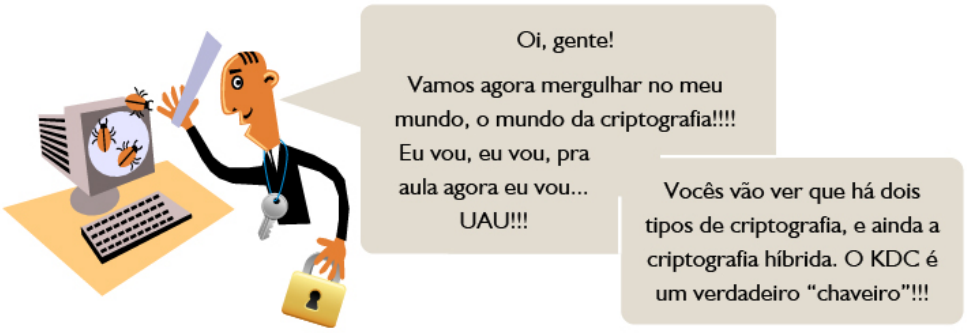
Segurança em Redes

Aula 03 - Criptografia

Apresentação



Nesta aula iremos estudar, mais detalhadamente, criptografia, seus tipos e centros de distribuição de chaves.

Vídeo 01 - Apresentação

Objetivos

- Diferenciar os tipos de criptografia.
- Distinguir os tipos de chave usados na criptografia.
- Conceituar criptografia simétrica e assimétrica.
- Conceituar um centro de distribuição de chaves (KDC).
- Saber utilizar a estratégia híbrida, com o uso da criptografia simétrica e assimétrica em conjunto.

Visão Geral

Você já sabe que existem vários mecanismos de segurança. Mas você sabia que grande parte deles usa criptografia? Por exemplo, as assinaturas digitais usam criptografia.

Ela ajuda a garantir confidencialidade, autenticidade, integridade e não repúdio. Lembra-se desses conceitos? Estudamo-los na aula passada.

Ainda recordando a aula passada, sobre os conceitos básicos de criptografia, **cifragem** é o processo de converter um texto original, comumente chamado de *plaintext,* para um texto cifrado ou criptografado, que é ilegível. A **decifragem** é o processo contrário, que recupera o texto original a partir de um texto cifrado.

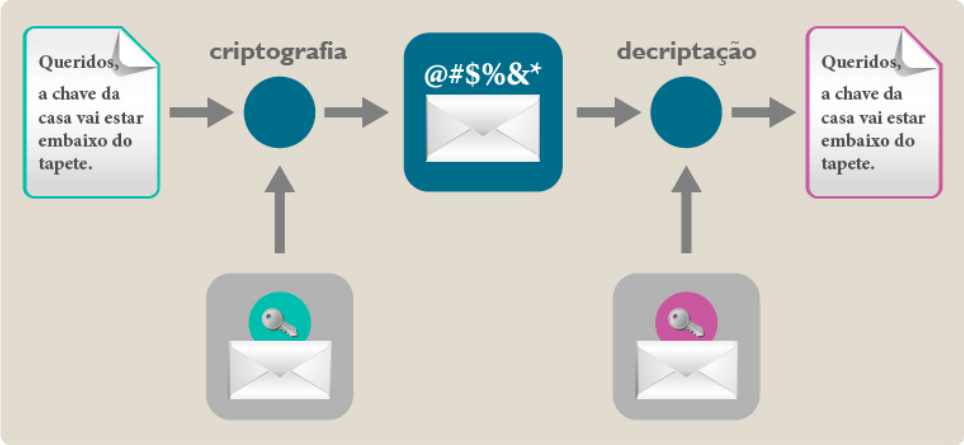
Há vários outros termos ligados à criptografia, tais como:

- **Criptologia**: estudo de tópicos das áreas de matemática, computação, psicologia etc., e técnicas relacionadas à criptoanálise.
- **Criptoanálise**: estudo de técnicas para se decifrar um texto sem conhecimento do método de criptografia ou da chave empregados.

