem.

Gabarito: E

---

40. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

Comentários:

Diferentemente da questão anterior que afirma a necessidade de se utilizar três chaves, aqui apenas cogita-se a possibilidade, não havendo problema nisso. Além disso, o IPSeC suporta os principais protocolos de criptografia atualmente existentes, entre eles o 3DES.

Gabarito: C

---

41. (CESPE – FUNPRESP/ Área 8/2016) Na criptografia assimétrica, a chave pública deve apresentar tamanho variado, e a chave privada, tamanho fixo com, no mínimo, 512 bites

Comentários:

Pessoal, a variação ocorre em ambas. Temos como exemplo o algoritmo RSA, que pode trabalhar com chaves de 1024,2048 ou 4096 bits.

Gabarito: E

---

42. (CESPE – FUNPRESP/ Área 8/2016) Na criptografia simétrica com uso do modo de cifra em bloco (CBC), cada bloco cifrado pode utilizar a mesma chave.

Comentários:

O CBC é o modelo mais intermediário de cifragem de bloco. A ideia do CBC é utilizar um vetor de inicialização - –I em uma operação com o primeiro bloco e, em seguida, usar o bloco cifrado para realimentar a entrada do segundo bloco. Ou seja, realiza-se uma operação entre o primeiro bloco cifrado com o segundo bloco em claro, para posterior aplicação da chave e assim sucessivamente.

Entretanto, percebemos que a mudança é tão somente na composição da entrada para cifragem, não gerando nenhuma alteração na chave por padrão. Alguns algoritmos implementam recurso de segurança para gerar chaves diferentes. Como a questão simplesmente quis avaliar a possibilidade de se utilizar a mesma chave, não temos problema em marcar CORRETO.

Gabarito: C

HORA DE PRATICAR!

QUESTÕES COMENTADAS COMPLEMENTARES

1. **FGV 2022 TRT - 6ª REGIÃO (MA) - Analista Judiciário - Tecnologia da Informação**

Os sistemas de chave pública são caracterizados pelo uso de um algoritmo criptográfico com duas chaves, uma privada e uma pública. Com relação às categorias de uso dos criptossistemas de chave pública, analise as afirmativas a seguir:

I. Criptografia/descriptografia: um emissor criptografa uma mensagem com a chave pública do seu destinatário.

II. Assinatura digital: um emissor assina uma mensagem com sua chave pública. A assinatura é feita por um algoritmo criptográfico aplicado à mensagem ou a um pequeno bloco de dados que é uma função da mensagem.

III. Troca de chave: dois lados cooperam para trocar uma chave de sessão. Várias técnicas diferentes são possíveis, envolvendo as chaves públicas de uma ou de ambas as partes.

Está correto o que se afirma em

A I, apenas.

B II, apenas.

C III, apenas.

D I e II, apenas.

E II e III, apenas.

Comentário:

I – Em que pese a péssima nomenclatura, o item está abordando a prática de confidencialidade. Digo isso pois, em todo caso de uso de chaves, teremos sempre a criptografia. O que muda, é a finalidade a partir da combinação das chaves. Sendo assim, para a finalidade de confidencialidade, a questão está correta. Tem-se a criptografia originária com a chave pública do destinatário, de tal modo que somente o destinatário, com sua chave privada, conseguirá acessar o conteúdo. **CORRETO**

II – Temos aqui uma inversão. Para fins de autenticidade, deve-se começar coma chave privada do emissor, ou seja, somente ele seria capaz de criptografar aquela mensagem uma vez que a decriptação será feita com a chave pública do próprio emissor. **ERRADO**

III – Aqui temos um problema pessoal. Entendo que esse item deveria ser considerado correto. Sem dúvida, algoritmos de criptografia assimétrica são utilizados para troca de chaves, no caso, chaves simétricas, como etapa inicial do processo de troca de conteúdo posteriormente a partir da criptografia simétrica. Entretanto, a banca deu esse item como errado. **ERRADO**

Gabarito: B (gabarito do professor: anulação)

---

2. **FGV - 2017 - ALERJ - Especialista Legislativo - Tecnologia da Informação**

A equipe de marketing da empresa XPTO está desenvolvendo um novo produto que necessita ser mantido em sigilo até sua divulgação na mídia. Para evitar vazamento de informação acerca do projeto, o Gerente da equipe de marketing decidiu que todos os arquivos do projeto sejam criptografados e, por questões de segurança, ele altera a senha utilizada na criptografia dos arquivos eventualmente, divulgando-a entre os membros de sua equipe de forma segura.

A forma de criptografia utilizada pelo gerente de marketing da empresa XPTO é

A hash.

B criptografia de chave assimétrica.

C criptografia de chave simétrica.

D assinatura digital.

E certificado digital.

Comentário:

O aspecto chave da questão pessoal é entender que temos um regime de chave compartilhada, ou seja, a mesma chave é utilizada para criptografar e descriptografar.

Gabarito: C

---

3. **FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã**

Um dos mecanismos importantes de segurança é aquele que tenta solucionar o problema da autenticidade. A criptografia moderna procura resolver esse problema através dos algoritmos de criptografia assimétrica.

Para que isso ocorra,

A o emissor criptografa a mensagem com a chave pública do receptor e o receptor confirma a autenticidade decriptografando a mensagem usando sua própria chave privada.

B o emissor gera um hash da mensagem e o envia para o receptor junto com a mensagem. O receptor recalcula o hash e o compara com o hash enviado, e se forem iguais, a autenticidade estará confirmada.

C o emissor gera um hash da mensagem e o criptografa com sua chave privada. Para confirmar a autenticidade, o receptor decriptografa o hash recebido usando a chave pública do emissor, e verifica se esse hash é o mesmo calculado da mensagem.

D o emissor e receptor compartilham uma chave para criptografar e assinar digitalmente o hash gerado da mensagem.

E o emissor criptografa a mensagem com o certificado digital do receptor e o receptor confirma a autenticidade usando o certificado digital do emissor.

Comentário:

Vamos aos itens:

a) A confirmação aqui é na ótica da confidencialidade, e não da autenticidade. **ERRADO**

b) Temos aqui a simples garantia da integridade por meio das funções HASH, não havendo autenticidade pela ausência dos algoritmos de criptografia assimétrica. **ERRADO**

c) Exatamente pessoal. Lembrem-se sempre da perspectiva. Se o foco é autenticidade, precisa começar no emissor. E para isso, tem-se que utilizar a sua chave privada. **CORRETO**

d) Aqui, não deveria ser essa chave compartilhada, mas sim a dinâmica de chave privada do emissor com a chave pública dele no uso pelo destinatário. **ERRADO**

e) O certificado em si, não é a chave utilizada no processo. **ERRADO**.

Gabarito: C

---

4. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã

Analise as afirmativas abaixo sobre o algoritmo de criptografia assimétrica Diffie-Helmann:

I. Não é vulnerável a ataques "man-in-the-middle".

II. Pode ser utilizado tanto para assinatura digital quanto para geração de chave simétrica.

III. Pode ser usado de três maneiras diferentes: anônimo, estático e efêmero, sendo essa última considerada a maneira mais segura.

Está correto apenas o que se afirma em

A I.

B II.

C III.

D I e II.

E I e III.

Comentário:

Vamos aos itens:

I – Dada a ausência dos recursos de autenticidade, mas tão somente a geração de chaves para possibilitar a troca, de fato, o DH é vulnerável ao ataque MITM, a partir da intercepção de chaves durante a troca. ERRADO

II – Conforme mencionado no item anterior, só atua na troca de chaves. ERRADO

III – Na linha do que vimos na nossa teoria, de fato, há os três tipos de implementação. **CORRETO**

Gabarito: C

---

5. **FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados**

Para preservar a integridade das evidências encontradas em uma perícia computacional, o perito utilizou hashes criptográficos, pois essas funções são consideradas uma impressão digital eletrônica do dado coletado. No entanto, o perito escolheu uma função de hash que não é mais considerada segura, pois pode ser calculada rapidamente e é particularmente vulnerável a colisões.

Essa função de hash, considerada atualmente insegura, seria a

A SHA-3.

B Blowfish.

C Whirlpool.

D MD5.

E DES.

Comentário:

Temos a referência a funções HASH representadas nos itens A e D. Na prática, a partir dos resumos de 128 bits, temos que o MD5 já é vulnerável, sendo recomendado, portanto, o uso do SHA-3-.

Gabarito: D

---

6. **FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados**

Os desenvolvedores de um jogo eletrônico usaram uma criptografia simétrica baseada em cifras de bloco para proteger certas partes do jogo. Para verificar se a proteção estava adequada, contrataram um perito para análise de vulnerabilidades. O perito verificou que o modo de operação da cifragem em bloco usada não era seguro o suficiente, pois além de não possuir proteção de integridade, não era semanticamente seguro, pois mantinha padrões que existiam nos dados em claro.

O modo de operação da cifragem de blocos da criptografia simétrica usado no jogo é o

A CBC (Cipher Bloco Chaining).

B ECB (Electronic Codebook).

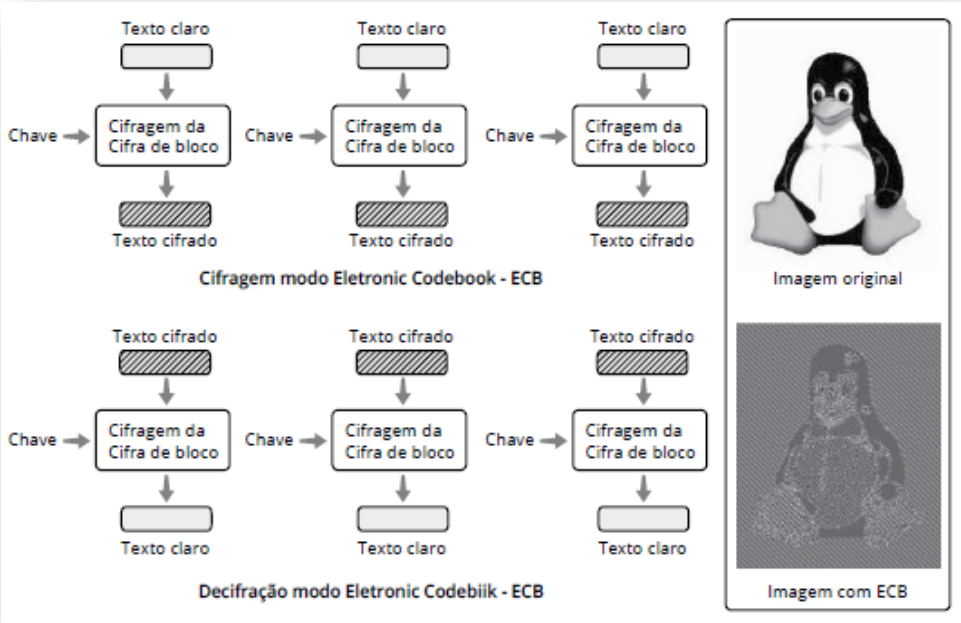
C OFB (Output Feedback).

