TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 16. Hacking Wireless Networks

Módulo 17. Hacking Mobile Applications

Módulo 18. IoT & OT Hacking

Módulo 19. Cloud Computing

Módulo 20. Cryptography

Conceitos de Criptografia:

Todo mundo tem segredos, e quando é necessário transferir essa informação secreta de uma pessoa para outra, é muito importante proteger essas informações durante a transferência. A criptografia faz com que textos simples sejam transformados em uma forma ilegível (texto cifrado) com a finalidade de manter a segurança dos dados que estão sendo transferidos.

Ele usa uma chave para transformar o texto cifrado de volta em dados legíveis quando a informação chega ao seu destino. A palavra criptografia é derivada da palavra grega kryptos. Kryptos foi usado para descrever qualquer coisa que foi ocultada, escondida, velada, secreta ou misteriosa. Graph é derivado de Graphia, o que significa escrita, portanto, criptografia significa a arte da "escrita secreta".

CEHv12 (ANSI)

20.Cryptography

A LONG, LONG TIME AGO...

“Por milhares de anos, reis, rainhas e generais confiaram em comunicações eficientes para governar seus Países e comandar seus Exércitos. Ao mesmo tempo, todos estavam cientes das consequências de suas mensagens caírem em mãos erradas, revelando preciosos segredos para Nações rivais e informação vital para forças oponentes. Foi a ameaça de interceptação inimiga que motivou o desenvolvimento de códigos e cifras: técnicas para disfarçar uma mensagem de modo que somente o destinatário pudesse lê-la.”

The Code Book

Criptografia do dia a dia

Prof. Keith Martin is Director of the Information Security Group at Royal Holloway, University of London and author of Everyday Cryptography. An active member of the cryptographic research community, he also has considerable experience in teaching cryptography to non-mathematical students, including industrial courses and young audiences.

"(...) a vida moderna dificilmente seria imaginável sem as redes de dispositivos de computação de que agora dependemos. Conversamos, escrevemos, negociamos, depositamos, jogamos - tudo em computadores. Nosso mundo, que antes dependia da presença física e dos limites para sua segurança, agora é um mundo digital aberto. Sem as devidas precauções, nunca podemos ter certeza, por exemplo, de quem está levando nosso dinheiro online, quanto está realmente levando e quem pode estar ouvindo. É assustador, se você pensar sobre isso por muito tempo.
A boa notícia é que esse mundo digital pode se tornar seguro por meio do uso de, adivinhem? Criptografia!"