Os algoritmos de criptografia e os processos de cifragem e decifragem são realizados com base em um algoritmo, e de outro parâmetro, a “chave criptográfica”. Os algoritmos de criptografia são públicos, estão disponíveis e podem ser utilizados por qualquer pessoa. Então, qualquer pessoa poderia aplicar o algoritmo em um texto cifrado e obter o texto original. Tem de haver algo, uma espécie de “senha”, que só seja conhecida pelo emissor e receptor do texto. Isso é justamente a chave, a única informação que se deve proteger.

Então, se Maria vai se comunicar com João, e eles querem manter o assunto em segredo, eles têm que compartilhar uma chave! Por exemplo, na Figura 1, a mensagem “Queridos, a chave da casa vai estar embaixo do tapete” foi criptografada e a chave foi utilizada como parâmetro do algoritmo de criptografia. O receptor decifra a mensagem cifrada usando o mesmo algoritmo usado para cifrá-la e também a mesma chave.

Figura 01 - Exemplo de criptografia.



A grosso modo, existem duas grandes classes de algoritmos de criptografia. A divisão é feita de acordo com o tipo de chave que eles utilizam:

- **Criptografia simétrica ou de chave secreta ou convencional**: nesse tipo de algoritmo, a cifragem e decifragem das mensagens são realizadas por uma única chave.
- **Criptografia assimétrica ou de chave pública**: nesses algoritmos, a cifragem e decifragem das mensagens são realizadas por chaves relacionadas, porém distintas.

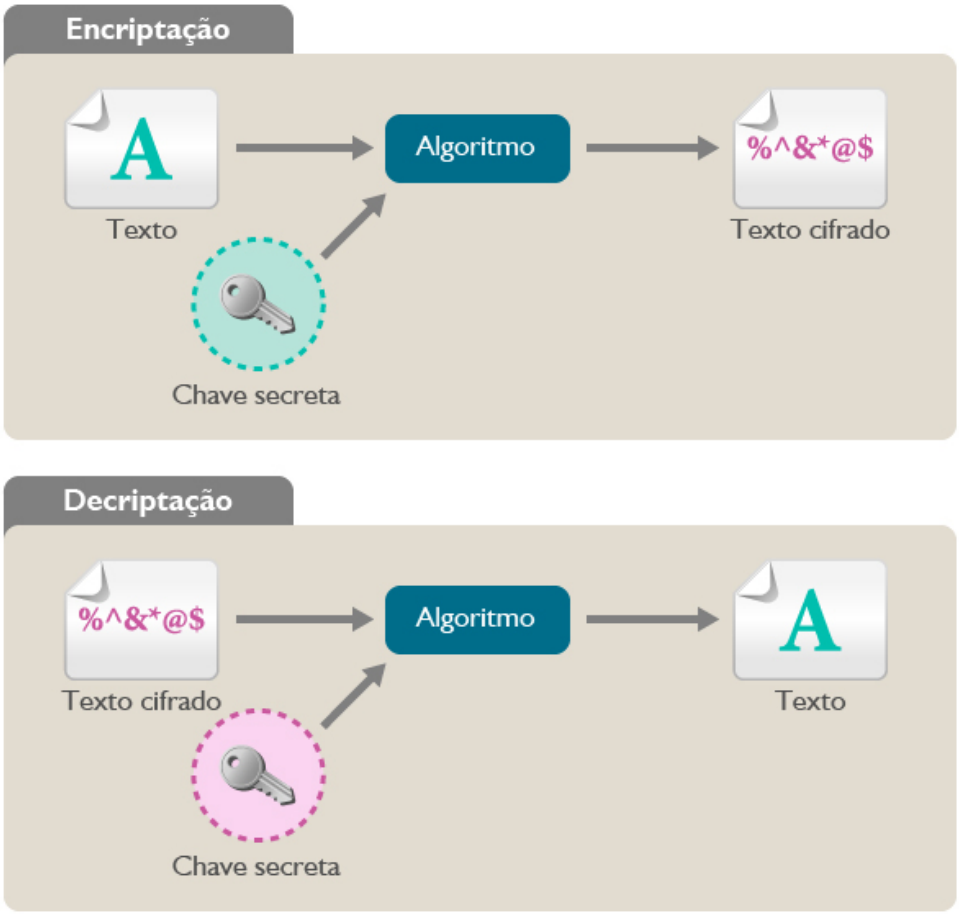
Atividade 01

1. Explique porque os algoritmos de criptografia são públicos.

Criptografia Simétrica

Os algoritmos simétricos utilizam uma mesma chave tanto para cifrar como para decifrar. A chave representa um segredo compartilhado entre duas ou mais partes, conforme mostrado no exemplo da **Figura 2**. A chave secreta – mostrada na figura – tem que ser a mesma, tanto para a cifragem quanto para decifragem.