D CFB (Cipher Feedback).

E CTR (Counter).

Comentário:

Importante lembrar das características básicas de cada modelo de cifragem. Especificamente falando, o ECB, que é o mais básico, não possui processo de retroalimentação e utiliza a mesma chave sempre, ou seja, a mesma entrada, sempre gerará a mesma saída, gerando assim, os padrões referenciados na questão.



Gabarito: B

---

7. FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados

O modo de operação de cifra de bloco da criptografia simétrica, no qual o bloco de texto claro atual é usado diretamente na entrada do algoritmo e criptografado com a mesma chave, de tal forma que, como consequência disso, sempre produz blocos de texto cifrado iguais para blocos de texto claro iguais, é o

A Cipher Block Chainning (CBC).

B Cipher Feedback (CFB).

C Output Feedback (OFB).

D Counter (CTR).

E Electronic Codebook (ECB).

Comentário:

Vejam o mesmo contexto de questão. De fato, mesma entrada e saída, a partir da utilização da mesma chave.

Gabarito: B

---

8. FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados

Sobre criptografia e compactação de arquivos, analise as afirmativas a seguir.

I. Todo arquivo criptografado está necessariamente compactado.

II. O processo de compactação usualmente explora a repetição de trechos e/ou padrões presentes no arquivo.

III. A compactação de arquivos de texto (.txt) alcança bons índices de compactação em relação a outros tipos de arquivos.

Está correto o que se afirma em:

A somente I;

B somente II;

C somente III;

D somente II e III;

E I, II e III.

Comentário:

Vamos aos itens:

I – Pessoal, a compactação anterior é uma boa prática, até mesmo para aumento da performance e eliminação de redundância. Agora não se trata de uma obrigatoriedade. **ERRADO**.

II – Essa é a ideia. Aspectos de redundância, que podem ser eliminados sem prejuízo da informação original, principalmente quanto à sua restauração. **CORRETO**

III – Essa alternativa merece uma explicação adicional, já adiantando que está correta.

A compactação de arquivos de texto (.txt) geralmente alcança bons índices de compactação em relação a outros tipos de arquivos, especialmente se o conteúdo do texto for composto por caracteres repetitivos e padrões.

Arquivos de texto são compostos por caracteres simples e sem formatação, e por isso, podem ser compactados facilmente usando algoritmos de compressão, como o LZ77, LZ78, Lempel-Ziv-Welch (LZW), ou Huffman. Esses algoritmos tiram proveito das redundâncias e padrões encontrados no texto para reduzir o tamanho do arquivo.

Por outro lado, outros tipos de arquivos, como arquivos de imagem e áudio, podem ser mais difíceis de compactar, especialmente se já estiverem em um formato comprimido. Por exemplo, arquivos JPEG e MP3 já passaram por compressão com perdas e possuem menos redundância, o que torna a compactação adicional menos eficiente.

O grau de compactação pode variar dependendo do conteúdo específico e do algoritmo utilizado.

Gabarito: D

---

9. FGV - 2021 - TCE-RO - Analista de Tecnologia da Informação - Desenvolvimento de Sistemas

Kátia, engenheira de segurança, recebeu de seu chefe uma mensagem a ser criptografada e enviada para uma das filiais da empresa em outro estado, de forma segura. A mensagem não é crítica para a empresa, logo o sistema de criptografia a ser utilizado pode ser computacionalmente simples. Kátia resolveu então usar uma cifra de transposição que não altera o conteúdo da mensagem, alterando apenas suas posições. Considerando que a chave utilizada foi MEGABUCK e o texto cifrado é

ISODAIAORPSOROPCUOCLSASMDSRENOLVOTIRCSMDTOIFROEEE RBUIATROSONOO

a alternativa que apresenta o texto em claro correto para o texto cifrado acima é:

A EMVIRTUDEDOSPROTESTOSOCORRIDOSLIBERAROSFUNCION ARIOSAPOSOALMOCO;

B EFETUARODEPOSITONACONTADAFILIALDERONDONIAHOJEIM PRETERIVELMENTE;

C ALTERARASFOLHASDEPAGAMENTOEDAROAUMENTOACORDA DONAREUNIAODEONTEM;

D TRANSFERIROFUNCIONARIOROBERTODODEPARTAMENTOBP ARAODEPARTAMENTOA;

E ENCAMINHARPOREMAILOPLANEJAMENTODEFERIASDODEPA RTAMENTOACADEMICO.

Comentário:

De antemão, adianto que a alternativa correta é a LETRA A. Uma forma de resolver é pela análise macro dos textos. Basicamente buscando as maiores repetições e tentando fechar o padrão. Vemos por exemplo a letra "O", que aparece no texto 13 vezes. Dado que é uma cifra de transposição, os quantitativos não mudam. Logo, qualquer alternativa que não tiver esse padrão, está errada.

Gabarito: A

---

10. FGV - 2021 - TCE-RO - Analista de Tecnologia da Informação - Desenvolvimento de Sistemas

Na implementação de tabelas Hash, quando as chaves não são perfeitamente distribuídas, é preciso lidar com as potenciais colisões que ocorrem quando:

A o espaço de endereçamento é superior ao número de chaves armazenadas;

B duas ou mais chaves têm o mesmo índice na tabela;

C as chaves são exclusivamente numéricas;

D as chaves são exclusivamente alfanuméricas;

E há duplicação de chaves.

Comentário:

Lembremos que o conceito de colisão se dá quando há duas entradas diferentes gerando a mesma saída, ou seja, o mesmo índice. Assim, algoritmos robustos são aqueles que geram a menor quantidade de colisões possíveis, e, por isso, o tamanho do HASH de saída é tão importante nesse processo, pois aumenta a difusão e, portanto, a menor probabilidade de colisão.

Assim, o trecho que descreve esse contexto da melhor forma é a alternativa B.

Gabarito: B

---

11. FGV - 2021 - TCE-RO - Analista de Tecnologia da Informação - Desenvolvimento de Sistemas

Uma técnica de criptografia largamente empregada para garantir segurança em transações digitais, que utiliza uma chave pública para ciframento de dados e uma outra chave privada para deciframento desses dados previamente cifrados, é:

A DES;

B AES;

C RSA;

D SHA;

E MD5.

Comentário:

Questão bem tranquila, para mapear os tipos de algoritmos. Lembremos:

a) Criptografia Simétrica

b) Criptografia Simétrica

c) Criptografia Assimétrica

d) Função HASH

e) Função HASH

Gabarito: C

---

12. FGV - 2018 - Prefeitura de Niterói - RJ - Analista de Políticas Públicas e Gestão Governamental - Gestão de Tecnologia

AES, RSA e RC4 são exemplos, respectivamente, de algoritmos de

A criptografia simétrica, de criptografia assimétrica e de dispersão criptográfica.

B criptografia simétrica, de criptografia assimétrica e de criptografia simétrica.

C criptografia simétrica, de criptografia de chave pública e de criptografia assimétrica.

D criptografia assimétrica, de criptografia simétrica e de criptografia assimétrica.

E criptografia assimétrica, de criptografia simétrica e de dispersão criptográfica.

Comentário:

Vamos lá:

AES e RC4 são criptografias simétricas, sendo a primeira por meio de cifra de bloco e a segunda por meio de cifra de fluxo.

RSA – Criptografia assimétrica.

Gabarito: B

---

13. FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e Comunicação

João quer enviar uma mensagem para Maria, mas assegurar que somente Maria será capaz de lê-la.

Então, João deve utilizar

A uma criptografia de chave pública e aplicar a chave-pública de Maria para fazer o ciframento da mensagem.

B uma criptografia assimétrica e aplicar a chave-privada de Maria para fazer o ciframento da mensagem.

C uma criptografia simétrica para fazer o ciframento da mensagem e não compartilhar a chave criptográfica.

D uma criptografia assimétrica para João colocar sua assinatura digital na mensagem.

E uma função de dispersão criptográfica para cifrar a mensagem e informar a Maria o algoritmo utilizado.

Comentário:

Lembremos sempre... Se o objetivo é a confidencialidade, somente o destinatário deve ser capaz de abrir. Logo, o recurso que ele precisará para ter esse nível de segurança é por meio da chave privada do destinatário.

Assim, é necessário, portanto, criptografar com a chave pública dele, para somente ele ser capaz de abrir com sua chave privada.

Gabarito: A

---

14. FGV - 2018 - Câmara de Salvador - BA - Analista de Tecnologia da Informação

Carlos é um analista de segurança. Ele pretende criptografar os dados dos servidores da sua empresa que possuem Windows Server 2012 como sistema operacional, protegendo-os contra roubos e acessos não autorizados, seja pela execução de ferramentas de ataque a software ou pela transferência do disco rígido do computador para outro computador.

A ferramenta por ele utilizada que reduz acessos não autorizados aos dados por meio do aperfeiçoamento das proteções de arquivo e sistema é o:

A AppLocker;

B BitLocker;

C Kerberos;

D NTLM;

E NTFS.

Comentário:

Vamos aos itens:

A) AppLocker: ajuda os administradores a controlarem quais aplicativos e arquivos os usuários podem executar. **Errado**

B) BitLocker:ferramenta de criptografia da Microsoft. **Certo**.

C) Kerberos: é um protocolo desenvolvido para fornecer poderosa autenticação em aplicações usuário/servidor, onde ele funciona como a terceira parte neste processo, oferendo autenticação ao usuário. Para garantir a segurança, ele usa criptografia de chave simétrica, com o DES. **Errado**

D) NTLM: em redes Windows, NTLM (NT LAN Manager) é um conjunto de protocolos de segurança da Microsoft que fornece autenticação, integridade e confidencialidade aos usuários. **Errado**

E) NTFS sistema padrão de arquivo para o Windows. **Errado**.

Gabarito: B

---

15. FGV - 2017 - ALERJ - Especialista Legislativo - Tecnologia da Informação

O protocolo SSL (Secure Sockets Layer) combina as criptografias assimétrica e simétrica para garantir a confidencialidade e a autenticidade na comunicação entre computadores na Internet. São exemplos, respectivamente, de algoritmos de criptografia assimétrica e simétrica:

A SHA e RSA;

B IDEA e SHA;

C RSA e MD5;

D AES e DES;

E RSA e IDEA.

Comentário:

Vamos aos itens:

A) SHA – Função HASH / RSA – Criptografia Assimétrica. **Errado**

B) IDEA – Criptografia Simétrica / SHA – Função HASH **Errado**

C) RSA – Criptografia Assimétrica / MD5 – Função HASH - **Errado**

D) AES – Criptografia Simétrica / DES – Criptografia Simétrica **Errado**

E) RSA – Criptografia Assimétrica / IDEA – Criptografia Simétrica. **Certo**.

