Segurança da Tecnologia da Informação

UNIDADE 06

Criptografia simétrica e assimétrica

Nesta Unidade, iremos estudar os mecanismos de criptografia simétricos e assimétricos. Conheceremos os elementos fundamentais da criptografia simétrica. Ainda, iremos nos aprofundar nos principais algoritmos de criptografia simétrica, tais como o algoritmo DES, Triplo DES e AES. Adicionalmente, demonstraremos o processo de distribuição chave simétricas de forma segura. Na sequência, vamos apresentar os princípios de cifração assimétrica, os elementos envolvidos na criptografia de chave pública. Também, iremos apresentar os principais algoritmos de cifração de chave pública, o algoritmo RSA, Diffie-Hellman, DSS e as Curvas elípticas. Além de ressaltar as vantagens e desvantagens de cada tipo de criptografia, vamos mostrar as principais aplicações que utilizam estes dois tipos de criptografia, tais como assinatura digital, autenticação de mensagens, certificados de chave pública, envelopes digitais, entre outras. Estaremos também conhecendo o processo de

distribuição de chave pública de forma segura, utilizando diretórios de chave pública, anúncio público, autoridades e certificados de chave pública. Por fim, demonstraremos como associar diferentes algoritmos de criptografia para obter um mecanismo mais seguro.

Princípios de Cifração Simétrica

A cifração simétrica, também conhecida como criptografia de chave secreta, era o único tipo de método de cifração utilizado antes da inserção da criptografia de chave pública no final da década de 1970. Esse método de criptografia ainda continua sendo amplamente utilizado.

Para compreender a criptografia simétrica primeiramente vamos definir alguns termos fundamentais. A mensagem original é conhecida como **texto claro**, ao passo que uma mensagem codificada é denominada como **texto cifrado**. Neste sentido, a ação de modificar um texto claro em um texto cifrado é chamado de **cifração**; por sua vez o processo de restaurar o texto claro a partir do texto cifrado é conhecido como **decifração**.

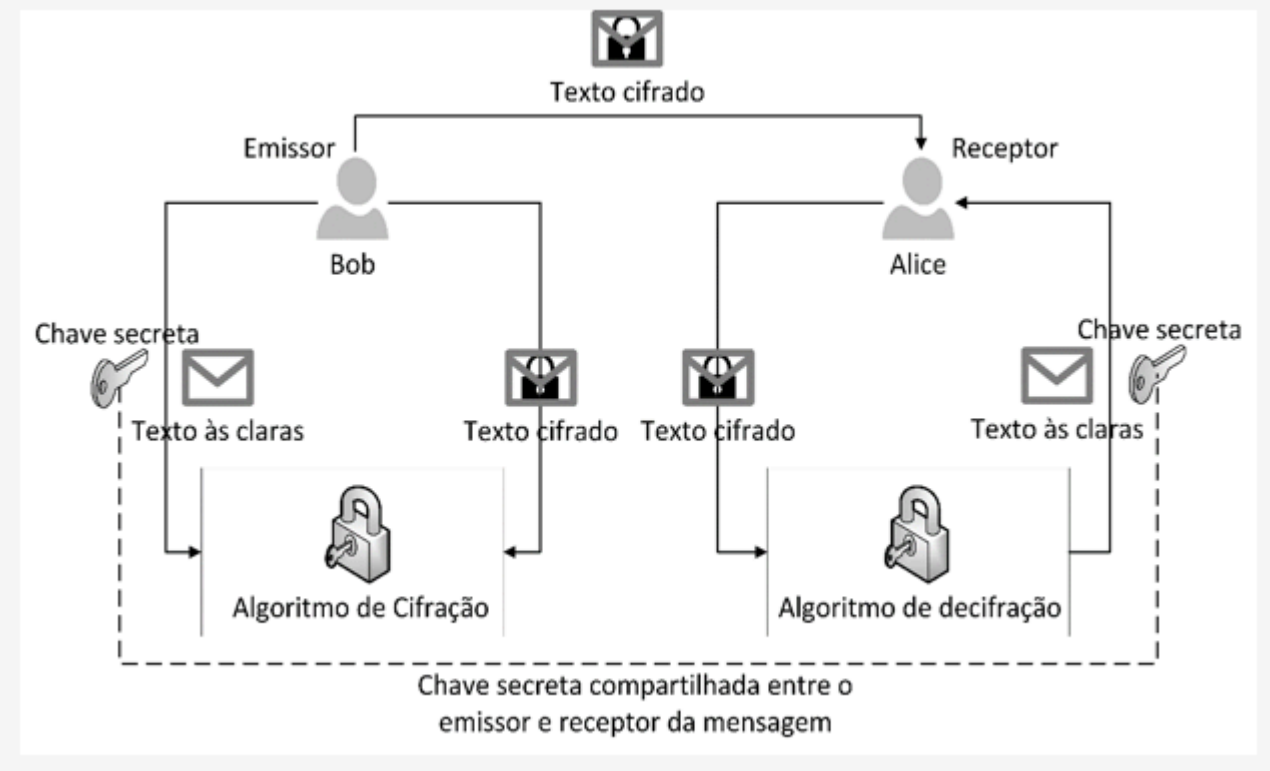
O estudo dos diversos métodos e procedimentos utilizados para cifragem/decifragem constituem a área de segurança conhecida como **criptografia**. Cada um desses métodos ou procedimentos é denominado como **sistema criptográfico** ou mais comumente chamado de **cifra**. Os métodos utilizados para decifrar um texto cifrado sem haver qualquer conhecimento dos detalhes do algoritmo de cifração estabelecem a área de **criptoanálise**. Por fim, a associação entre as áreas de criptografia e criptoanálise são denominadas como criptologia.