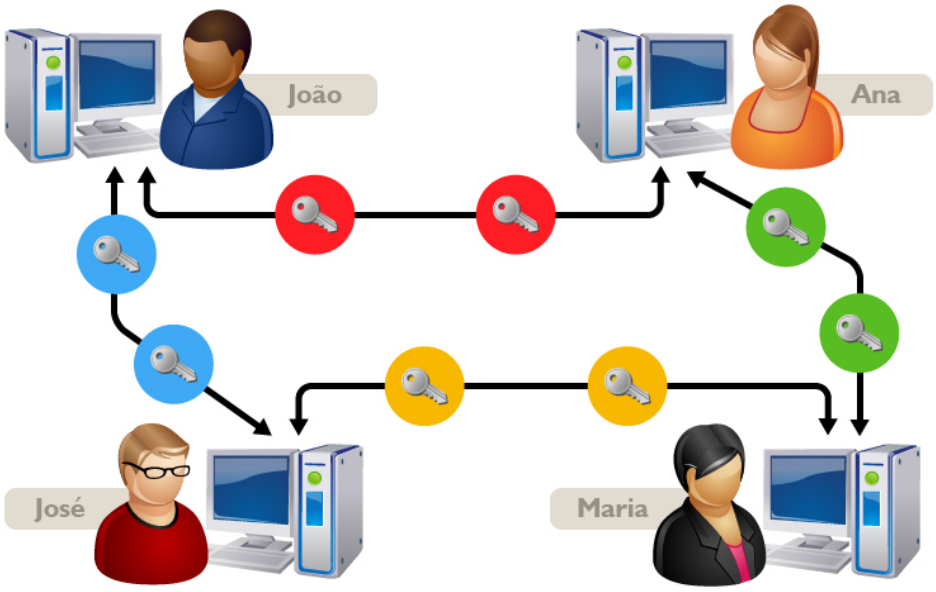
Figura 02 - Criptografia de chave secreta.



Por haver uma chave compartilhada, que deve ser mantida em segredo pelos dois ou mais parceiros da comunicação, para usar a criptografia simétrica, é necessário um canal, ou seja, uma forma segura para a troca de chaves entre as partes comunicantes. A necessidade de compartilhar um segredo com cada parceiro é a maior desvantagem da criptografia simétrica. Já que a transmissão das chaves entre os envolvidos pode não ser segura, e uma chave pode acabar caindo na mão de terceiros.

A **Figura 3** mostra outro problema da criptografia simétrica, conhecido como "problema da explosão de chaves". Nele cada usuário terá de armazenar e gerenciar o número de chaves de acordo com a quantidade de pessoas com as quais ele se comunica. Na Figura 3, João tem duas chaves compartilhadas, uma para se comunicar com Maria e uma para se comunicar com José. Se João quiser trocar mensagens com Ana de forma confidencial, ele terá de adquirir e gerenciar mais uma chave.

Figura 03 - Problema de explosão de chaves.



Portanto, dois grandes problemas precisam ser gerenciados na criptografia simétrica:

- Como transmitir a chave de forma confiável entre dois pontos de um sistema distribuído?
- Como administrar o problema de explosão de chaves?

Um exemplo simples de criptografia simétrica pode ser observado a seguir. Neste caso, temos um algoritmo bastantes simples que pode ser resumido por:

Para cada letra do alfabeto existente na mensagem original ou cifrada, realizar a sua substituição, conforme solicitado pela chave.

Neste caso, um possível exemplo de chave seria:

Letra:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Muda Para:	Y M R J U P T O V D X Z B S H F W C N G E I Q K A L

De posse do algoritmo e da chave, podemos realizar a cifragem, como no exemplo a seguir:

Texto original: "Haverá prova surpresa hoje à noite"

Texto cifrado: "OYIUCY FCHIY NECFCUNY OHDU Y SOIGU"

Depois de realizarmos a cifragem, podemos transmitir o texto cifrado para outra pessoa. Veja que, conforme estudamos há pouco, um aluno que conheça o algoritmo, e tenha interceptado o texto cifrado, nada poderá fazer, pois ele não possui a chave. Porém, se ele obtiver a mesma, ele saberá decifrar a mensagem e irá ler a mensagem original.