Gabarito: E

---

16. FCC – TRE-SP/Analista Judiciário – Análise de Sistemas/2017

Um Analista de Sistemas do TRE-SP utilizará, em uma situação hipotética, o recurso de assinatura digital para os documentos eletrônicos emitidos pelo Tribunal. O processo da assinatura digital compreende, inicialmente, o uso de __I__ para criar um resumo do documento, seguido da criptografia do resumo utilizando Chave __II__ . Finalmente, o autor do documento utiliza-se de __III__ para assinar o documento juntamente com o resultado da etapa anterior. As lacunas I, II e III são, correta e respectivamente, preenchidas por

a) Certificado – Privada – Chave Pública

b) Hash – Privada – Certificado

c) Certificado – Pública – Chave Privada

d) Autenticação – Privada – Certificado

e) Hash – Pública – Chave Privada

Comentário:

A questão apresenta descrição das etapas realizadas para geração da assinatura digital. De maneira objetiva:

1. Gera-se o HASH da Mensagem.

2. Cifra-se com a Chave Privada do Emissor.

3. Envia o HASH cifrado em conjunto com a mensagem em texto claro.

4. O receptor decifra o HASH CIFRADO utilizando a chave pública do emissor.

5. O receptor gera um novo HASH a partir da mensagem em claro recebida.

6. Compara-se os HASH obtidos nas etapas 4 e 5.

Então pessoal, esse é o funcionamento básico da assinatura digital, garantindo a integridade, autenticidade e não-repúdio. Entretanto, a banca acabou misturando com a criptografia da mensagem para garantir o princípio da confidencialidade, situação em que se utilizou, na etapa II, da chave pública. Isso extrapola o conceito de assinatura digital, gerando, mais uma vez, prejuízo da análise do candidato. Mais uma vez, entendo que a questão deveria ser anulada.

Na página 273 do Livro do Stallings- "Criptografia e Segurança de Redes", temos:

“A assinatura digital direta envolve apenas as partes em comunicação (origem, destino). Considera-se que o destino conhece a chave pública da origem. Uma assinatura digital pode ser formada criptografando-se a

mensagem inteira com a chave privada do emissor (Figura II.Ic) ou criptografando-se um código de hash da mensagem com a chave privada do emissor.

A confidencialidade pode ser obtida pela criptografia adicional da mensagem inteira mais a assinatura com a chave pública do receptor (criptografia de chave pública) ou com uma chave secreta compartilhada (criptografia simétrica); como exemplo, veja as Figuras II.Id e II.Sd. Observe que e importante realizar a função de assinatura primeiro e, depois, uma função de confidencialidade externa."

Gabarito: E (Gabarito do Professor: Anulação)

---

17. FGV - 2017 - IBGE - Analista Censitário - Análise de Sistemas - Suporte à Comunicação e Rede

Em relação à criptografia, analise as afirmativas abaixo:

I. A criptografia simétrica é a ideal para ser usada para a finalidade de autenticação.

II. O protocolo SSL utiliza uma mistura de criptografia simétrica e assimétrica.

III. Uma das vantagens da criptografia simétrica sobre a assimétrica é a velocidade de processamento.

Está correto somente o que se afirma em:

A I;

B II;

C III;

D I e II;

E II e III.

Comentário:

Vamos aos itens:

I – **INCORRETO. Comentário no último item.**

II – **CORRETO.** Comentário no próximo item.

III – **CORRETO** . Exatamente. Por isso que, no processo de tunelamento, primeiro se usa a criptografia assimétrica para autenticação e integridade por meio da troca de chaves e estabelecimento da chave compartilhada. Em seguida, todo o tráfego de conteúdo é feito com a criptografia simétrica.

Gabarito: E

---

18. FGV - 2015 - DPE-RO - Analista da Defensoria Pública - Analista de Redes e Comunicação de Dados

A respeito de criptografia simétrica, analise as afirmativas a seguir:

I. Exemplo de algoritmos de criptografia simétrica são o AES, Blowfish e RC4.

II. Para ser considerada segura nos padrões atuais, o tamanho mínimo de chave simétrica deve ser 1024 bits.

III. O protocolo SSL utiliza essa forma de criptografia para cifragem dos dados, pois demanda menos poder de processamento. Está correto somente o que se afirma em:

A I;

B II;

C III;

D I e II;

E I e III;

Comentário:

Vamos aos itens:

I – **CORRETO.** Lembrando que AES e BLowfish são cifras de bloco, e o RC4 cifra de fluxo.

II –. **INCORRETO** Vimos que há processamentos via AES com 128 bits, sendo completamente seguro. Este é só um exemplo.

III – **CORRETO** . Exatamente. Por isso que, no processo de tunelamento, primeiro se usa a criptografia assimétrica para autenticação e integridade por meio da troca de chaves e estabelecimento da chave compartilhada. Em seguida, todo o tráfego de conteúdo é feito com a criptografia simétrica.

Gabarito: E

---

19. FGV - 2015 - TCM-SP - Agente de Fiscalização - Tecnologia da Informação

Pedro quer enviar uma mensagem para Maria, porém o sigilo é importante nesta comunicação. Somente Maria deve ser capaz de ler a mensagem. Por outro lado, Maria precisa ter a garantia de que a mensagem foi enviada por Pedro.

Para garantir a autenticação do autor e a confidencialidade dos dados, será necessário utilizar:

A dois algoritmos fortes de criptografia simétrica;

B criptografia simétrica para garantir a autoria e assimétrica para ciframento dos dados;

C dois pares de chaves públicas e privadas;

D criptografia assimétrica para assinatura digital;

E assinatura digital para autoria e um algoritmo de hashing para assegurar a confidencialidade.

Comentário:

Pessoal, temos duas sequências de utilização de chaves distintas para finalidades distintas.

Assim sendo, temos:

Para autenticação – Deve-se usar a Chave privada do emissor para criptografia e a chave pública do receptor para descriptografar.

Para confidencialidade – Deve-se usar a Chave pública do destinatário para criptografar e a chave privada do destinatário para descriptografar.

Gabarito: C

---

20. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O uso da encriptação é fundamental para manter a segurança das comunicações e transações comerciais na internet.

Sobre os algoritmos de encriptação, analise as afirmativas a seguir.

I. O algoritmo RC4 é um algoritmo simétrico de criptografia utilizado nos protocolos Secure Socket Layers (SSL) (para proteger o tráfego Internet) e WEP (para a segurança de redes sem fios).

II. O algoritmo AES é um algoritmo simétrico de criptografia com várias aplicações na internet e na proteção de direitos autorais (DRM) que emprega atualmente chaves com pelo menos 2048 bits.

III. O algoritmo RSA é um algoritmo simétrico de criptografia projetado para ter implementações eficientes tanto em hardware como em software, sendo utilizado atualmente com chaves entre 128 e 256 bits.

Está correto o que se afirma em

A I, apenas.

B II, apenas.

C III, apenas.

D I e III, apenas.

E I, II e III.

Comentário:

Vamos aos itens:

I – **CORRETO.** Sem muito o que acrescentar, a não ser lembrar que o RC4 é uma cifra de fluxo.

II – **INCORRETO.** O AES atua com três chaves (128, 192 e 256), mantendo fixo o tamanho do bloco em 128 bits.

III – **INCORRETO**. O RSA é um algoritmo de criptografia assimétrica, e traz como contexto de uso chaves de 1024, 2048 e 2096 bits.

Gabarito: A

---

21. FGV - 2015 - TCM-SP - Agente de Fiscalização - Tecnologia da Informação

Pedro quer enviar uma mensagem para Maria, porém o sigilo é importante nesta comunicação. Somente Maria deve ser capaz de ler a mensagem. Por outro lado, Maria precisa ter a garantia de que a mensagem foi enviada por Pedro.

Para garantir a autenticação do autor e a confidencialidade dos dados, será necessário utilizar:

A dois algoritmos fortes de criptografia simétrica;

B criptografia simétrica para garantir a autoria e assimétrica para ciframento dos dados;

C dois pares de chaves públicas e privadas;

D criptografia assimétrica para assinatura digital;

E assinatura digital para autoria e um algoritmo de hashing para assegurar a confidencialidade.

Comentário:

Pessoal, temos duas sequências de utilização de chaves distintas para finalidades distintas.

Assim sendo, temos:

Para autenticação – Deve-se usar a Chave privada do emissor para criptografia e a chave pública do receptor para descriptografar.

Para confidencialidade – Deve-se usar a Chave pública do destinatário para criptografar e a chave privada do destinatário para descriptografar.

Gabarito: C

---

22. FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015

O técnico judiciário da área de TI do TRT da 3a Região deve escolher o esquema de criptografia mais adequado para a seguinte situação. Ele deve receber uma informação de forma segura, ou seja, criptografada, de outro Tribunal, mas não tem meios para enviar um código secreto (chave) de forma segura para aquele Tribunal. Nessa situação, o técnico deve utilizar o esquema de criptografia de chave

a) simétrica.

b) privada.

c) assimétrica.

d) unificada.

e) isolada.

Comentário:

Pessoal, vimos que um dos principais propósitos da criptografia de chave assimétrica é para permitir a transferência da chave privada de forma segura em meios inseguros. Apenas lembrando que neste processo, deve-se criptografar a chave a ser enviada com a chave pública do destinatário.

Dessa forma, somente o destinatário que é dono da respectiva chave privada será capaz de interpretar a mensagem.

Gabarito: C

---

23. FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015

Um dos padrões de criptografia mais difundidos mundialmente é o Data Encryption Standard – DES. Atualmente ele é utilizado na forma denominada Triple DES, devido à fragilidade identificada no DES que utiliza uma chave com

a) 48 bits.

b) 56 bits.

c) 128 bits.

d) 84 bits.

e) 64 bits.

Comentário:

Temos aqui uma questão que demonstra a interpretação da banca FCC a respeito do DES. Lembremos que a estrutura básica do DES utiliza chaves de 64 bits. Entretanto, 8 desses bits são apenas paridade, ou seja, não representam de fato uma parcela da chave. Nesse sentido, considerando o tamanho da chave e robustez do algoritmo, deve-se considerar o DES com chave de 56 bits, conforme mencionamos na nossa teoria.

Gabarito: B

---

24. FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015 Considere:

M = Mensagem

KS = Chave Secreta compartilhada

MACr = Código de Autenticação de Mensagem gerado pelo remetente

KPr = Chave pública do remetente

MACd = Código de Autenticação de Mensagem gerado pelo destinatário

KPd = Chave Pública do destinatário

Um resumo criptográfico pode ser usado para verificar a integridade de uma mensagem - se ela não foi modificada. Para garantir a integridade da mensagem e autenticar a origem dos dados, uma das formas é: o remetente, por meio de uma função hash e usando a M concatenada com

a) KS, gera um MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KS, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

b) KS, gera um MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KPr, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

c) KPr, gera um MACr que, juntamente com M é enviado por um canal seguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KPr, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

d) KPr, gera um MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KS, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

e) KS e KPr, gera um MACr que, juntamente com M é enviado por um canal seguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KPd, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

Comentário:

Questão bem extensa e complicada, não é? Devemos avaliar com calma. Entretanto, a banca foi "amiga" em nos apresentar a resposta logo no primeiro item. Temos aqui pessoal a descrição da Assinatura Digital Simétrica, conforme mencionei em aula.