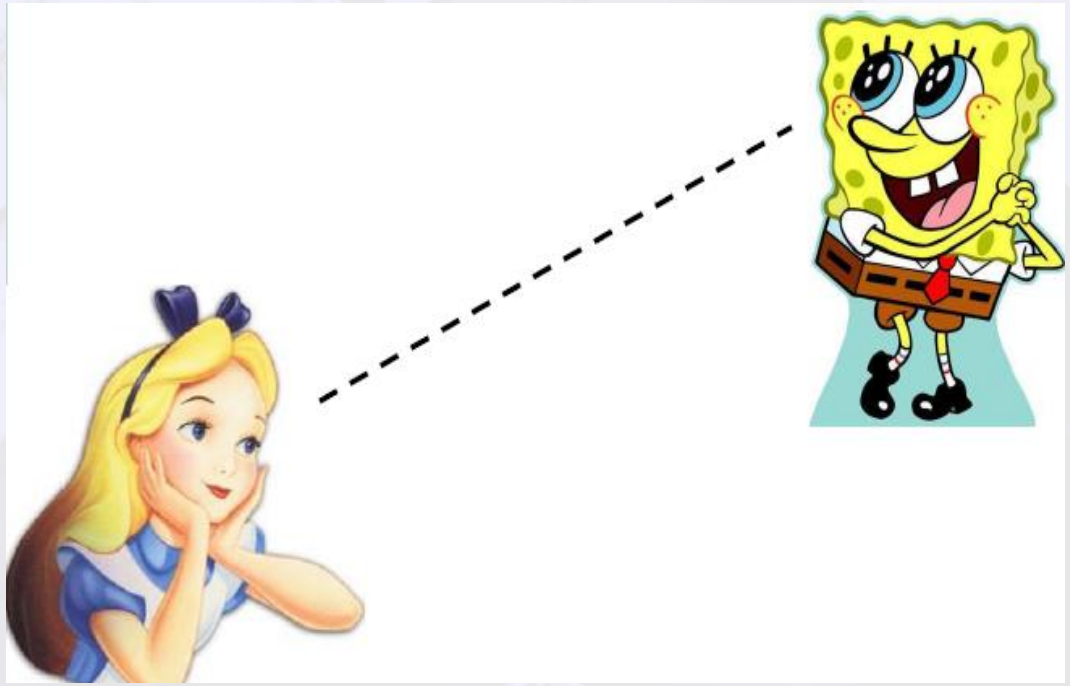
Criptografia do dia a dia

Keith M. Martin

Visão Geral

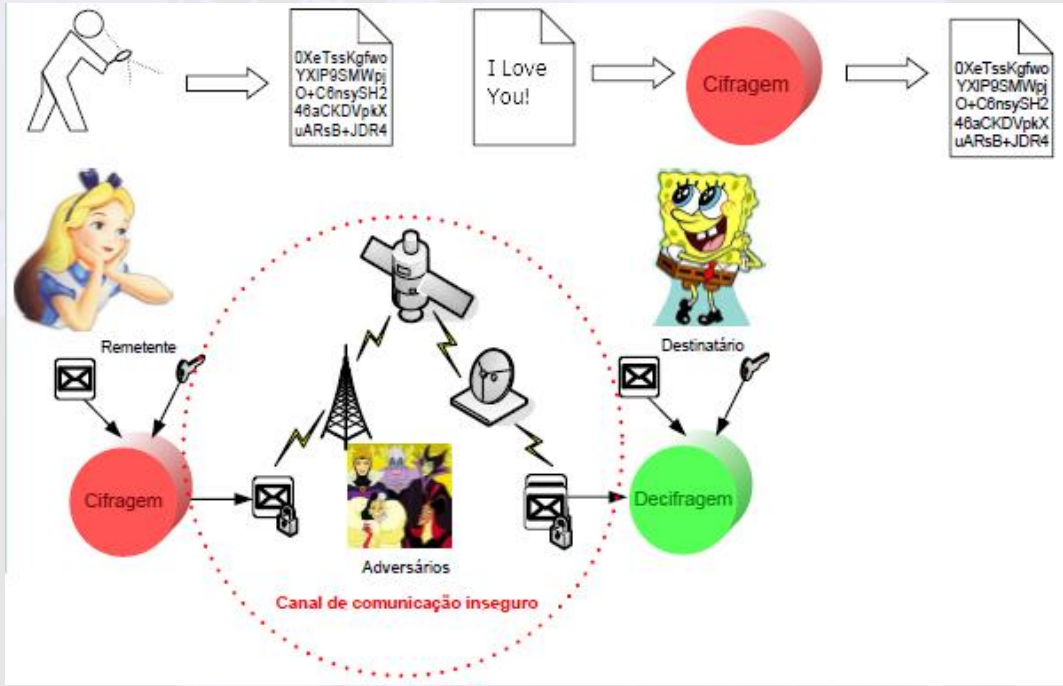
CRIPTOGRAFIA

- Armazenar e transmitir
- Somente pessoas autorizadas



CRIPTOANÁLISE

- Decifrar mensagem
- Recuperar chave
- Redução de esforço



ALGUNS SINÔNIMOS

Algoritmo criptográfico: cifra, cifrador

Cifragem: cifração

Texto legível: texto em claro, texto plano, mensagem

Texto cifrado: texto criptografado, texto ilegível, criptograma

Criptografia simétrica: criptografia de chave secreta

Criptografia assimétrica: criptografia de chave pública

ALGUMAS DEFINIÇÕES

Algoritmo Criptográfico: conjunto de regras matemáticas usadas para cifrar e decifrar.

Criptoanálise: busca obter o conhecimento do texto legível ou da chave utilizada para criptografar, sem o conhecimento desta chave. Busca também obter os parâmetros criptográficos.

Chave (key): Sequência secreta de bits (ou instruções) utilizada para cifrar e decifrar.

Agrupamento de chave (key clustering): caso em que duas chaves diferentes geram o mesmo texto cifrado a partir do mesmo texto claro.

Espaço de chaves (keyspace): uma coleção de possíveis valores a partir dos quais podem ser construídas as chaves.

Texto claro (plaintext): informação em um formato legível.

Texto cifrado (ciphertext): informação em formato ilegível.