Alguns dos algoritmos mais conhecidos de criptografia simétrica são o DES (*Data Encryption Standard*); AES *(Advanced Encryption Standard)* e o IDEA (*International Data Encryption Algorithm*). Basicamente, todos eles trabalham com *bits* ao invés de letras do alfabeto, e, simplesmente, realizam centenas (ou milhares) de operações de substituição e permutação (onde dois *bits* são trocados de lugar), com base no algoritmo e na chave dada como entrada.

Um ponto importante para se analisar nos algoritmos de criptografia é o **tamanho da chave** que eles usam. Por exemplo, chave de 56 *bits*, de 64 *bits*, de 128 *bits* etc. Quanto maior a chave, mais difícil de descobri-la, ou seja, mais difícil de "quebrar a chave". Por quê? Por exemplo, uma chave de 8 *bits* gera apenas 256 combinações diferentes, pois esse é o resultado de 2ˆ8. Portanto, a chave de 8 *bits* não é muito segura. Uma chave de 256 *bits*, por exemplo, é mais difícil de quebrar, pois precisaria de muito mais esforço com um método de tentativa e erro.

Vídeo 02 - Criptografia Simétrica

Atividade 02

1. Você saberia dizer o motivo pelo qual as chaves são secretas, mas os algoritmos não?

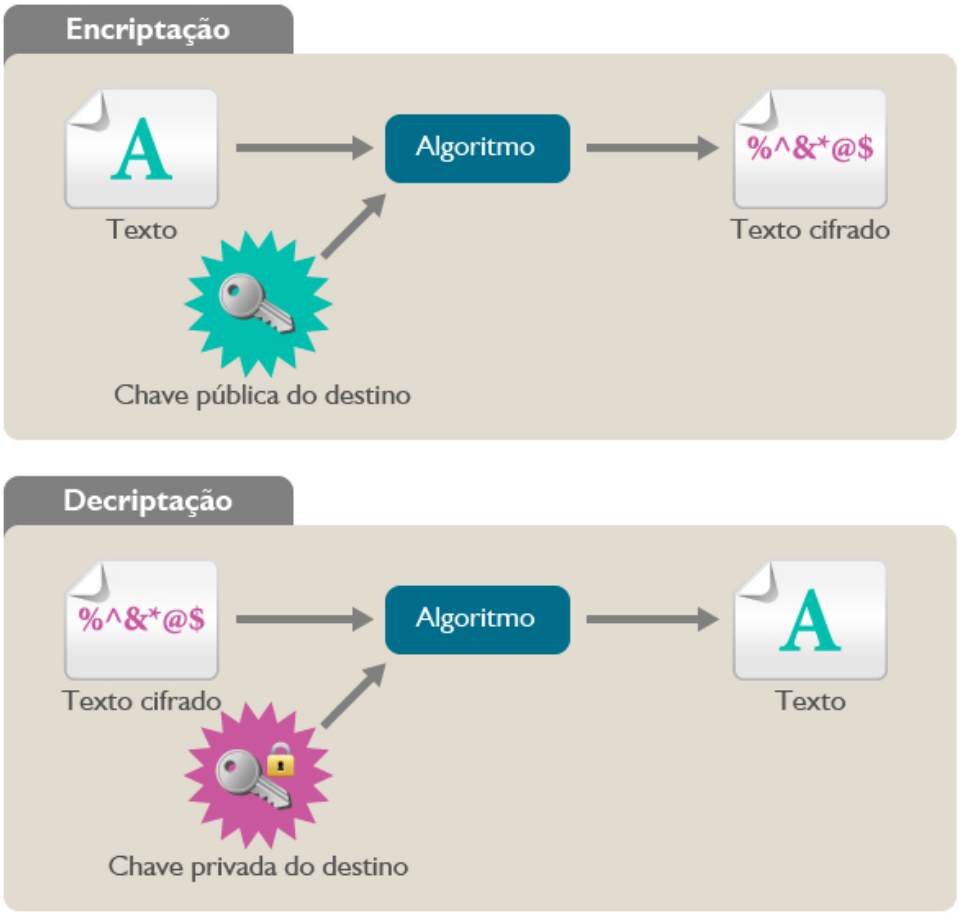
Criptografia Assimétrica

Os algoritmos assimétricos usam chaves relacionadas, porém distintas, uma para cifrar e outra para decifrar. Além disso, a chave usada para decifrar não pode ser obtida a partir do conhecimento da chave de cifragem. Nos algoritmos assimétricos, as chaves são sempre geradas aos pares: uma para cifrar e a sua correspondente para decifrar.