Vamos analisar cada etapa sendo descrita:

1 uma função hash e usando a M concatenada com KS, gera um MACr. (Temos aqui a primeira parte do conjunto a ser enviado, que é o HASH da mensagem concatenada com a chave secreta que é de conhecimento mútuo).

2 MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. (Aqui já temos o resultado final do conjunto a ser enviado, que é o HASH e a mensagem que também foi utilizada dentro do HASH).

3 O destinatário separa a MACr de M e, usando M concatenada com a KS, gera um MACd (Assim que o destinatário recebe o conjunto, ele separa o HASH da Mensagem. Pegando apenas a mensagem e sabendo da chave secreta, ele gerará um novo HASH para comparação com o HASH recebido)

4 MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica. (Tendo em mãos o HASH recebido e o HASH gerado a partir do mesmo bloco de dados, que é a Mensagem e a chave secreta, ele está apto a comparar os resultados.)

Uma observação ao fato de que a banca tentou levar o candidato ao erro ao inserir as chaves públicas no enunciado. É natural que tendemos a sempre vincular a criptografia assimétrica com a utilização das chaves públicas e privadas para tais finalidades.

Entretanto, devemos lembrar desse modelo de Assinatura Digital Simétrica.

Gabarito: A

---

25. FCC – TRE-RR/Analista Judiciário – Análise de Sistemas/2015

Um sistema de computador envia uma mensagem para um receptor, acompanhada de um resumo dessa mensagem cifrado com chave privada. O objetivo é garantir que o sistema receptor decifre o resumo com uma chave pública enviada pelo remetente, calcule um novo resumo com base na mensagem recebida e compare o resultado com a mensagem original para garantir a integridade. Essa função criptográfica é chamada:

a) Criptografia pública cptu.

b) Criptografia privada cptp.

c) Resumo criptográfico hash.

d) Criptografia simétrica simt.

e) Resumo criptográfico gram.

Comentário:

Temos a descrição do procedimento de checagem da integridade no processo de assinatura digital padrão com criptografia assimétrica. O HASH gerado sobre a MENSAGEM e criptografada com a CHAVE PRIVADA é chamado de Resumo criptografado HASH.

De posse da mensagem original e do HASH, obtidos por intermédio da chave pública do remetente, o destinatário será capaz de gerar um novo HASH da mensagem recebida e comparar os resumos

Gabarito: C

---

26. FCC – CNMP/Analista do CNMP – Suporte e Infraestrutura/2015

Em segurança da informação, a criptografia é a técnica que utiliza a cifragem e, frequentemente, uma chave criptográfica para transformar a informação original para que apenas o interlocutor, ou as pessoas autorizadas, possam ler a informação original. Dentre as diferentes técnicas de criptografia atualmente utilizadas, a que utiliza o esquema de chave assimétrica é

a) AES.

b) DES.

c) RSA.

d) IDEA.

e) RC4.

Comentário:

Mais uma questão básica a respeito da simples distinção dos algoritmos. Como vimos, todos os da lista são algoritmos de criptografia simétrica, com exceção do RSA. Vale lembrar que o RC4 é um algoritmo de criptografia simétrico que utiliza cifras de fluxo, enquanto os demais utilizam cifras de bloco.

Gabarito: C

---

27. FCC – TJ-AP/Analista Judiciário – TI/2014

Para fornecer confidencialidade com criptografia de chave simétrica, uma solução é usar a criptografia de chaves simétricas para a codificação da informação a ser transmitida e a criptografia de chaves assimétricas para o compartilhamento da chave secreta, neste caso, também chamada de chave de

a) hash.

b) autenticação.

c) Diffie-Hellman.

d) enlace.

e) sessão.

Comentário:

Temos aí a descrição de um modelo básico de comunicação utilizado. Lembremos sempre que a criptografia assimétrica, em regra, é utilizada para a troca de chaves, enquanto a simétrica é utilizada para a criptografia dos dados de fato por apresentar melhor desempenho.

Nesse sentido, em cada comunicação iniciada, os nós trocam uma nova chave secreta entre si que será utilizada durante aquele período de comunicação. Ao se encerrar, essa chave será descartada e, caso haja necessidade de uma nova comunicação, gera-se uma nova chave secreta e utiliza-se novamente a criptografia assimétrica para o compartilhamento da nova chave. **Assim, cada chave secreta gerada é utilizada como uma chave de sessão.**

Tal modelo impede que, caso haja violação da chave secreta em um dado momento, futuramente ela não fará mais sentido pois será descartada, reduzindo os prejuízos no vazamento dessa chave secreta.

Gabarito: E

---

28. FCC – TJ-AP/Analista Judiciário – TI/2014

Para prover segurança à rede sem fio da empresa, um especialista em segurança de redes adotou o padrão WPA2, que possui um método de criptografia mais forte e algoritmos mais rápidos que padrões anteriores. O WPA2 adota a criptografia

a) RC4 que permite chaves de 256 ou 512 bits

b) RC4 que permite chaves de 256 bits.

c) AES que permite chaves de 256 bits.

d) 3DES que permite chaves de 168 bits.

e) AES que permite chaves de 512 bits

Comentário:

Um dos principais avanços em termos de segurança do WPA2 em relação ao WPA e ao WEP é a utilização do algoritmo AES no lugar do RC4. Como vimos, o AES suporta a utilização de 128, 192 ou 256 bits, restando, assim, apenas o item C como resposta.

Gabarito: C

---

29. (FCC – TJ-AP/Analista Judiciário – TI/2014) Um Analista de TI do Tribunal de Justiça recebeu a incumbência de planejar e implementar um esquema de criptografia de Chave Pública para a troca de informações entre as duas comarcas de Macapá. Dentre os diferentes algoritmos existentes, ele deve escolher o

a) AES.

b) RC6.

c) DES.

d) IDEA.

e) RSA

Comentário:

Vejamos o tanto de questões que resolveríamos por simplesmente lembrar que o RSA é um algoritmo de criptografia assimétrica.

Gabarito: E

---

30. FCC – TRT – 1° Região (RJ)/Analista Judiciário – TI/2014

Um Analista em Tecnologia da Informação do TRT da 1ª Região deve escolher um algoritmo de criptografia assimétrica para os serviços de acesso à rede de computadores do Tribunal. O Analista deve escolher o

a) DES.

b) IDEA.

c) AES.

d) RSA.

e) RC4.

Comentário:

Para reforçar minha afirmação na questão anterior. Percebam que é uma questão também de 2014 e de tribunal.

Gabarito: D

---

31. FCC – TRF – 4ªRegião/Técnico Judiciário – TI/2014

Basicamente, um esquema de criptografia simétrica possui cinco itens que são:

a) texto claro, algoritmo de criptografia, chave secreta compartilhada emissor/receptor, texto codificado e algoritmo de decriptografia.

b) texto claro, algoritmo de criptografia, chave secreta do emissor, chave secreta do receptor e texto codificado.

c) algoritmo de criptografia, chave secreta do emissor, chave pública do receptor, texto codificado e algoritmo de decriptografia.

d) algoritmo de criptografia, chave pública do emissor, chave secreta do receptor, texto codificado e algoritmo de decriptografia.

e) texto claro, algoritmo de criptografia, chave pública compartilhada emissor/receptor, chave secreta do receptor e texto decodificado.

Comentário:

Se estivermos falando de criptografia simétrica, devemos lembrar que não há chaves públicas ou privadas, mas tão somente a chave secreta de conhecimento das duas partes.

Assim, não há o que se falar em chave pública ou chave secreta de um ou de outro.

Gabarito: A

---

32. FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015

Diversos recursos e ferramentas são utilizados para melhorar a segurança da informação, principalmente a transmissão de informações pela rede de computadores. Nesse contexto, o hash é utilizado para

a) gerar um conjunto de dados de tamanho fixo independentemente do tamanho do arquivo original.

b) criar uma chave criptográfica específica e personalizada para o arquivo a ser transmitido pela rede.

c) verificar a autenticidade da mensagem utilizando a chave simétrica gerada no processo de hashing.

d) armazenar, em um arquivo, e transmitir a chave assimétrica utilizada para criptografar os dados.

e) checar a veracidade de uma assinatura digital junto a uma Autoridade Certificadora.

Comentário:

As funções HASH são regidas por algumas características básicas, entre elas:

Deverá suportar mensagens de entrada de quaisquer tamanhos para a produção de mensagens de saída de tamanho fixo (Message Digest);

Deverá ser unidirecional, ou seja, não deve ser possível, a partir da mensagem de saída, retornar à mensagem de entrada;

Mensagens de entrada distintas devem produzir mensagens de saída distintas;

A mesma mensagem de entrada deve produzir sempre a mesma mensagem de saída;

Desse modo, verificamos que a alternativa A nos apresenta a característica elencada no item 1.

Ademais, temos os outros itens:

b) A função HASH não depende de chave criptográfica, mas tão somente um cálculo matemático que recebe uma entrada e produz uma saída. **INCORRETO**

c) Mais uma vez não se aplica os conceitos de chave, muito menos a geração delas no processo de HASHING. **INCORRETO**

d) Novamente, a mesma confusão de conceitos. **INCORRETO**

e) Uma das aplicações do HASH é para a constituição da assinatura digital. Entretanto, não tem relação com o processo de checagem junto à uma autoridade certificadora. **INCORRETO**

Portanto, temos como gabarito a alternativa A.

Gabarito: A

---

33. FCC – TRT – 18ª Região (GO)/Analista Judiciário – TI/2013

Observe as regras de um algoritmo de criptografia:

Para criptografar uma mensagem, fazemos: c = m^e mod n

Para descriptografá-la: m = c^d mod n

Onde: m = texto simples c = mensagem criptografada n = é o produto de dois números primos o par (e, n) = chave pública o par (d, n) = chave privada ^ = é a operação de exponenciação (a^b: a elevado à potência b) mod = é a operação de módulo (resto da divisão inteira) Este algoritmo é de domínio público e é amplamente utilizado nos navegadores para sites seguros e para criptografar e-mails.Trata-se do algoritmo.

a) simétrico DES - Data Encryption Standard.

b) simétrico AES - Advanced Encryption Standard.

c) assimétrico RSA - Rivest, Shamir and Adleman.

d) assimétrico AES - Advanced Encryption Standard.

e) simétrico RSA - Rivest, Shamir and Adleman.