Fator de trabalho (work factor): tempo, esforço e recursos necessários estimados para quebrar um sistema criptográfico.

SERVIÇOS DE SEGURANÇA

SIGILO (CONFIDENCIALIDADE)

Garantia de que apenas os usuários (ou processos) autorizados tenham acesso à informação.

AUTENTICIDADE

Garantia da identificação correta dos participantes da informação.

INTEGRIDADE

Garantia de que a informação original não sofreu alteração.

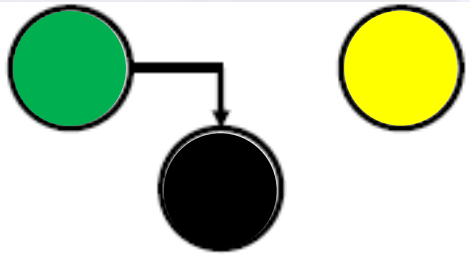
DISPONIBILIDADE

Garantia de que as informações armazenadas em um sistema de informações ou transmitidas via rede de computadores possam ser acessadas por usuários legítimos quando estes o desejarem.

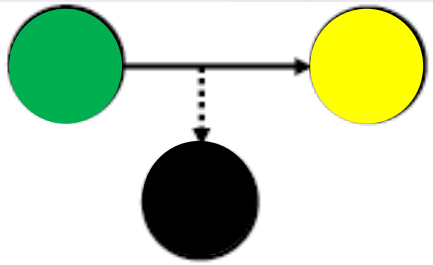
NÃO-REPÚDIO

Garantia de que os participantes não possam negar ação anterior da qual participaram.

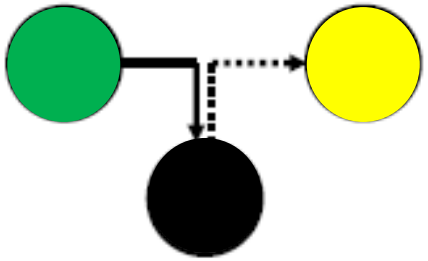
ATAQUES



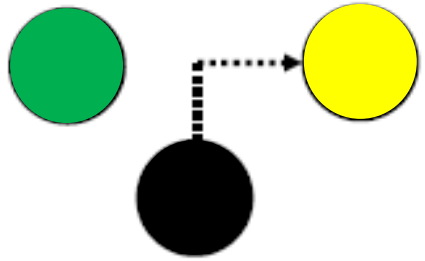
Bloqueio/Interrupção
(ataque contra a disponibilidade)



interceptação
(ataque contra o sigilo)



Falsificação/Modificação
(ataque contra a integridade)



Personificação/Fabricação
(ataque contra a autenticação)

ESQUEMA DE CRIPTOGRAFIA

Notações

m: texto claro (plaintext)

c: texto cifrado (ciphertext)

k: chave criptográfica (key)

E: algoritmo de cifração

D: algoritmo de decifração

$$Ek(m) = c$$

$$Dk(c) = m$$

$$Dk(Ek(m)) = m$$

TENTANDO ADVINHAR A SENHA

"busca exaustiva offline" – atacante já obteve acesso a um banco de dados, mas ele está cifrado (Média 500.000 senhas/segundo)

Tamanho da senha	Minúsculas	+ Maiúsculas	+ Números e Símbolos
6 caracteres	10 minutos	10 horas	18 dias
7 caracteres	4 horas	23 dias	4 anos
8 caracteres	4 dias	3 anos	463 anos
9 caracteres	4 meses	178 anos	44.530 anos

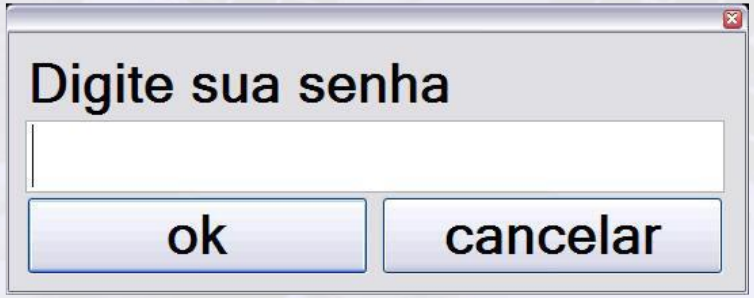
Fonte: Revista Businessweek

Em uma "busca exaustiva online", o atacante não teve acesso ao banco de dados; ele tem apenas acesso à tela de login. Nesse tipo de ataque, é raro se conseguir velocidade maior do que algumas centenas de tentativas por segundo (os números na tabela acima teriam de ser muito maiores).