A chave usada para cifrar a mensagem é dita **pública**, e pode ser divulgada para o transmissor da mensagem. A chave usada para decifrar a mensagem é dita **privada**, ou seja, é um segredo pertencente ao receptor. Como o nome já diz, a chave pública é distribuída livremente. A chave privada, por sua vez, é a única capaz de decifrar uma mensagem cifrada com a chave pública correspondente. Ou seja, somente o receptor é capaz de decifrar o que qualquer pessoa o envia. Dessa forma, cada usuário tem uma chave pública e uma chave privada.

A **Figura 4** mostra o processo de cifragem e decifragem usando criptografia assimétrica. Na cifragem, o usuário origem usa a chave pública do destino como entrada do algoritmo de criptografia, juntamente com o texto original. Na decifragem, o usuário destino, ao receber o texto cifrado, usa sua chave privada – que somente ele conhece – como entrada do mesmo algoritmo de criptografia, para obter novamente o texto original.

Figura 04 - Criptografia Assimétrica



Como são usadas chaves diferentes, não existe o problema de manutenção e transmissão de chaves que existe na criptografia simétrica. No entanto, os algoritmos de criptografia assimétrica também possuem seus problemas. O principal deles e de desempenho, por eles exigirem um alto nível de processamento, que os torna, segundo Nakamura (2007), muito mais lentos do que os algoritmos simétricos. Isso faz com que uma estratégia bem interessante seja usar os dois tipos de algoritmos em conjunto, visando aproveitar os pontos fortes e reduzir, então, os pontos fracos de ambos os tipos de criptografia.

Os principais algoritmos de criptografia assimétrica são: RSA; Diffie-Helman e DSA. Dado sua complexidade, não iremos entrar em detalhes do seu funcionamento, contudo, existe uma imensa gama de informações sobre eles na internet.

Vídeo 03 - Criptografia Assimétrica

Atividade 03

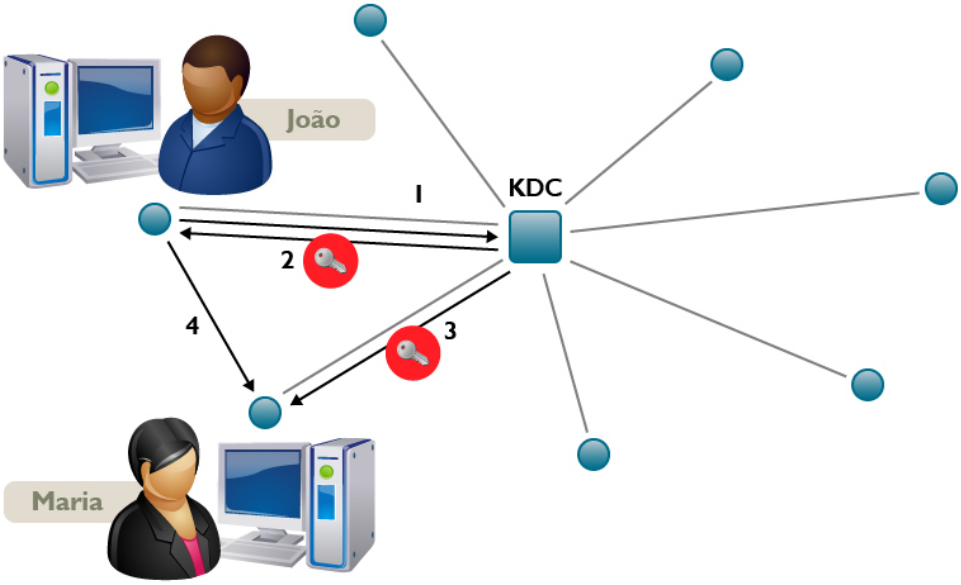
1. Faça um comparativo dos pontos fortes e fracos dos algoritmos simétricos e assimétricos.