Comentário:

Percebam que para resolvermos a questão, não necessitamos saber do funcionamento do algoritmo, mas tão somente a complexidade matemática envolvida no principal algoritmo de criptografia assimétrica que é o RSA em relação à fatoração do produto de número primos grandes, certo?

Gabarito: C

LISTA DE QUESTÕES

1. **(CESPE – SE-DF/Analista de Redes/2017) No contexto de uma infraestrutura de chaves públicas, um documento eletrônico assinado digitalmente com a chave pública do remetente falhará na verificação de integridade e autoria pelo destinatário, caso essa verificação seja realizada com a aplicação da mesma chave pública do remetente.**

---

2. **(CESPE – TCE-PR/Analista de Controle – Área TI/2016) Assinale a opção correta, no que concerne a conceitos básicos de criptografia e criptografia simétrica e assimétrica.**

a) A principal diferença entre os algoritmos de criptografia simétrica e os algoritmos de criptografia assimétrica consiste no fato de que os primeiros são fundamentados em técnicas de transposição e os segundos em técnicas de substituição.
b) Um esquema de criptografia será considerado computacionalmente seguro se o tempo para se quebrar sua cifra for superior ao tempo de vida útil da informação por ele protegida.

c) Em uma transmissão de dados em que se use criptografia simétrica, as chaves de criptografia e decriptografia têm de ser distintas, embora tenham de ter o mesmo tamanho.

d) O valor da chave de criptografia depende do texto claro a ser criptografado e do algoritmo a ser usado para criptografar esse texto.

e) Em um ataque por força bruta, exploram-se a natureza e as características do algoritmo na tentativa de deduzir as chaves

---

3. **(CESPE – TCE-PR/Analista de Controle – Área TI/2016) Em um esquema de criptografia de chaves públicas, caso um sistema participante opte por alterar sua chave privada, para que seja mantida a comunicação, será necessário**

a) gerar uma nova chave privada a partir da chave pública existente e substituir a chave pública pela nova chave.

b) gerar uma nova chave privada e publicar essa nova chave privada.

c) gerar um novo par de chaves e publicar as duas novas chaves — pública e privada.

d) gerar um novo par de chaves e publicar a nova chave pública.

e) gerar um novo par de chaves, substituir a chave privada e, consequentemente, descartar a nova chave pública gerada.

---

4. **(CESPE – TCE-PR/Analista de Controle – Área TI/2016) Acerca da criptografia, assinale a opção correta.**

a) O algoritmo DES utilizado para chaves simétricas é imune a ataques do tipo meet-in-the-middle (encontro no meio).

b) Em um esquema de criptografia simétrica, a chave secreta, além de ser a saída para o algoritmo de criptografia, é também a chave para decriptografar e depende do texto claro e do algoritmo.

c) O algoritmo Diffie-Hellman é utilizado para criptografia com chave pública e pode ser utilizado tanto para assinatura digital quanto para decriptografia.

d) O algoritmo RSA é imune a ataques matemáticos, mas suscetível a ataques do tipo força bruta.

e) O algoritmo RSA permite que o emissor criptografe uma mensagem com a chave pública do destinatário ou, ainda, que assine uma mensagem com sua chave privada.

---

5. **(CESPE – TCE-SC/AFCE – Área TI/2016) Os algoritmos de criptografia de chave pública devem ser computacionalmente fáceis, a fim de que o receptor de uma mensagem cifrada com uma chave pública a decriptografe utilizando sua chave privada para recuperar a mensagem original.**

---

6. **(CESPE - TJ STF/Apoio Especializado/Tecnologia da Informação/2013) A criptologia incorpora estudos e conhecimentos das áreas de criptografia e criptoanálise.**

---

7. **(CESPE - AJ TRT10/Apoio Especializado/Tecnologia da Informação/2013) Na criptografia de chave pública assimétrica, são utilizadas duas chaves diferentes: uma chave privada confidencial, para criptografar os dados, e outra chave pública, para decriptografar os dados, a qual é distribuída para os destinatários.**

8. **(CESPE - PCF/Área 2/2013) A compressão de dados antes da encriptação geralmente aumenta a segurança do sistema, por reduzir a redundância na mensagem, dificultando a criptoanálise.**

---

9. **(CESPE - PCF/Área 2/2013) Esquemas de criptografia de chave pública também são conhecidos como de criptografia simétrica, pois possuem apenas uma chave, tanto para encriptação quanto para desencriptação.**

---

10. **(CESPE - PCF/Área 3/2013) Um aplicativo que utiliza recursos biométricos para a criptografia de arquivos, como a impressão digital de um indivíduo tanto para encriptar quanto decriptar, assemelha-se a um sistema criptográfico simétrico.**

---

11. **(CESPE - PCF/Área 3/2013) Modos de operação de cifra de bloco permitem cifrar mensagens de tamanhos arbitrários com a utilização de algoritmos de cifragem de blocos, que trabalham com blocos de tamanho fixo. Os modos de operação existentes asseguram a confidencialidade e a integridade da mensagem cifrada, embora nem todos possam ser utilizados para autenticação.**

---

12. **(CESPE - PCF/Área 3/2013) A confidencialidade e a integridade de uma comunicação são garantidas com o uso de criptografia tanto simétrica quanto assimétrica. No entanto, para garantir autenticidade e irretratabilidade, é necessário o uso combinado desses dois tipos de criptografia**

---

13. **(CESPE - AA (TCE-ES)/Informática/2013) Criptografia é uma técnica matemática capaz de transformar uma informação da sua forma original para outra forma totalmente ilegível, a partir da qual um processo inverso pode voltar a recuperar a informação para seu formato original. Acerca dessas informações, assinale a opção correta.**

a) A técnica criptográfica garante os atributos de autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação.

b) Os algoritmos de chaves simétricas e assimétricas são as categorias básicas de algoritmos criptográficos, sendo os de chaves assimétricas a base conceitual da certificação digital.

c) Os algoritmos RSA e as curvas elípticas são exemplos de algoritmos criptográficos com base em chaves simétricas.

d) Os algoritmos DES e AES são exemplos de algoritmos criptográficos com base em chaves assimétricas.

e) Quando criptografada, a informação passa a ter a garantia de nível máximo de proteção.

14. (CESPE - Ana Info (TCE-RO)/2013) Na criptografia simétrica, são geradas duas chaves criptográficas, uma privada e outra pública, para que um arquivo seja transferido, entre dois computadores, de forma criptografada.

15. (CESPE - AJ (STF)/Apoio Especializado/Análise de Sistemas de Informação /2013) Criptografia de chave simétrica, que também é conhecida como criptografia de chave pública, utiliza chaves distintas para codificar e decodificar as informações. Uma dessas chaves é pública e a outra é do gerador da criptografia.

16. (CESPE - Ana Sist (SUFRAMA)/2014) Para averiguar a integridade de um arquivo de computador a ser transmitido por um meio inseguro, pode-se gerar um hash antes da transmissão e verificar o hash após a transmissão.

17. (CESPE - TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013) Para evitar o acesso de terceiros não confiáveis aos dados, pode-se utilizar a criptografia simétrica, técnica que confere confidencialidade às informações.

18. (CESPE - TJ TRT17/Apoio Especializado/Tecnologia da Informação/2013) A função de hashing, por apresentar utilidade criptográfica, caracteriza-se por bidirecionalidade, compressão, tamanho variável, facilidade de cálculo, difusão, colisão simples e colisão forte.

19. (CESPE - Aud Gov (CGE PI)/Tecnologia da Informação/2015) Se, em um esquema de criptografia de chave pública, o emissor E criptografar uma mensagem M utilizando a chave pública do receptor R, então, nesse esquema, é oferecida confidencialidade, mas não autenticação.

20. (CESPE - PCF/Área 3/2013) AES é uma cifra de bloco, enquanto o RC4 é uma cifra de fluxo. Apesar dessa diferença, ambos têm em comum a utilização de um tamanho de chave de 128, 192 ou 256 bits.

21. (CESPE - ANTAQ/TI - Analista de Infraestrutura/2014) Na criptografia simétrica, a mesma chave compartilhada entre emissor e receptor é utilizada tanto para cifrar quanto para decifrar um documento. Na criptografia assimétrica, utiliza-se um par de chaves distintas, sendo a chave pública do receptor utilizada pelo emissor para cifrar o documento a ser enviado; posteriormente, o receptor utiliza sua chave privada para decifrar o documento.

22. (CESPE - Ana MPU/Tecnologia da Informação e Comunicação/Desenvolvimento de Sistemas/2013) Em uma troca de dados, via Internet, entre dois computadores que estejam utilizando um algoritmo de criptografia assimétrica, antes de trocarem os dados, os usuários deverão compartilhar entre eles a chave, já que ela deve ser a mesma para os dois usuários.

---

23. (CESPE - ANATEL/ Analista - Suporte e Infraestrutura de Tecnologia da Informação/2014) Uma das propriedades de uma função de hash, conhecida como resistência à primeira inversão ou propriedade unidirecional, garante que, dada uma mensagem, não é possível encontrar uma mensagem alternativa que gere o mesmo valor de hash da mensagem original.

---

24. (CESPE - ANATEL/Analista - Suporte e Infraestrutura de Tecnologia da Informação/2014) Para que a criptografia de chave pública seja considerada segura, uma das premissas é que o conhecimento do algoritmo, o conhecimento de uma das chaves e a disponibilidade de amostras de texto cifrado sejam, em conjunto, insuficientes para determinar a outra chave.

---

25. (CESPE - ANATEL/Analista - Desenvolvimento de Sistemas de Informação/2014) Nos métodos mais seguros de criptografia, a função e a chave utilizadas na encriptação devem ser de conhecimento exclusivo do remetente da mensagem.

---

26. (CESPE - Tec MPU/Técnico Administrativo/Tecnologia da Informação e Comunicação/2013) Se um usuário cifra uma mensagem com a chave pública do destinatário e depois cifra novamente com sua própria chave privada, apenas o destinatário será capaz de recuperar a mensagem em claro.

---

27. (CESPE - Tec MPU/Técnico Administrativo/Tecnologia da Informação) Em sistemas de criptografia assimétrica existem duas chaves com funções complementares que devem ser mantidas em segredo.

---

28. (CESPE - PCF/Área 3/2013) SHA-1 e MD-5 são exemplos de hashes criptográficos largamente utilizados na Internet. O MD-5 tem sido substituído pelo SHA-1 pelo fato de este gerar um hash maior e ser o único à prova de colisões.

---

29. (CESPE - PCF/Área 3/2013) O SHA-1, comumente usado em protocolos de segurança, como TLS, SSH e IPSec, também é utilizado por alguns sistemas de controle de versão como Git e Mercurial para garantir a integridade das revisões.

---

30. (CESPE - Ana Info (TCE-RO)/2013) O hash poderá auxiliar na verificação da integridade de um arquivo transferido de um computador para outro.