Um método de criptografia simétrica possui cinco elementos fundamentais:

- **Texto às claras**: é a mensagem original que é atribuída como entrada para o algoritmo de criptografia.
- **Algoritmo de cifração**: é um algoritmo matemático que executa várias substituições e transformações no texto às claras para gerar o texto cifrado.
- **Chave secreta**: a chave secreta é um segundo elemento de entrada para o algoritmo de cifração. Esta chave é um valor individual que não depende nem do texto claro e nem do algoritmo de cifragem. Para cada chave secreta o algoritmo de cifração produzirá uma saída diferente (texto cifrado). As substituições e transformações que serão realizadas pelo algoritmo dependem exclusivamente da chave utilizada.
- **Texto cifrado**: É a mensagem codificada produzida como saída. Esta mensagem é embaralhada, ela depende do texto às claras e da chave secreta. Destaca-se que uma mensagem cifrada com duas chaves diferentes irá gerar dois textos cifrados distintos.

- **Algoritmo de decifração**: é um algoritmo matemático que executa o algoritmo de cifragem de maneira inversa, ou seja, ele recebe como entrada o texto cifrado e a chave secreta e produz o texto original.

A Figura abaixo dispõe do modelo de criptografia simétrica.



Fonte: Autor

Existem dois requisitos que devem ser atendidos para utilização da cifração simétrica de forma segura:

1. Adotar um algoritmo de cifração forte. O algoritmo deve ser robusto o suficiente para impedir que o adversário que conheça o algoritmo e tenha acesso a um ou mais textos cifrados, não seja capaz de decifrar o texto cifrado ou adivinhar a chave secreta.

2. O emissor e receptor de uma mensagem deve obter cópias da chave secreta de maneira segura e preservá-las em segurança. Pois, qualquer indivíduo que conseguir acesso à chave e descobrir o algoritmo utilizado, terá acesso a toda comunicação realizada com essa chave.

Em geral, existem basicamente duas abordagens que os adversários utilizam para atacar um esquema de criptografia simétrica. O primeiro é o ataque de criptoanálise, neste ataque o adversário explora a natureza do algoritmo, além das características gerais do texto às claras e amostras em pares - amostras do texto às claras e o mesmo texto cifrado. Este ataque explora as características do algoritmo para tentar decifrar um texto às claras específico ou deduzir qual a chave secreta que foi utilizada. Caso o ataque seja bem-sucedido na dedução da chave, isto

poderá gerar um efeito desastroso em cascata, pois todas as mensagens que foram cifradas com esta chave serão comprometidas, incluindo as mensagens transmitidas anteriormente e as mensagens a serem enviadas.

A segunda técnica, é a utilização de um ataque de força bruta. Tratando-se do cenário de criptografia simétrica este ataque consiste em utilizar todas as chaves secretas possíveis em uma amostra de texto cifrado até conseguir ter acesso ao texto às claras. Uma estimativa denota que em média é necessário testar metade de todas as chaves secretas possíveis para obter sucesso neste ataque. Conforme exposto por Stallings é necessário 1ms para executar uma única tentativa de decifração [Stallings,2014], considerando um computador atual com uma configuração razoável. Abaixo uma tabela contendo o estudo realizado pelo autor, na tabela é apresentado o tempo médio para decifrar uma mensagem considerando tamanho de chaves diferentes.