Centro de Distribuição de Chaves (*KDC – Key Distribution Center*)

Vimos que na criptografia simétrica o grande problema é a distribuição das chaves secretas. A criptografia assimétrica não tem esse problema, mas, no entanto, como podemos obter, com certeza, a chave pública verdadeira de alguém (e não de um atacante disfarçado)? Os dois problemas: determinação de uma chave compartilhada para a criptografia simétrica e obtenção de uma chave pública confiável, para a criptografia assimétrica, podem ser solucionados usando-se um **intermediário confiável**, que pode ser chamado de **Centro de Distribuição de Chaves (KDC).**

Na criptografia assimétrica, o intermediário de confiança é chamado de autoridade certificadora (*certification authority – CA*). Uma CA certifica que uma chave pública pertence a uma determinada entidade (uma pessoa ou servidor, por exemplo). Se a CA é confiável, pode-se também confiar nas chaves que ela fornece. A chave pública “certificada” pode ser distribuída de qualquer lugar, como um servidor ou uma página Web pessoal. Nessa seção iremos nos concentrar no KDC, uma vez que teremos outra aula exclusivamente sobre autoridades certificadoras.

Figura 05 - Centro de Distribuição de Chaves (KDC).



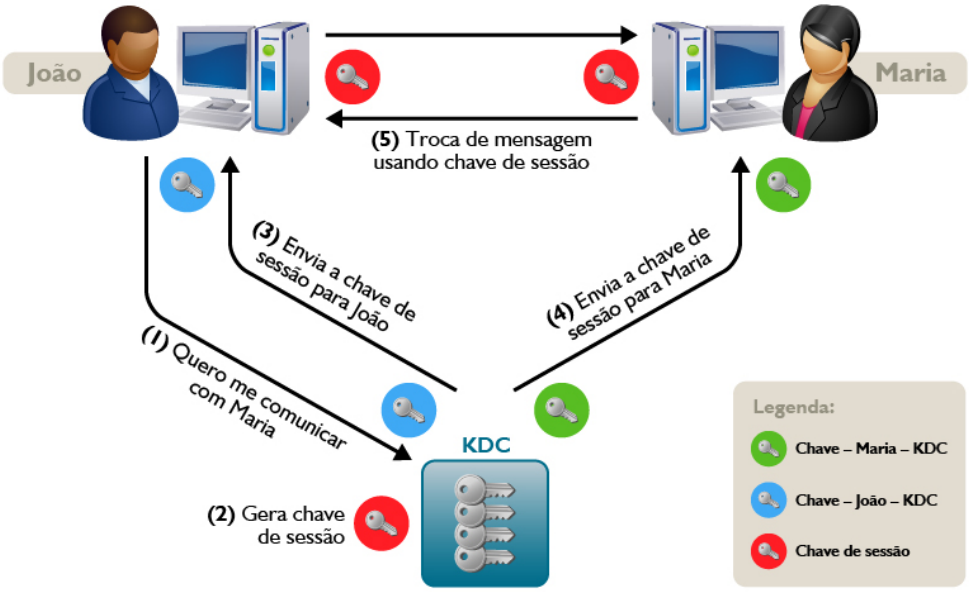
A **Figura 5** mostra duas pessoas, João e Maria, desejando se comunicar de forma segura. A seguinte sequência de ações acontece:

1. João pede, ao KDC, para se comunicar com Maria.
2. O KDC envia a chave a João.
3. O KDC envia a mesma chave a Maria.
4. A comunicação entre João e Maria acontece de forma segura, com os dados sendo cifrados com a chave que eles receberam.