---

31. (CESPE - TJ STF/Apoio Especializado/Tecnologia da Informação/2013) Os algoritmos de criptografia simétricos apresentam menor desempenho que os algoritmos assimétricos.

---

32. (CESPE - TJ STF/Apoio Especializado/Tecnologia da Informação/2013) No RSA (Rivest-Shamir-Adleman), o texto claro é criptografado em blocos com valor binário limitado.

---

33. (CESPE - AJ (STF)/Apoio Especializado/Análise de Sistemas de Informação /2013) O algoritmo de criptografia MD5 (Message-Digest Algorithm 5) é um método que transforma uma palavra em um código criptografado único, ou seja, não é possível que duas strings diferentes produzam o mesmo hash.

---

34. (CESPE - AJ (STF)/Apoio Especializado/Suporte em Tecnologia da Informação/2013) O algoritmo RSA gera chaves públicas de tamanho fixo e limitado a 2.048 bits.

---

35. (CESPE - AA (ANATEL)/Desenvolvimento de Sistemas de Informação/2014) O texto cifrado F é obtido a partir do texto aberto C, utilizando-se o método monoalfabético de criptografia com chave igual a 3.

---

36. (CESPE - AA (ANATEL)/Suporte e Infraestrutura de Tecnologia da Informação/2014) O algoritmo de criptografia AES (advanced encryption standard) opera em quatro estágios: um de permutação e três de substituição. O estágio de permutação ShiftRows é reversível e os estágios de substituição SubBytes, MixColumns e AddRoundKey são não-reversíveis.

---

37. (CESPE - AUFC/Controle Externo/Auditoria de Tecnologia da Informação/2015) No algoritmo AES, a cifra de decriptografia é idêntica à cifra de criptografia, assim como a sequência de transformações para a decriptografia é a mesma para a criptografia, o que pode ser considerado uma vantagem, já que apenas um único módulo de software ou firmware é necessário para aplicações que exigem tanto criptografia quanto decriptografia.

---

38. (CESPE – TRE/RS / Analista Judiciário/2015) Assinale a opção correta relativamente a criptografia.

a) O algoritmo de criptografia AES utiliza quatro estágios diferentes, dois de permutação e dois de substituição.

b) No modo de operação de cifra de bloco cipher block chaining, o texto claro é tratado em blocos — um bloco por vez — e cada bloco de texto claro é criptografado mediante o uso de uma mesma chave.

c) Um código gerado por uma função hash para um conjunto de dados pode garantir a sua integridade porque, ao ser calculado novamente sobre o mesmo conjunto de dados, a qualquer tempo, pode determinar, inequivocadamente, se esse conjunto foi alterado ou não.

d) Esquema de criptografia incondicionalmente seguro significa que o custo para quebrar a cifra é superior ao valor da informação codificada ou que o tempo exigido para quebrar a cifra é superior ao tempo de vida útil da informação.

e) A criptoanálise, técnica para ataque a um esquema de criptografia convencional, caracteriza-se pela experimentação de cada chave possível em um trecho do texto cifrado, até que se obtenha uma tradução inteligível para texto claro.

---

39. (CESPE – TRE/RS / Técnico Judiciário/2015) A propósito de criptografia, assinale a opção correta.

a) Há, no envio de e-mail com o hash, garantia de autenticidade, pois ele criptografa a mensagem enviada.

b) Na criptografia de chave pública, ou assimétrica, a chave utilizada para encriptar mensagens é distribuída livremente, ao passo que a chave privada decripta a mensagem.

c) São utilizadas, na criptografia simétrica, duas chaves: uma para encriptar e outra para decriptar.

d) O AES é um algoritmo de criptografia simétrica que usa chaves de 168 bites.

e) A criptografia, simétrica além de garantir a integridade dos dados, atende plenamente aos demais princípios de segurança como a integridade e a autenticidade, por exemplo.

---

40. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) O protocolo 3DES possui três chaves criptográficas: a primeira e a segunda criptografam informações; a terceira é usada para descriptografar aquelas.

---

41. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) Em uma VPN com IPSEC é possível fazer uso do 3DES com algoritmo de criptografia que emprega três chaves de 56 bits.

---

42. (CESPE – FUNPRESP/ Área 8/2016) Na criptografia assimétrica, a chave pública deve apresentar tamanho variado, e a chave privada, tamanho fixo com, no mínimo, 512 bites

---

43. (CESPE – FUNPRESP/ Área 8/2016) Na criptografia simétrica com uso do modo de cifra em bloco (CBC), cada bloco cifrado pode utilizar a mesma chave.

LISTA DE QUESTÕES COMPLEMENTARES

1. FGV 2022 TRT - 6ª REGIÃO (MA) - Analista Judiciário - Tecnologia da Informação

Os sistemas de chave pública são caracterizados pelo uso de um algoritmo criptográfico com duas chaves, uma privada e uma pública. Com relação às categorias de uso dos criptossistemas de chave pública, analise as afirmativas a seguir:

I. Criptografia/descriptografia: um emissor criptografa uma mensagem com a chave pública do seu destinatário.

II. Assinatura digital: um emissor assina uma mensagem com sua chave pública. A assinatura é feita por um algoritmo criptográfico aplicado à mensagem ou a um pequeno bloco de dados que é uma função da mensagem.

III. Troca de chave: dois lados cooperam para trocar uma chave de sessão. Várias técnicas diferentes são possíveis, envolvendo as chaves públicas de uma ou de ambas as partes.

Está correto o que se afirma em

A I, apenas.

B II, apenas.

C III, apenas.

D I e II, apenas.

E II e III, apenas.

---

2. FGV - 2017 - ALERJ - Especialista Legislativo - Tecnologia da Informação

A equipe de marketing da empresa XPTO está desenvolvendo um novo produto que necessita ser mantido em sigilo até sua divulgação na mídia. Para evitar vazamento de informação acerca do projeto, o Gerente da equipe de marketing decidiu que todos os arquivos do projeto sejam criptografados e, por questões de segurança, ele altera a senha utilizada na criptografia dos arquivos eventualmente, divulgando-a entre os membros de sua equipe de forma segura.

A forma de criptografia utilizada pelo gerente de marketing da empresa XPTO é

A hash.

B criptografia de chave assimétrica.

C criptografia de chave simétrica.

D assinatura digital.

E certificado digital.

---

3. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã

Um dos mecanismos importantes de segurança é aquele que tenta solucionar o problema da autenticidade. A criptografia moderna procura resolver esse problema através dos algoritmos de criptografia assimétrica.

Para que isso ocorra,

A o emissor criptografa a mensagem com a chave pública do receptor e o receptor confirma a autenticidade decriptografando a mensagem usando sua própria chave privada.

B o emissor gera um hash da mensagem e o envia para o receptor junto com a mensagem. O receptor recalcula o hash e o compara com o hash enviado, e se forem iguais, a autenticidade estará confirmada.

C o emissor gera um hash da mensagem e o criptografa com sua chave privada. Para confirmar a autenticidade, o receptor decriptografa o hash recebido usando a chave pública do emissor, e verifica se esse hash é o mesmo calculado da mensagem.

D o emissor e receptor compartilham uma chave para criptografar e assinar digitalmente o hash gerado da mensagem.

E o emissor criptografa a mensagem com o certificado digital do receptor e o receptor confirma a autenticidade usando o certificado digital do emissor.

---

4. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã

Analise as afirmativas abaixo sobre o algoritmo de criptografia assimétrica Diffie-Helmann:

I. Não é vulnerável a ataques "man-in-the-middle".

II. Pode ser utilizado tanto para assinatura digital quanto para geração de chave simétrica.

III. Pode ser usado de três maneiras diferentes: anônimo, estático e efêmero, sendo essa última considerada a maneira mais segura.

Está correto apenas o que se afirma em

A I.

B II.

C III.

D I e II.

E I e III.

---

5. FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados

Para preservar a integridade das evidências encontradas em uma perícia computacional, o perito utilizou hashes criptográficos, pois essas funções são consideradas uma impressão digital eletrônica do dado coletado. No entanto, o perito escolheu uma função de hash que não é mais considerada segura, pois pode ser calculada rapidamente e é particularmente vulnerável a colisões.

Essa função de hash, considerada atualmente insegura, seria a

A SHA-3.

B Blowfish.

C Whirlpool.

D MD5.

E DES.

---

6. FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados

Os desenvolvedores de um jogo eletrônico usaram uma criptografia simétrica baseada em cifras de bloco para proteger certas partes do jogo. Para verificar se a proteção estava adequada, contrataram um perito para análise de vulnerabilidades. O perito verificou que o modo de operação da cifragem em bloco usada não era seguro o suficiente, pois além de não possuir proteção de integridade, não era semanticamente seguro, pois mantinha padrões que existiam nos dados em claro.

O modo de operação da cifragem de blocos da criptografia simétrica usado no jogo é o

A CBC (Cipher Bloco Chaining).

B ECB (Electronic Codebook).

C OFB (Output Feedback).

D CFB (Cipher Feedback).

E CTR (Counter).

---

7. FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados

O modo de operação de cifra de bloco da criptografia simétrica, no qual o bloco de texto claro atual é usado diretamente na entrada do algoritmo e criptografado com a mesma chave, de tal forma que, como consequência disso, sempre produz blocos de texto cifrado iguais para blocos de texto claro iguais, é o

A Cipher Block Chainning (CBC).

B Cipher Feedback (CFB).

C Output Feedback (OFB).

D Counter (CTR).

E Electronic Codebook (ECB).

---

8. FGV - 2022 - PC-AM - Perito Criminal - 4ª Classe - Processamento de Dados

Sobre criptografia e compactação de arquivos, analise as afirmativas a seguir.

I. Todo arquivo criptografado está necessariamente compactado.

II. O processo de compactação usualmente explora a repetição de trechos e/ou padrões presentes no arquivo.

III. A compactação de arquivos de texto (.txt) alcança bons índices de compactação em relação a outros tipos de arquivos.

Está correto o que se afirma em:

A somente I;

B somente II;

C somente III;

D somente II e III;

E I, II e III.

---

9. FGV - 2021 - TCE-RO - Analista de Tecnologia da Informação - Desenvolvimento de Sistemas

Kátia, engenheira de segurança, recebeu de seu chefe uma mensagem a ser criptografada e enviada para uma das filiais da empresa em outro estado, de forma segura. A mensagem não é crítica para a empresa, logo o sistema de criptografia a ser utilizado pode ser computacionalmente simples. Kátia resolveu então usar uma cifra de transposição que não altera o conteúdo da mensagem, alterando apenas suas posições. Considerando que a chave utilizada foi MEGABUCK e o texto cifrado é

ISODAIAORPSOROPCUOCLSASMDSRENOLVOTIRCSMDTOIFROEEE RBUIATROSONOO

a alternativa que apresenta o texto em claro correto para o texto cifrado acima é:

A EMVIRTUDEDOSPROTESTOSOCORRIDOSLIBERAROSFUNCION ARIOSAPOSOALMOCO;

B EFETUARODEPOSITONACONTADAFILIALDERONDONIAHOJEIM PRETERIVELMENTE;

C ALTERARASFOLHASDEPAGAMENTOEDAROAUMENTOACORDA DONAREUNIAODEONTEM;

D TRANSFERIROFUNCIONARIOROBERTODODEPARTAMENTOBP ARAODEPARTAMENTOA;

E ENCAMINHARPOREMAILOPLANEJAMENTODEFERIASDODEPA RTAMENTOACADEMICO.