LIMITANDO O Nº DE TENTATIVAS

> 3 erros (mesmo username) = bloqueio (proteção contra busca exaustiva)

Sujeito à ataque de Negação de Serviço



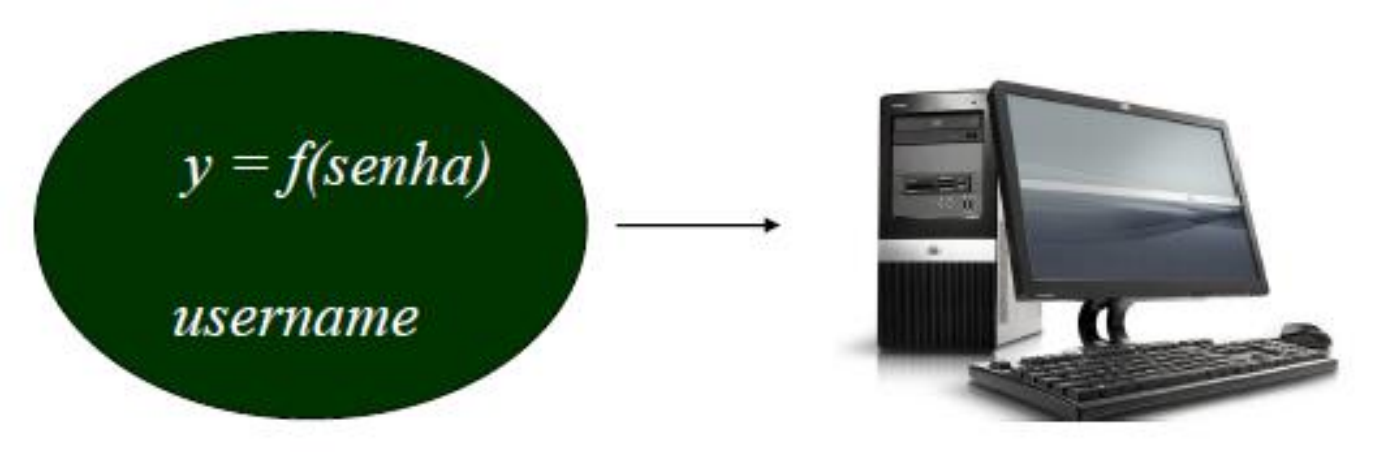
NA PRÁTICA ...

Grande parte dos usuários utilizam senhas "simples", baseadas em palavras comuns (“disnei123”);
Nomes de parentes, namorado(a), marido/esposa, filhos, bichos de estimação, lugares, números simples ("123456", "111111", entre outros), datas de nascimento, placas de carro e números de telefone são os mais comuns;
Daí a existência do chamado "ataque de força bruta por dicionário".
Um ataque por dicionário mais elaborado é capaz de descobrir também variações de textos legíveis (P@sS0Rd, CR1pT0gr@fI@, ...)

As senhas mais robustas são aquelas que, além de serem compostas de maiúsculas, minúsculas, números e caracteres especiais, são também o mais próximas possível de um string aleatório(ex. 63Ivj7>yQ$`84W)

AUTENTICAÇÃO DE USUÁRIO

Login: Computa f(senha) e compara com armazenado
y = f(senha) deve ser uma função unidirecional.
Normalmente, f é uma função Hash.
Atenção: Recuperação de senha por e-mail !!!!!



FORÇA DE UM CRIPTOSSISTEMA

Algoritmo + Sigilo da chave + Tamanho da chave

Algoritmo robusto:
Corretamente implementado (livre de backdoors)
Chave de tamanho apropriado.
Quebra total de um sistema criptográfico:
Descobrir a chave!!

- Força bruta.
- Quanto tempo para descobrir?
- Compartilhamento e exposição da chave.
- Qual é o elo mais fraco?