Tamanho da chave (bits)	Número de chaves possíveis	Tempo requerido em 1 decifração/μs	Tempo requerido em 10 decifrações/ μs
32	232=4,3∗109" id="MathJax-Element-4-Frame" tabindex="0"> $2^{32} = 4{,}3*10^{9}$	231 μ" id="MathJax-Element-5-Frame" tabindex="0"> 2^{31} μ s * 35,8 minutos	2,15 milissegundos
56	256=7,2∗1016" id="MathJax-Element-6-Frame" tabindex="0"> $2^{56} = 7{,}2*10^{16}$	255 μ" id="MathJax-Element-7-Frame" tabindex="0"> ^{55} μ s = 1142 anos	10,01 horas
128	2128=3,4∗1038" id="MathJax-Element-3-Frame" tabindex="0"> $2^{128} = 3{,}4*10^{38}$	2127 m" id="MathJax-Element-8-Frame" tabindex="0"> 2^{127} m s = 5,4 * 224" id="MathJax-Element-12-Frame" tabindex="0"> 2^{24} anos	5,4 * 11018" id="MathJax-Element-11-Frame" tabindex="0"> 0^{18} anos
168	2168=3,7∗1050" id="MathJax-Element-9-Frame" tabindex="0"> $2^{168} = 3{,}7*10^{50}$	2127 μ" id="MathJax-Element-10-Frame" tabindex="0"> 2^{127} μ s = 5,9 * 1036" id="MathJax-Element-13-Frame" tabindex="0"> 10^{36} anos	5,9 * 11030" id="MathJax-Element-14-Frame" tabindex="0"> 0^{30} anos

26 caracteres (permutação)	26!=4∗1026" id="MathJax-Element-15-Frame" tabindex="0"> $26! = 4*10^{26}$	2∗1026 μ" id="MathJax-Element-17-Frame" tabindex="0"> $2 * 10^{26}$ μ s = 6,4 * 1012" id="MathJax-Element-16-Frame" tabindex="0"> 10^{12} anos	6,4 * 106" id="MathJax-Element-18-Frame" tabindex="0"> 10^{6} anos

Ressalta-se que com a utilização de processamento paralelo é possível reduzir consideravelmente o tempo necessário para "quebrar uma chave". Observe que na última coluna da tabela está sendo apresentado o de um sistema que é capaz de processar um milhão de chaves por microssegundo. Consequentemente, uma chave de 56 bits não deve ser mais considerada segura.

Algoritmos de Criptografia Simétrica

Os algoritmos de criptografia simétrica mais utilizados são as cifras de bloco. A cifra de bloco processa o texto às claras fornecido como entrada utilizando blocos de tamanho fixo, como resultado gera um bloco de texto cifrado de tamanho igual para cada um dos blocos de texto às claras. Este algoritmo processa as sequências de caracteres mais longas de texto às claras como sendo uma série de blocos de tamanho fixo. Entre os algoritmos simétricos mais importantes destacam-se o *Data Encryption Standard* (DES), o *Triple DES* (DES triplo) e o *Advanced Encryption Standard* (AES).

Data Encryption Standard

O algoritmo *Data Encryption Standard* (DES) é um dos principais algoritmos de chave simétrica, foi desenvolvido pela IBM em 1971, tornou-se um padrão adotado pelo NIST1 (*National Institute of Standards and Technology*) em 1977, então publicado na FIPS PUB 46 (*Federal Information Processing Standard*).

CURIOSIDADE

NIST (*National Institute of Standards and Technology*) em 1977 ainda era conhecido como *National*

Bureau of Standards (Escritório Nacional de Padrões)

Este algoritmo também ficou conhecido como algoritmo de cifração de dados, termo advindo do inglês DEA (*Data Encryption Algorithm*). O algoritmo recebe como entrada um bloco de texto às claras de 64 bits e uma chave secreta composta por 56 bits, como resultado gera um bloco cifrado de 64 bits.

A utilização do algoritmo DES institui duas grandes preocupações, relacionadas a implementação do algoritmo em si e outra relativo à utilização de uma chave de 56 bits. A primeira preocupação refere-se a explorar as características do algoritmo utilizando técnicas de criptoanálise. Destaca-se que o algoritmo DES foi intensamente estudado, ao longo dos anos foram realizadas numerosas tentativas de encontrar fraquezas neste algoritmo. Apesar de inúmeras abordagens, não foi reportado nenhuma fraqueza crítica.

Porém, em julho de 1998 o algoritmo DES mostrou ser inseguro, quando a *Electronic Frontier Foundation* (EFF) anunciou que havia decifrado uma cifração DES em uma máquina especializada, denominada DES *cracker*. Dado a evolução do *hardware*, os computadores desempenham um número maior de atividades em um menor tempo, os microprocessadores estão cada vez mais rápidos, o que torna o algoritmo DES praticamente inadequado.