Para garantir que quem está lhe dando a chave é mesmo o KDC, ele compartilha uma chave simétrica secreta diferente com cada um dos seus usuários registrados. Essa chave é criada pelo servidor, no momento que o usuário se registra pela primeira vez. O KDC conhece a chave secreta de cada usuário, e cada um deles pode se comunicar com segurança com o KDC usando sua chave. Mostraremos como dois usuários podem se comunicar de forma segura a seguir:

Se João e Maria são usuários do KDC, eles conhecem apenas a sua chave secreta com o KDC. Chamamos a chave de João com o KDC de *Chave-João-KDC*, e a chave de Maria com o KDC de *Chave-Maria-KDC*. Para se comunicar, então, João dá o primeiro passo, como ilustra a Figura 6:

Figura 06 - Comunicação usando o Centro de Distribuição de Chaves (KDC).



1. João, usando sua chave secreta com o KDC, diz que ele, João, quer se comunicar com Maria.

2. O KDC recebe a mensagem e tem certeza que ela vem de João, porque somente João tem a chave secreta (*Chave-João-KDC*) que eles compartilham.

3. O KDC decifra a mensagem e vê que João quer se comunicar com Maria. Em seguida, gera uma chave para tal comunicação, *(Chave-joão-maria)*. Tal chave é chamada de "chave de sessão", pois João e Maria vão usá-la apenas durante uma única sessão de comunicação. Agora o KDC precisa enviar a chave para João e Maria.

4. **Para enviar a chave para João**: o KDC cifra a chave de sessão *(Chave-joão-maria)* com a chave que compartilha com João, a *Chave-Joao-KDC*.

5. **Para enviar a chave para Maria**: o KDC cifra a chave de sessão *(Chave-joão-maria)* com a chave que compartilha com Maria, a *Chave-Maria-KDC*.

6. João e Maria recebem suas mensagens, decifram e obtêm a chave de sessão *(Chave-joão-maria)* para se comunicar. Toda mensagem que João mandar para Maria e que Maria mandar para João deve ser cifrada usando a chave de sessão.

Observe que com essa criptografia está se garantindo:

- **Confidencialidade**, pois apenas João e Maria podem decifrar as mensagens que são cifradas com a chave de sessão.

- **Autenticidade,** pois quando João recebe uma mensagem cifrada com *(Chave-joão-maria)*, ele sabe que é de Maria, já que apenas ela conhece essa chave. Da mesma forma, quando Maria recebe uma mensagem cifrada com *(Chave-joão-maria)*, ela sabe que veio de João.

- **Não Repúdio,** pois nem Maria nem João podem negar que foi um deles que enviou uma mensagem cifrada com *(Chave-joão-maria).*

Vídeo 04 - KDC

Estratégia Híbrida – Criptografia Simétrica e Assimétrica

A Criptografia híbrida, como o próprio nome já diz, consiste em unir a segurança da criptografia assimétrica com a velocidade de processamento da simétrica. Assim, são usadas tanto chaves públicas e privadas quanto as chaves de sessão. Quanta chave, hein? Pois é, precisamos trancar "muitas portas" para evitar que atacantes tenham sucesso, e queremos fazer isso de forma eficiente. Por isso a combinação dos dois tipos de criptografia. Em suma, a estratégia híbrida usa:

1. Criptografia assimétrica para distribuir a chave secreta, e simétrica de forma segura.

2. Criptografia simétrica para criptografar as informações em si, uma vez que os algoritmos são mais rápidos.

Funcionamento:

1. João quer se comunicar com Ana e, para isso, gera uma chave secreta de sessão. Essa é a chave a ser usada para encriptar as mensagens trocadas entre João e Ana. No entanto, Ana ainda não conhece essa chave. É preciso que João envie a chave para ela.