SEGURANÇA DOS ALGORITMOS CRIPTOGRÁFICOS

Incondicionalmente Seguro

- Impossível de ser quebrado, mesmo com recursos ilimitados
- Não há informação suficiente para determinar de maneira única o par chave/texto claro

Comprovadamente Seguro

- Pode ser provado que a quebra do algoritmo é equivalente a resolução de um problema que seja computacionalmente intratável

Computacionalmente Seguro

- Não pode ser quebrado com os recursos computacionais disponíveis
- É o nível de segurança mínimo buscado pelos criptógrafos

Suficientemente Seguro

- O custo para quebrá-lo é maior que o valor da informação protegida
- Muito utilizado, por ser rápido ou barato

Tipos de Criptografia

Symmetric Encryption

Symmetric encryption (secret-key, shared-key, and private-key) **uses the same key** for encryption as it does for decryption

Asymmetric Encryption

Asymmetric encryption (public-key) **uses different encryption keys** for encryption and decryption. These keys are known as public and private keys

Tipos de Criptografia

Criptografia Simétrica

O método de criptografia simétrica utiliza a mesma chave para a criptografia e descriptografia. O remetente utiliza uma chave para criptografar o texto simples e envia a mensagem cifrada para o receptor. O receptor descriptografa o texto cifrado com a mesma chave que é utilizada para criptografia e lêr a mensagem em texto simples.

Como uma única chave secreta é utilizada neste processo de criptografia simétrica, esse processo também é conhecido como criptografia de chave secreta. Este tipo de criptografia funciona bem quando você está se comunicando com apenas algumas pessoas.

O problema com a chave secreta é transferi-la através da Internet, evitando que ela caia em mãos erradas. Neste processo, qualquer pessoa que conheça a chave secreta pode descriptografar a mensagem. Este problema pode ser corrigido pela criptografia assimétrica.

Tipos de Criptografia

Criptografia Assimétrica

A criptografia assimétrica utiliza chaves diferentes para criptografia e descriptografia. Neste tipo de criptografia, um usuário final em uma rede pública ou privada tem um par de chaves: uma chave pública para a encriptação e uma chave privada para a decodificação. Aqui a chave privada não pode ser derivada da chave pública.

Os métodos de criptografia assimétrica tem sido seguro contra atacantes. Na criptografia assimétrica, o emissor codifica a mensagem com a ajuda de uma chave pública e o receptor descodifica a mensagem usando uma chave aleatória gerada pelo remetente da chave publica.

Tipos de Criptografia

DES

DES é o nome do Federal Information Processing Standard (FIPS) 46-3 que descreve o algoritmo de encriptação de dados (DES). **É um sistema de criptografia simétrica concebido para ser executado em hardware e usado para criptografia de usuário único, como armazenar arquivos em um disco rígido de forma criptografada.**

O DES dá 72 quatrilhões ou mais chaves de criptografia possíveis e escolhe uma chave aleatória para cada mensagem a ser encriptada. Embora o DES seja considerado uma criptografia forte, no momento, o DES tripo é usado por muitas organizações. O DES triplo aplica três chaves sucessivamente.

AES

O Advanced Encryption Standard (AES) é um Instituto Nacional de Padrões e especificação de Tecnologia para a criptografia de dados eletrônicos. **Ele pode ser usado para criptografar informações digitais, como telecomunicações, financeiras e dados do governo**. O AES consiste em um algoritmo de chave simétrica, isto é, a criptografia e descriptografia são realizadas utilizando a mesma chave.

É uma cifra de bloco que funciona repetindo as etapas definidas várias vezes. Ela tem um tamanho de bloco de 128 bits, com tamanhos de chaves de 128, 192 e 256 bits, respectivamente, para AES-128, AES-192 e AES-256.

Tipos de Criptografia

RC4, RC5, RC6

RC4 – O RC4 é uma cifra de fluxo que Ronald Rivest designou para a RSA. É um fluxo de cifra de tamanho de chave variável com operações orientadas em byte e é baseada no uso de uma permutação aleatória. De acordo com algumas análises, o período de cifra é susceptível a ser maior que 10100.

DSA

Para cada byte de saída, de oito a dezesseis operações do sistema são utilizadas, o que significa que a cifra pode ser executada rapidamente em softwares. Analistas independentes tiveram um olhar atento e crítico sobre o algoritmo, e é considerado seguro. **Produtos como RSA SecurPC usam este algoritmo para criptografia de arquivos. O RC4 também é usado para comunicações seguras, como criptografia de tráfego, que protege sites com o protocolo SSL.**

RC5 – O RC5 é uma cifra de bloco conhecida por sua simplicidade. Ronald Rivest projetou. Este algoritmo tem um tamanho de bloco variável e tamanho de chave e um número variável de rodadas. As escolhas para o bloco de tamanho são de 32 bits, 64 bits e 128 bits. As iterações variam de 0 a 255, ao passo que os tamanhos das chaves têm uma faixa de 0 a 2040 bits. Ele tem três rotinas: chave de expansão, criptografia e descriptografia.