CURIOSIDADE

DES cracker – máquina denominada como decifradora DES, construída por250 mil dólares na época.

Destaca-se que um ataque de força bruta destinado a busca de chave envolve mais do que somente executar todas as chaves possíveis. O analista deve ser capaz de reconhecer o texto às claras após a decriptação, ou seja, seu conteúdo deve ser compreensível. Quando a mensagem for composta por apenas texto às claras em um determinado idioma, o resultado será imediato, sendo apenas necessário reconhecer o idioma de forma automatizada. Porém, se o texto for comprimido antes de realizar a cifração, o processo de reconhecimento possui um grau maior de complexidade. Ainda, tratando-se de uma mensagem contendo um tipo de dado mais específico, como o código de alguma linguagem de programação ou arquivo numérico, e se este arquivo for comprimido, a técnica torna-se muito mais difícil de ser automatizada.

Deste modo, será necessária uma abordagem complementar ao ataque de força bruta, sendo preciso um certo grau de conhecimento sobre o texto às claras e uma forma de distinguir automaticamente se a mensagem cifrada retornou ao formato original. A estratégia adotada pela EFF trata exatamente este contexto, e ainda apresenta várias técnicas automatizadas que poderiam ser utilizadas em diferentes cenários.

Uma contramedida para mitigar o ataque de força bruta realizado ao algoritmo de cifração, seria adotar chaves mais longas. Considerando a tecnologia atual podemos realizar uma estimativa, caso a decifradora conseguisse executar um milhão de decifrações por milissegundos, então um código DES poderia ser "quebrado" em torno de 10 horas. Tendo em mente o aumento da velocidade de aproximadamente sete vezes em relação a tecnologia utilizada na decifradora da EFF. Considerando este cenário, para quebrar uma chave de 128 bits seria necessário mais de 10^{18} anos. Os resultados demostram que atualmente utilizar um ataque de força bruta sobre um algoritmo que utiliza uma chave de 128 bits é impraticável.

Triple Data Encryption Standard

A algoritmo DES foi utilizado como base para estruturar o algoritmo triplo DES (3DES), que na verdade não é nada mais que a implementação do algoritmo DES tradicional repetido três vezes, utilizando duas ou ainda três distintas, gerando um tamanho de chave de 112 ou 168 *bits* respectivamente. O triplo DES foi padronizado em 1985 como padrão ANSI X9.17, sendo então bastante utilizado em aplicações financeiras. Então, em 1999 foi adicionado ao FIPS PUB 46-3 como sendo uma parte do DES.

O triplo DES traz duas características bastante relevantes que asseguram seu uso para os próximos anos. A primeira característica está relacionada ao comprimento da chave, com uma chave de 168 *bits* o triplo DES consegue superar as vulnerabilidades impostas pelo ataque de força bruta no DES. A segunda característica é que o algoritmo de cifragem incluído dentro do triplo DES é o mesmo que inserido no DES.

Esse algoritmo mais do que qualquer outro algoritmo de cifração foi submetido a ataques de criptoanálise, porém nenhum ataque efetivo foi encontrado, a não ser o ataque de força bruta que levaria milhões de anos para ser "quebrado". Existe um alto nível de confiança da resistência do algoritmo triplo DES em relação aos ataques de criptoanálise. Na seleção de um algoritmo de cifragem, se a segurança fosse o único aspecto a ser avaliado, com certeza o triplo DES seria uma escolha conveniente.

Contudo o triplo DES possui desvantagens, a principal é que este algoritmo acaba sendo extremamente lento em software. O algoritmo DES foi projetado em hardware na década de 1970, porém não apresentava um código em software eficiente. Por sua vez, o triplo DES necessita de três vezes mais processamento, consequentemente muito mais lento. Outra desvantagem, apresentada tanto no DES como no triplo DES, ambos utilizam um tamanho de bloco de 64 *bits*. Levando em consideração tanto a eficiência como a segurança, trabalhar com tamanho de blocos maiores é apreciável.

Advanced Encryption Standard

Observando as desvantagens anteriormente apresentadas, o triplo DES não é um forte candidato para ser utilizado a longo prazo. Neste sentido, em 1997 o NIST publicou uma chamada para criação de novo algoritmo de cifração, o novo algoritmo deveria ter um nível de segurança equivalente ou superior ao 3DES e uma eficiência que fosse expressivamente melhor. Ainda, o NIST especificou que o novo algoritmo deveria ter uma cifra de bloco com comprimento de blocos de 128 *bits*, e forneceria suporte para chaves de 128, 192 e 256 *bits*. Conforme estabelecido pelo NIST, os critérios de avaliação contemplavam a segurança, eficiência computacional do algoritmo, consumo de memória, flexibilidade, algoritmo ajustável (*hardware e software*).