---

10. FGV - 2021 - TCE-RO - Analista de Tecnologia da Informação - Desenvolvimento de Sistemas

Na implementação de tabelas Hash, quando as chaves não são perfeitamente distribuídas, é preciso lidar com as potenciais colisões que ocorrem quando:

A o espaço de endereçamento é superior ao número de chaves armazenadas;

B duas ou mais chaves têm o mesmo índice na tabela;

C as chaves são exclusivamente numéricas;

D as chaves são exclusivamente alfanuméricas;

E há duplicação de chaves.

---

11. FGV - 2021 - TCE-RO - Analista de Tecnologia da Informação - Desenvolvimento de Sistemas

Uma técnica de criptografia largamente empregada para garantir segurança em transações digitais, que utiliza uma chave pública para ciframento de dados e uma outra chave privada para deciframento desses dados previamente cifrados, é:

A DES;

B AES;

C RSA;

D SHA;

E MD5.

---

12. FGV - 2018 - Prefeitura de Niterói - RJ - Analista de Políticas Públicas e Gestão Governamental - Gestão de Tecnologia

AES, RSA e RC4 são exemplos, respectivamente, de algoritmos de

A criptografia simétrica, de criptografia assimétrica e de dispersão criptográfica.

B criptografia simétrica, de criptografia assimétrica e de criptografia simétrica.

C criptografia simétrica, de criptografia de chave pública e de criptografia assimétrica.

D criptografia assimétrica, de criptografia simétrica e de criptografia assimétrica.

E criptografia assimétrica, de criptografia simétrica e de dispersão criptográfica.

---

13. FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e Comunicação

João quer enviar uma mensagem para Maria, mas assegurar que somente Maria será capaz de lê-la.

Então, João deve utilizar

A uma criptografia de chave pública e aplicar a chave-pública de Maria para fazer o ciframento da mensagem.

B uma criptografia assimétrica e aplicar a chave-privada de Maria para fazer o ciframento da mensagem.

C uma criptografia simétrica para fazer o ciframento da mensagem e não compartilhar a chave criptográfica.

D uma criptografia assimétrica para João colocar sua assinatura digital na mensagem.

E uma função de dispersão criptográfica para cifrar a mensagem e informar a Maria o algoritmo utilizado.

---

14. FGV - 2018 - Câmara de Salvador - BA - Analista de Tecnologia da Informação

Carlos é um analista de segurança. Ele pretende criptografar os dados dos servidores da sua empresa que possuem Windows Server 2012 como sistema operacional, protegendo-os contra roubos e acessos não autorizados, seja pela execução de ferramentas de ataque a software ou pela transferência do disco rígido do computador para outro computador.

A ferramenta por ele utilizada que reduz acessos não autorizados aos dados por meio do aperfeiçoamento das proteções de arquivo e sistema é o:

A AppLocker;

B BitLocker;

C Kerberos;

D NTLM;

E NTFS.

---

15. FGV - 2017 - ALERJ - Especialista Legislativo - Tecnologia da Informação

O protocolo SSL (Secure Sockets Layer) combina as criptografias assimétrica e simétrica para garantir a confidencialidade e a autenticidade na comunicação entre computadores na Internet. São exemplos, respectivamente, de algoritmos de criptografia assimétrica e simétrica:

A SHA e RSA;

B IDEA e SHA;

C RSA e MD5;

D AES e DES;

E RSA e IDEA.

***16.* (FCC – TRE-SP/Analista Judiciário – Análise de Sistemas/2017) Um Analista de Sistemas do TRE-SP utilizará, em uma situação hipotética, o recurso de assinatura digital para os documentos eletrônicos emitidos pelo Tribunal. O processo da assinatura digital compreende, inicialmente, o uso de __I__ para criar um resumo do documento, seguido da criptografia do resumo utilizando Chave __II__ . Finalmente, o autor do documento utiliza-se de __III__ para assinar o documento juntamente com o resultado da etapa anterior. As lacunas I, II e III são, correta e respectivamente, preenchidas por**

a) Certificado – Privada – Chave Pública

b) Hash – Privada – Certificado

c) Certificado – Pública – Chave Privada

d) Autenticação – Privada – Certificado

e) Hash – Pública – Chave Privada

---

17. (FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015) O técnico judiciário da área de TI do TRT da 3a Região deve escolher o esquema de criptografia mais adequado para a seguinte situação. Ele deve receber uma informação de forma segura, ou seja, criptografada, de outro Tribunal, mas não tem meios para enviar um código secreto (chave) de forma segura para aquele Tribunal. Nessa situação, o técnico deve utilizar o esquema de criptografia de chave

a) simétrica.

b) privada.

c) assimétrica.

d) unificada.

e) isolada.

---

18. (FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015) Um dos padrões de criptografia mais difundidos mundialmente é o Data Encryption Standard – DES. Atualmente ele é utilizado na forma denominada Triple DES, devido à fragilidade identificada no DES que utiliza uma chave com

a) 48 bits.

b) 56 bits.

c) 128 bits.

d) 84 bits.

e) 64 bits.

---

19. (FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015) Considere:

M = Mensagem

KS = Chave Secreta compartilhada

MACr = Código de Autenticação de Mensagem gerado pelo remetente

KPr = Chave pública do remetente

MACd = Código de Autenticação de Mensagem gerado pelo destinatário

KPd = Chave Pública do destinatário

Um resumo criptográfico pode ser usado para verificar a integridade de uma mensagem - se ela não foi modificada. Para garantir a integridade da mensagem e autenticar a origem dos dados, uma das formas é: o remetente, por meio de uma função hash e usando a M concatenada com

a) KS, gera um MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KS, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

b) KS, gera um MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KPr, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

c) KPr, gera um MACr que, juntamente com M é enviado por um canal seguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KPr, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

d) KPr, gera um MACr que, juntamente com M é enviado por um canal inseguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KS, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

e) KS e KPr, gera um MACr que, juntamente com M é enviado por um canal seguro ao destinatário. O destinatário separa a MACr de M e, usando M concatenada com a KPd, gera um MACd que é comparado com o MACr. Se forem iguais M é considerada autêntica.

---

20. **(FCC – TRE-RR/Analista Judiciário – Análise de Sistemas/2015) Um sistema de computador envia uma mensagem para um receptor, acompanhada de um resumo dessa mensagem cifrado com chave privada. O objetivo é garantir que o sistema receptor decifre o resumo com uma chave pública enviada pelo remetente, calcule um novo resumo com base na mensagem recebida e compare o resultado com a mensagem original para garantir a integridade. Essa função criptográfica é chamada:**

a) Criptografia pública cptu.

b) Criptografia privada cptp.

c) Resumo criptográfico hash.

d) Criptografia simétrica simt.

e) Resumo criptográfico gram.

---

21. (FCC – CNMP/Analista do CNMP – Suporte e Infraestrutura/2015) Em segurança da informação, a criptografia é a técnica que utiliza a cifragem e, frequentemente, uma chave criptográfica para transformar a informação original para que apenas o interlocutor, ou as pessoas autorizadas, possam ler a informação original. Dentre as diferentes técnicas de criptografia atualmente utilizadas, a que utiliza o esquema de chave assimétrica é

a) AES.

b) DES.

c) RSA.

d) IDEA.

e) RC4.

---

22. (FCC – TJ-AP/Analista Judiciário – TI/2014) Para fornecer confidencialidade com criptografia de chave simétrica, uma solução é usar a criptografia de chaves simétricas para a codificação da informação a ser transmitida e a criptografia de chaves assimétricas para o compartilhamento da chave secreta, neste caso, também chamada de chave de

a) hash.

b) autenticação.

c) Diffie-Hellman.

d) enlace.

e) sessão.

---

23. (FCC – TJ-AP/Analista Judiciário – TI/2014) Para prover segurança à rede sem fio da empresa, um especialista em segurança de redes adotou o padrão WPA2, que possui um método de criptografia mais forte e algoritmos mais rápidos que padrões anteriores. O WPA2 adota a criptografia

a) RC4 que permite chaves de 256 ou 512 bits

b) RC4 que permite chaves de 256 bits.

c) AES que permite chaves de 256 bits.

d) 3DES que permite chaves de 168 bits.

e) AES que permite chaves de 512 bits

---

24. (FCC – TJ-AP/Analista Judiciário – TI/2014) Um Analista de TI do Tribunal de Justiça recebeu a incumbência de planejar e implementar um esquema de criptografia de Chave Pública para a troca de informações entre as duas comarcas de Macapá. Dentre os diferentes algoritmos existentes, ele deve escolher o

a) AES.

b) RC6.

c) DES.

d) IDEA.

e) RSA.

---

25. (FCC – TRT – 1° Região (RJ)/Analista Judiciário – TI/2014) Um Analista em Tecnologia da Informação do TRT da 1ª Região deve escolher um algoritmo de criptografia assimétrica para os serviços de acesso à rede de computadores do Tribunal. O Analista deve escolher o

a) DES.

b) IDEA.

c) AES.

d) RSA.

e) RC4.

---

26. (FCC – TRF – 4ªRegião/Técnico Judiciário – TI/2014) Basicamente, um esquema de criptografia simétrica possui cinco itens que são:

a) texto claro, algoritmo de criptografia, chave secreta compartilhada emissor/receptor, texto codificado e algoritmo de decriptografia.

b) texto claro, algoritmo de criptografia, chave secreta do emissor, chave secreta do receptor e texto codificado.

c) algoritmo de criptografia, chave secreta do emissor, chave pública do receptor, texto codificado e algoritmo de decriptografia.

d) algoritmo de criptografia, chave pública do emissor, chave secreta do receptor, texto codificado e algoritmo de decriptografia.

e) texto claro, algoritmo de criptografia, chave pública compartilhada emissor/receptor, chave secreta do receptor e texto decodificado.

---

27. (FCC – TRT – 3ª Região(MG)/Técnico Judiciário – Área de TI/2015) Diversos recursos e ferramentas são utilizados para melhorar a segurança da informação, principalmente a transmissão de informações pela rede de computadores. Nesse contexto, o hash é utilizado para

a) gerar um conjunto de dados de tamanho fixo independentemente do tamanho do arquivo original.

b) criar uma chave criptográfica específica e personalizada para o arquivo a ser transmitido pela rede.

c) verificar a autenticidade da mensagem utilizando a chave simétrica gerada no processo de hashing.

d) armazenar, em um arquivo, e transmitir a chave assimétrica utilizada para criptografar os dados.

e) checar a veracidade de uma assinatura digital junto a uma Autoridade Certificadora.