RC6 - É uma cifra de bloco que se baseia no RC5. Como no RC5, o tamanho do bloco, o tamanho da chave, e o número de rodadas são variáveis no algoritmo RC6. O tamanho de chave varia de 0 a 2040 bits. Em comparação com o RC5, o RC6 tem mais duas características, que são a adição de multiplicação inteira e o uso de quatro 4-bits de registradores como uma alternativa aos dois registos de 2-bits do RC5.

Tipos de Criptografia

DSA

Uma assinatura digital é um esquema matemático utilizado para a autenticação de uma mensagem digital. Digital Signature Algorithm (DSA) destina-se a sua utilização no Federal Information Processing Standard EUA (FIPS 186) chamado Digital Signature Standard (DSS). **O DSA foi realmente proposto pelo Instituto Nacional de Padrões e Tecnologia (NIST)** em agosto de 1991. O NIST fez a patente EUA 5.231.668 que cobre DSA disponíveis em todo o mundo livremente. **É o primeiro esquema de assinatura digital reconhecido por qualquer governo.**

RSA

O RSA é um sistema de criptografia de chave pública. Ele usa aritmética modular e as teorias dos números elementares para executar cálculos usando dois grandes números primos. **A criptografia RSA é amplamente utilizada e é de fato o padrão de criptografia.**

Ron Rivest, Adi Shamir e Leonard Adleman formularam o RSA, um sistema de criptografia de chave pública para criptografia e autenticação. **Ele geralmente é usado com um sistema de criptografia de chave secreta, como DES.** O sistema RSA é largamente utilizado em uma variedade de produtos, plataformas e indústrias. Muitos sistemas operacionais como Microsoft, Apple, Sun e Novell construíram os algoritmos RSA para as versões existentes. Ele também pode ser encontrado no hardware de telefones seguros, em placas de rede Ethernet, e em cartões inteligentes.

Tipos de Criptografia

MD5

É uma função hash que é uma transformação que aceita uma variável de qualquer tamanho como uma entrada e retorna uma cadeia de caracteres de um determinado tamanho. Os requisitos fundamentais para as funções de hash criptográficas são:

- Entrada de qualquer tamanho
- Saída de um tamanho fixo

O principal papel de uma função hash criptográfica é fornecer assinaturas digitais. As funções hash são relativamente mais rápidas do que os algoritmos de assinatura digital. Assim, a sua principal característica é a de calcular a assinatura do valor de hash do documento, que é menor do que o documento. Além disso, uma síntese pode ser utilizada publicamente sem mencionar o conteúdo do documento e a fonte do documento.

SHA

O algoritmo aceita uma mensagem de 264 bits de comprimento e uma mensagem de saída de 160 bits é produzida, que é concebido para complicar a busca do texto, que é semelhante ao dado de hash. O algoritmo é ligeiramente mais lento que o MD5, mas o resumo maior da mensagem a torna mais segura contra colisão de força bruta e ataques de inversão. A seguir estão as funções de hash criptográficas projetado pela Agência de Segurança Nacional (NSA):

SHA1 - SHA1 produz um resumo de 160 bits de uma mensagem com um comprimento máximo de (264-1) bits, e assemelha-se o algoritmo MD5.

SHA2 - SHA2 é uma família de duas funções de hash semelhantes, com diferentes tamanhos de bloco, ou seja, SHA-256 que utiliza palavras de 32 bits e SHA-512 que usa palavras de 64 bits.

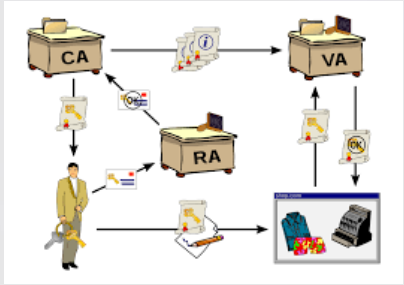
SHA-3 - SHA-3 é um padrão de função de hash futuro ainda em desenvolvimento, escolhido em um processo de revisão pública dos desenhadores não-governamentais.