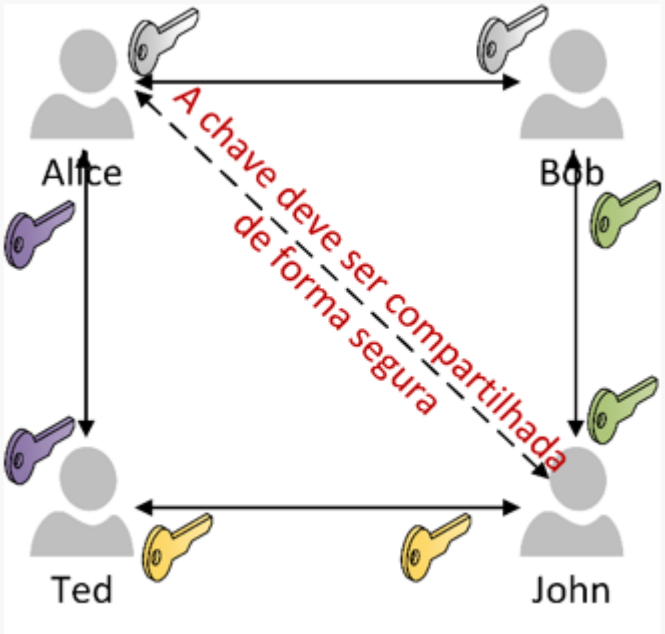
Na primeira etapa da avaliação foram selecionados 15 algoritmos de cifragem. Em uma segunda rodada, dos 15 algoritmos foram selecionados apenas 5 algoritmos. Por fim, em novembro de 2001 o NIST finalizou o processo de avaliação, selecionando o algoritmo de Rijndael como padrão final. Este algoritmo foi denominado Advanced Encryption Standard (AES). O AES foi então publicado no FIPS PUB 197, atualmente este algoritmo está amplamente presente em diversos produtos comerciais.

Distribuição de Chave Simétrica

Conforme mencionado, os algoritmos de criptografia simétricos utilizam a mesma chave tanto para cifrar como para decifrar. A chave secreta é compartilhada entre duas ou mais partes. Destaca-se que a chave secreta deve ser a mesma, tanto para a cifragem quanto para decifragem.

Considerando que a chave é de uso compartilhado e deve ser mantida em segredo pelas duas partes envolvidas na comunicação, para utilizar a criptografia simétrica, é essencial existir um canal para permitir a troca de forma segura das chaves entre as partes envolvidas na comunicação. Ressalta-se que na criptografia simétrica a necessidade de compartilhar a chave secreta com cada parceiro é o que impõem a sua maior fragilidade. Tendo em vista, que a transmissão das chaves entre os envolvidos pode não ser realizada de forma segura, e esta chave pode acabar de posse de um indivíduo mal-intencionado.

A figura a seguir mostra um outro problema da criptografia simétrica, a distribuição das chaves. Onde, cada usuário terá de armazenar e gerenciar o número de chaves de acordo com a quantidade de pessoas com as quais ele se comunica. Por exemplo, conforme disposto na figura, Alice tem duas chaves compartilhadas, uma para se comunicar com Bob e outra para se comunicar com Ted. Se Alice quiser trocar mensagens com John de forma confidencial, ela precisará adquirir e gerenciar mais uma chave.



Fonte: Autor

Neste sentido, dois grandes problemas necessitam ser avaliados tratando-se de criptografia simétrica:

- Transmitir a chave secreta de uma forma segura e confiável entre as duas partes envolvidas na comunicação.

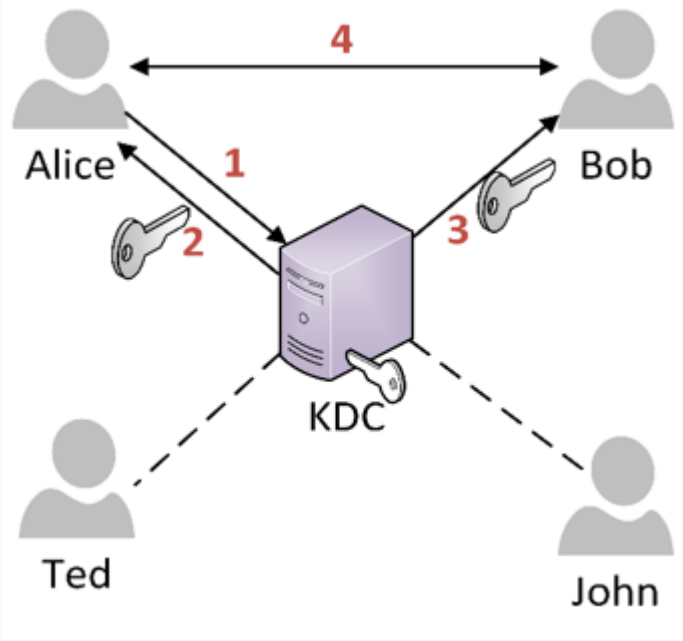
- Administrar o problema da distribuição de um número considerável de chaves (armazenar uma chave para cada comunicação distinta).