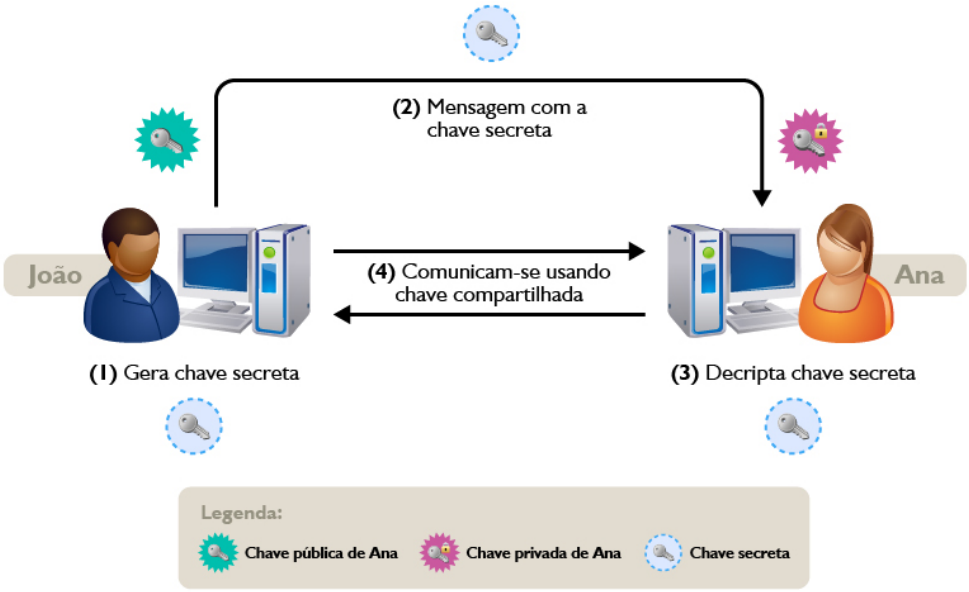
2. João manda uma mensagem para Ana, criptografada com a chave pública pertencente a ela, e contendo a chave se sessão.

3. Ana recebe a mensagem e a decifra com sua chave privada, obtendo a chave de sessão que vai ser usada para comunicação com João.

4. João e Ana se comunicam usando a chave de sessão que somente eles conhecem.

A **Figura 7** mostra o funcionamento da criptografia híbrida.

Figura 07 - Exemplo de criptografia híbrida.



Curiosidade

Em toda a história da humanidade, o desenvolvimento de métodos cada vez mais avançados de criptografia esteve ligado às guerras e à necessidade de se esconder informações de forças inimigas. Existem diversos exemplos a respeito disso, que você pode pesquisar na internet.

Talvez o maior expoente da criptografia com objetivos militares seja a "enigma", uma "máquina de escrever" usada pelo exército alemão durante a segunda guerra mundial, entre 1939 e 1945. Nessa máquina, além das teclas alfanuméricas, existia uma série de "rotores", que podiam ser ajustados para um valor, antes de se iniciar a digitação **(essa era a chave de seu algoritmo)**. Então, um digitador experiente digitava o texto original e o que aparecia no papel era completamente ilegível. Esse documento era enviado para o destino, onde outro digitador experiente ajustava o valor dos rotores para o mesmo valor, e digitava o texto ilegível. O que aparecia no papel era o texto original!

Apenas recentemente, com a disseminação da internet, e a necessidade de

proteger nossos dados pessoais, permitir as compras via internet etc., o uso da criptografia deixou de ter como "eixo principal" o militar.

Funções Hash

Vídeo 06 - Funções Hash

Leitura Complementar

Sobre criptografia:

http://www.infowester.com/criptografia.php

Sobre história da criptografia:

http://www.numaboa.com/criptografia/historia/156-historia

Pesquise

Você sabe o que é esteganografia?

Pesquise e elabore um texto explicando o assunto.

Resumo

Nesta aula você estudou os conceitos de criptografia simétrica e assimétrica. Também conheceu o KDC (Centro de Distribuição de Chaves) e sua aplicabilidade. Encerramos a nossa aula estudando como utilizar a estratégia híbrida, que aproveita vantagens da criptografia simétrica e assimétrica.

Autoavaliação

1. Qual o principal problema de se usar criptografia simétrica?
2. Quais as principais vantagens de se utilizar um KDC?
3. Qual a importância do tamanho da chave para os algoritmos de criptografia simétricos?
4. Coloque V (verdadeiro) ou F (falso):

a. O processo de cifragem é bastante lento na criptografia simétrica. ( )

b. Os algoritmos de criptografia não são secretos, podendo ser divulgados. ( )

c. Na criptografia assimétrica, cada usuário possuirá vários pares de chaves publicas/privadas. ( )

d. Um tipo de KDC usado na criptografia assimétrica é chamado de CA. ( )

Referências

NAKAMURA, E.; GEUS, P. L. **Segurança em redes em ambientes cooperativos**. Rio de Janeiro.: Editora Novatec, 2007.

STALLINGS, W. **Cryptography and network security**: principles and practice. 5th ed. New York: Prentice Hall, 2010. 744 p.