---

28. (FCC – TRT – 18ª Região (GO)/Analista Judiciário – TI/2013) Observe as regras de um algoritmo de criptografia:

Para criptografar uma mensagem, fazemos: c = m^e mod n

Para descriptografá-la: m = c^d mod n

Onde: m = texto simples c = mensagem criptografada n = é o produto de dois números primos o par (e, n) = chave pública o par (d, n) = chave privada ^ = é a operação de exponenciação (a^b: a elevado à potência b) mod = é a operação de módulo (resto da divisão inteira) Este algoritmo é de domínio público e é amplamente utilizado nos navegadores para sites seguros e para criptografar e-mails.Trata-se do algoritmo.

a) simétrico DES - Data Encryption Standard.

b) simétrico AES - Advanced Encryption Standard.

c) assimétrico RSA - Rivest, Shamir and Adleman.

d) assimétrico AES - Advanced Encryption Standard.

e) simétrico RSA - Rivest, Shamir and Adleman.

GABARITO

Gabarito CESPE

1	C	15	E	29	C	43	C
2	B	16	C	30	C		
3	D	17	C	31	E		
4	C	18	E	32	C		
5	C	19	C	33	E		
6	C	20	X	34	E		
7	E	21	C	35	C		
8	C	22	E	36	E		
9	E	23	E	37	E		
10	C	24	C	38	C		
11	E	25	E	39	B		
12	E	26	C	40	E		
13	B	27	E	41	C		
14	E	28	E	42	E		

Gabarito Questões Complementares

1	B	15	E	29	E
2	C	16	E	30	D
3	C	17	E	31	A
4	C	18	E	32	A
5	D	19	C	33	C
6	B	20	A	34	
7	B	21	C	35	
8	D	22	C	36	
9	A	23	B	37	
10	B	24	A	38	
11	C	25	C	39	
12	B	26	C	40	
13	A	27	E	41	
14	B	28	C	42	

RESUMO

- **Criptografia:** é uma ciência que tem como objetivo "embaralhar" as informações.
  - Três métodos de cifragem:
    - ✓ **Substituição** - é um método de codificação que busca alterar um caractere, símbolo ou dado em algum outro.
    - ✓ **Transposição** - foca no simples embaralhamento das letras segundo alguma rotina.
    - ✓ **Esteganografia** - tem como objetivo esconder uma mensagem dentro de outra.
  - **Cifragem de Bloco – Cipher Block**
    - ✓ **Eletronic Code Book – ECB -** É uma técnica não randômica pela simples concatenação dos blocos resultado da fragmentação da mensagem original.
    - ✓ **Cipher Block Chaining – CBC -** É o método mais utilizado. Utiliza a operação XOR devidamente representada na imagem a seguir pelo círculo em volta do sinal de "+".
    - ✓ **Cipher FeedBack – CFB -** Suporta qualquer tamanho de entrada, independentemente do bloco. Por esse motivo, se torna útil para aplicações que dependem de transmissão imediata.
  - **Cifragem de Fluxo – Stream Cipher**

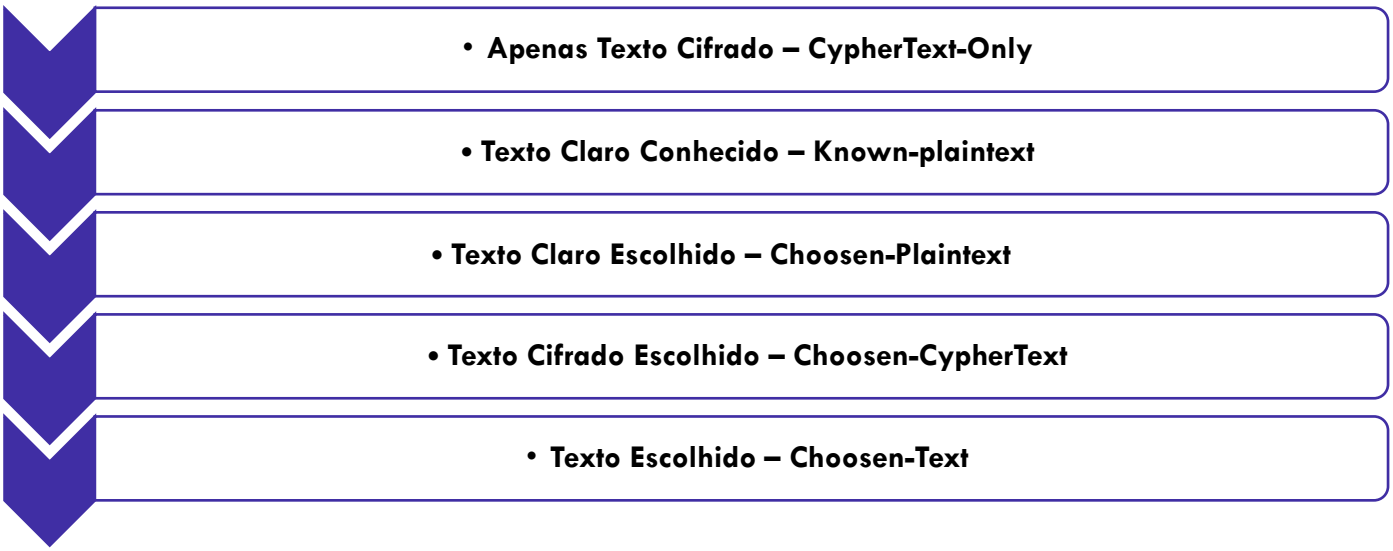
- ✓ A cifra de fluxo não necessita aguardar o processamento de toda a mensagem para se aplicar o algoritmo. A ideia é ser algo mais dinâmico e ágil de tal forma que, à medida que os dados vão chegando, vai se aplicando o algoritmo de forma contínua.

- **Identificação de Dados Criptografados**

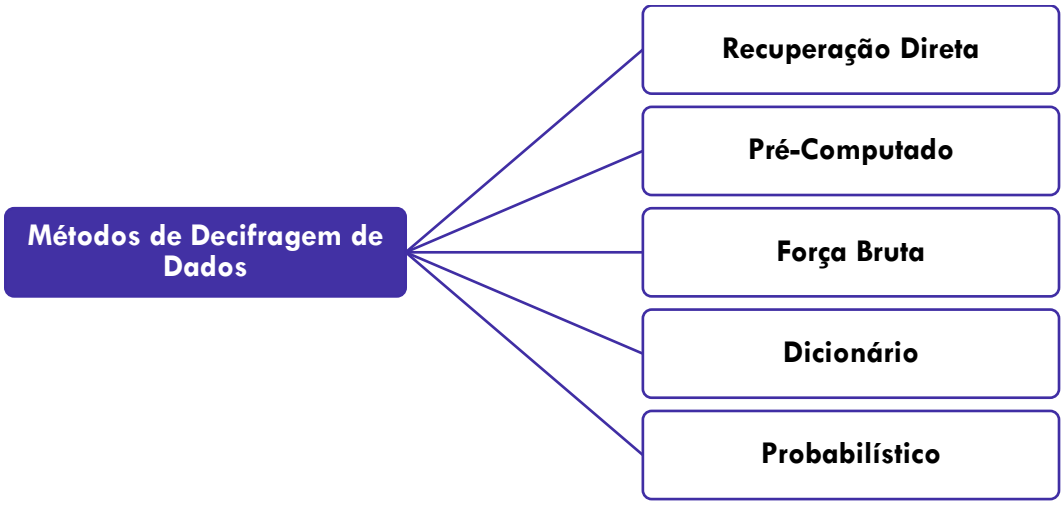
  - ✓ **Arquivos Criptografados -** criptografia aplicada somente ao conteúdo de determinados arquivos.
  - ✓ **Discos Virtuais Criptografados -** utiliza-se um arquivo-contêiner devidamente criptografado em que, a partir da sua decriptação, gera-se um disco virtual com sistema de arquivos próprio. Cria-se uma unidade de disco acessível no sistema de arquivos.
  - ✓ **Discos Completamente Criptografados -** todo o sistema de arquivos e sistema operacional estão devidamente criptografados.

- **Criptoanálise**

  - A criptoanálise tem foco no entendimento de como funciona o algoritmo de criptografia.



- **Métodos de Decifragem de Dados**



- **Criptografia Simétrica**

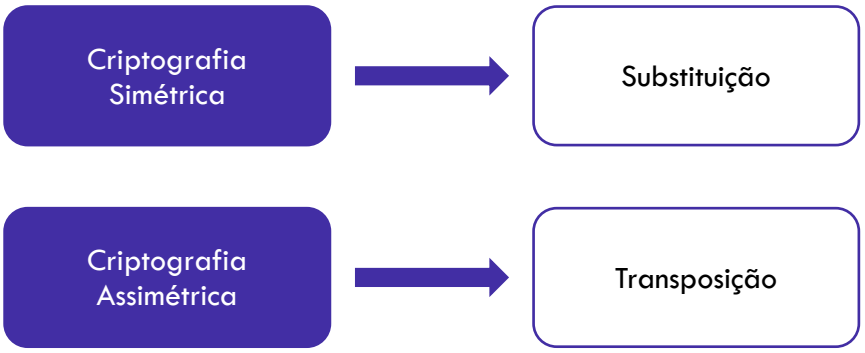
  - A criptografia simétrica possui como princípio o fato de se utilizar a mesma chave para o procedimento de criptografia e descriptografia.

  - Visa garantir apenas o princípio da confidencialidade.
  - Principais algoritmos de criptografia simétrica:
    - ✓ DES
    - ✓ 3DES
    - ✓ AES

- **Criptografia Assimétrica**

  - ✓ Também conhecida como criptografia de chaves públicas é caracterizada pelo fato de se utilizar duas chaves no processo criptográfico, ou seja, caso seja utilizada uma para criptografar os dados, deve-se, necessariamente, usar a outra para descriptografar.

  - ✓ O processo de criptografia de chave pública não se restringe a uma única sequência, isto é, não necessariamente se criptografa com a chave privada e decriptografa com a pública.



  - Principais algoritmos de criptografia simétrica:

    - ✓ Diffie-Hellman – DH
    - ✓ Rivest,Shamir and Adelman – RSA
    - ✓ El Gamal

- **Funções HASH**

  - São algoritmos criptográficos unidirecionais.
  - Funções matemáticas que permitem gerar um resultado de tamanho fixo independentemente do tamanho do conteúdo de entrada.
  - Aplicações das funções HASH são para garantir os princípios de integridade, autenticidade e confidencialidade.
  - Ataques de Colisão
  - Ataque de Aniversário
  - Algoritmos de HASH:

    ✓ MD5
    ✓ MD4
    ✓ SHA

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.