Centro de Distribuição de Chaves (KDC)

De acordo com o que estudamos, uma das grandes limitações da criptografia simétrica é justamente a distribuição das chaves secretas. Como podemos distribuir a chave secreta de maneira segura entre a duas partes. Para tal, podemos utilizar um intermediário de confiança denominado como centro de distribuição de chaves, ou do termo inglês KDC (*Key Distribution Center*). O KDC é considerado uma entidade de confiança na rede com quem o usuário estabelece uma chave secreta compartilhada, a partir desta entidade os usuários podem obter as chaves compartilhadas necessárias para uma comunicação segura com os demais usuários da rede, evitando assim algumas estratégias do adversário para capturar a chave secreta.

A figura a seguir mostra duas partes, Alice e Bob, tentando estabelecer uma comunicação segura utilizando o KDC. Para isto, a seguinte sequência de passos é realizada:

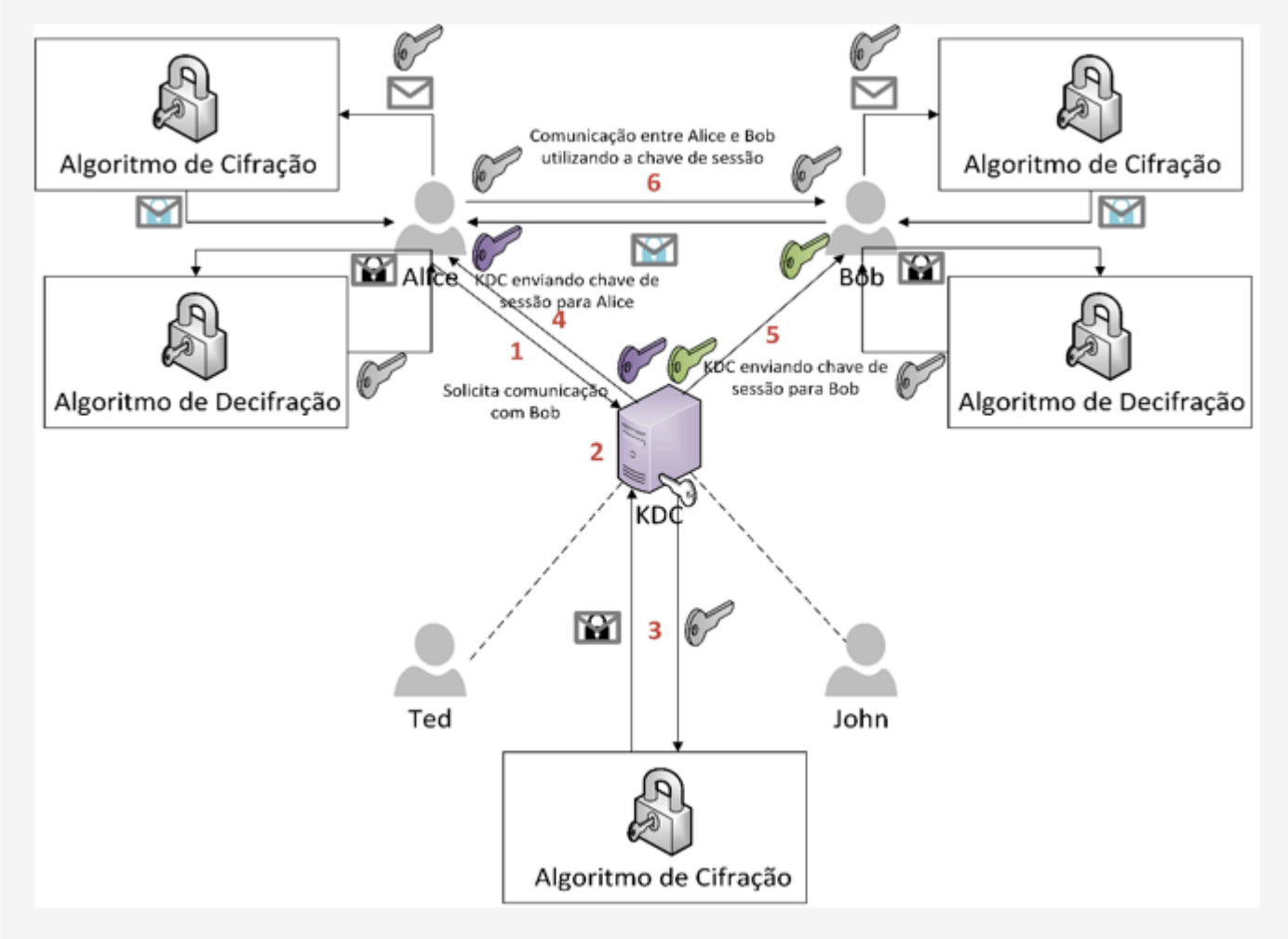
1. Alice solicita ao KDC que deseja se comunicar com Bob.
2. O KDC envia uma chave a Alice.
3. O KDC envia a mesma chave a Bob.
4. A chave que Alice e Bob receberam permitem estabelecer uma comunicação de forma segura, os dados são cifrados com a chave que foi enviada pelo KDC.