Public Key Infrastructure - PKI

Public Key Infrastructure (PKI) é uma arquitetura de segurança desenvolvida para aumentar a confidencialidade das informações trocadas através da Internet. Ela inclui hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, distribuir, utilizar, armazenar e revogar certificados digitais.

Na criptografia, a PKI ajuda a ligar as chaves públicas com a identidade do usuário correspondente por meio de uma autoridade certificadora (CA). A seguir estão os componentes da PKI:

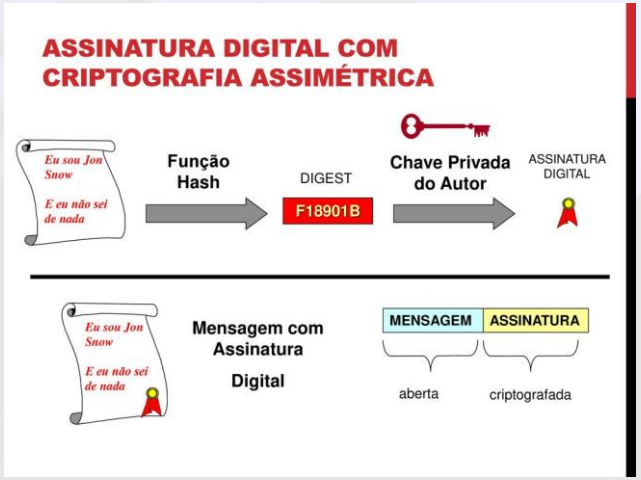
- Uma autoridade certificadora (CA) que verifica os certificados digitais.
- Um sistema de gestão de certificado para geração, distribuição, armazenamento e verificação dos certificados (VA).
- Um ou mais diretórios onde os certificados (com suas chaves públicas) são armazenados.
- A Autoridade de Registro (RA), que atua como o verificador da autoridade certificadora.
- As chaves criptográficas podem ser entregues com segurança entre os usuários pela PKI.



Assinatura digital

Uma assinatura digital é um método de autenticação de informação digital. A criptografia de chave pública, que utiliza um algoritmo de chave assimétrica, é usada para criar a assinatura digital. Os dois tipos de chaves na criptografia de chave pública é a chave privada e a chave pública. Uma função hash é um processo, ou um algoritmo, que é usado na criação e verificação de uma assinatura digital.

Este algoritmo cria uma representação digital de uma mensagem, que é também conhecido como uma "impressão digital". Esta impressão digital é um "valor de hash" de um comprimento padrão, que é muito menor do que a mensagem, mas é única para ele. Se qualquer alteração for feita na mensagem, isso irá produzir automaticamente um resultado hash diferente



SSL

SSL é acrônimo para Secured Sockets Layer desenvolvido pela Netscape. É um protocolo para o envio de documentos privados através da Internet. Ele funciona com a ajuda da chave privada para criptografar dados que são transferidos através de uma conexão SSL. O principal motivo por trás da elaboração do protocolo SSL é proporcionar privacidade entre dois aplicativos de comunicação, como um cliente e um servidor. Além disso, o protocolo é concebido para autenticar o servidor e o cliente, o SSL requer um protocolo de transporte de confiança tal como TCP para a transmissão e recepção de dados.

TLS

O TLS é um protocolo para estabelecer uma conexão segura entre um cliente e um servidor e garantir a privacidade e integridade das informações durante a transmissão. É um protocolo criptográfico destinado a fornecer a segurança da informação através da Internet. O TLS criptografa os segmentos de conexão de rede na camada de aplicação para a camada de transporte.

Ele usa criptografia assimétrica para troca de chaves, criptografia simétrica de confidencialidade, e códigos de autenticação de mensagens para a integridade da mensagem.

Conceitos de Criptografia:

Todo mundo tem segredos, e quando é necessário transferir essa informação secreta de uma pessoa para outra, é muito importante proteger essas informações durante a transferência. A criptografia faz com que textos simples sejam transformados em uma forma ilegível (texto cifrado) com a finalidade de manter a segurança dos dados que estão sendo transferidos.

Ele usa uma chave para transformar o texto cifrado de volta em dados legíveis quando a informação chega ao seu destino. A palavra criptografia é derivada da palavra grega kryptos. Kryptos foi usado para descrever qualquer coisa que foi ocultada, escondida, velada, secreta ou misteriosa. Graph é derivado de Graphia, o que significa escrita, portanto, criptografia significa a arte da "escrita secreta".

CEHv12 (ANSI)

20.Cryptography

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.