Fonte: Autor

Visando garantir que realmente a chave foi concedida pelo KDC, ele fornece uma chave secreta simétrica diferente para cada um dos seus usuários cadastrados. Sendo esta chave criado no servidor no instante que o usuário se cadastra no KDC. Deste modo, o KDC conhece a chave que foi distribuída para cada usuário, o que permite que o usuário e o KDC se comuniquem com segurança.

Na figura abaixo demonstramos o processo para estabelecer a comunicação entre duas partes.



Fonte: Autor

Considerando que Alice e Bob são usuários do KDC, eles conhecem somente a chave secreta com o KDC. Alice deseja iniciar a comunicação.

1. Então Alice, utiliza sua chave secreta para se comunicar com o KDC, diz que deseja se comunicar com Bob.

2. O KDC recebe a mensagem de Alice, neste momento o KDC tem certeza da origem da mensagem, sendo que apenas Alice possui esta chave secreta que eles compartilham.

3. O KDC então decifra a mensagem enviada por Alice, verifica a intenção de Alice de se comunicar com Bob. Então, na sequência o KDC cria uma chave para que Alice e Bob possam estabelecer esta comunicação. Esta chave é denominada como "chave de sessão". A chave de sessão será utilizada para estabelecer a comunicação uma única vez, ou seja, uma única sessão de comunicação. Após o KDC criar a chave ele necessita enviar esta chave para Alice e Bob.

4. Para enviar a chave de sessão para Alice, o KDC cifra a chave de sessão utilizando a chave secreta que é compartilhada exclusivamente com Alice.

5. Para enviar a chave de sessão para Bob, o KDC cifra a chave de sessão utilizando a chave secreta que é compartilhada exclusivamente com Bob.

6. Após Alice e Bob receberem suas mensagens, eles decifram a mensagem utilizando a chave secreta que cada um deles compartilha com o KDC. Ao decifrar a mensagem Alice e Bob terão acesso a chave de sessão para se comunicar. Agora toda comunicação realizada entre Alice e Bob deve ser cifrada utilizando a chave de sessão.

Utilizando a criptografia simétrica, distribuindo a chave secreta por meio do KDC, conseguimos garantir as seguintes propriedades de segurança:

- **Confidencialidade**: somente Alice e Bob conseguem decifrar as mensagens cifradas com a chave de sessão.

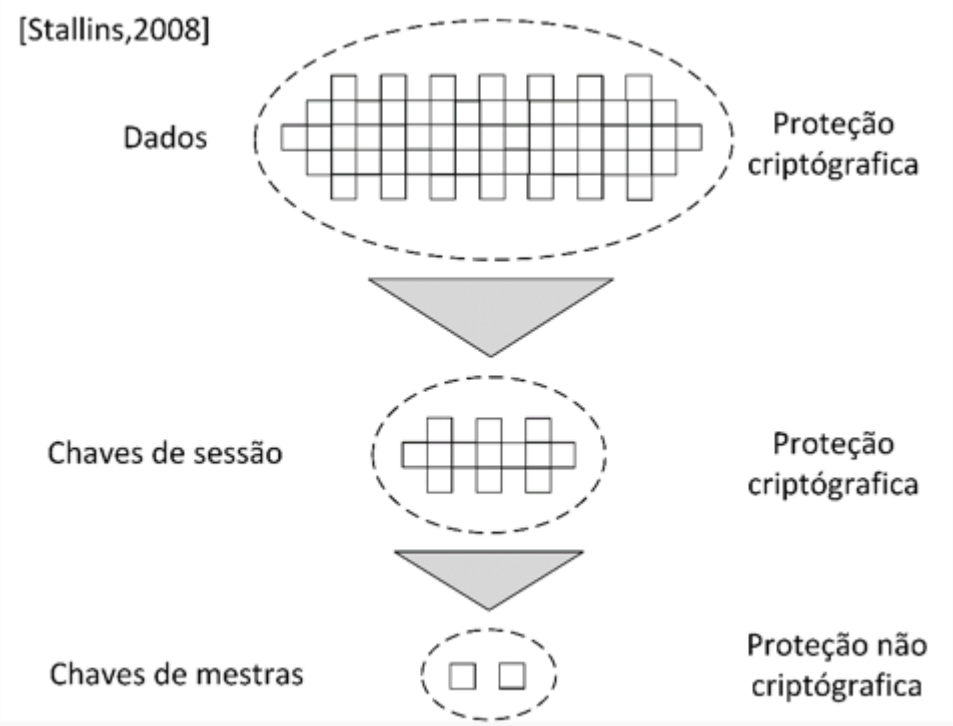
- **Autenticidade**: quando Alice recebe uma mensagem cifrada com a chave de sessão, ela sabe exatamente com quem a chave é compartilhada, neste caso com Bob, já que apenas Bob conhece essa chave. Da maneira similar, quando Bob recebe uma mensagem cifrada com chave de sessão que compartilha com Alice, ele sabe exatamente que a mensagem foi enviada por Alice.

- **Não Repúdio**: sendo que a chave de sessão é apenas compartilhada entre Alice e Bob eles não poderão negar a autoria da mensagem, ou seja, negar que foi um deles que enviou uma mensagem cifrada com a chave de sessão que apenas ambos compartilham.

Hierarquia de Chaves

O uso de um KDC depende de uma estrutura de hierarquia de chaves. A hierarquia de chaves permite conceder níveis diferentes de criptografia para as chaves. O KDC necessita de no mínimo dois níveis de chaves. Em geral, a comunicação realizada entre os sistemas finais é cifrada utilizando uma chave temporária, a chave de sessão. Geralmente, a chave de sessão é utilizada

dentro da duração de tempo fornecida por uma conexão lógica, tal como uma conexão de transporte. Após o tempo de duração a chave de sessão perde sua validade e então é descartada. A chave de sessão é obtida a partir do KDC sob a mesma infraestrutura de rede utilizada para comunicação do usuário final. A figura abaixo mostra a representação adaptada da hierarquia de chaves proposta por Stallings [Stallings,2008].



Fonte: Adaptada de Stallings

Na sequência, a chave deve ser transmitida ao usuário final de maneira cifrada para que uma terceira parte não tenha acesso a chave de sessão. Para cifrar a chave de sessão deve ser utilizado uma chave mestra, a chave criada pelo KDC assim que o usuário é cadastrado.

Não é necessário centralizar a distribuição de chaves em um único KDC. Em redes maiores pode não ser viável fazer isso. Alternativamente, é possível estabelecer uma hierarquia de KDC. Por exemplo, é possível distribuir os KDC's locais, cada qual fica responsável por um determinado domínio ou subdomínio.

Assim, o KDC local fica responsável por distribuir as chaves dentro do domínio local para entidades que foram ali cadastradas. Contudo, caso duas entidades associados a domínios diferentes desejem se comunicar, então os KDC´s locais podem se comunicar com um KDC global a fim provisionar uma chave de sessão para que as partes consigam se comunicar de forma segura. Neste sentido, qualquer um dos três KDC´s pode realmente gerir a chave. O conceito hierárquico pode ser estendido a três ou mais camadas, dependendo do tamanho da rede e da quantidade de usuários.

O esquema hierárquico permite reduzir o efeito associado à distribuição da chave mestra, tendo em vista a grande quantidade das chaves mestras que serão compartilhadas por um KDC local com suas respectivas entidades. Adicionalmente, este esquema permite restringir a abrangência do dano causado por KDC defeituoso tendo impacto apenas na sua área local.

Princípios de Cifração Assimétrica

O conceito de cifração assimétrica, amplamente conhecido como criptografia de chave pública evoluiu da tentativa de resolver dois problemas complexos associados a cifração simétrica. O primeiro, já mencionado, é o problema relacionado a distribuição de chaves. Conforme discutido, a distribuição de chaves de uma abordagem utilizando cifração simétrica necessita que as duas partes comunicantes compartilhem uma chave que lhes foi atribuída anteriormente. Consequentemente, sendo necessário o uso de KDC. Um outro requisito foi abordado por Whitfield Diffie e Martin Hellman, criadores do algoritmo de cifração de chave pública. Consideraram um aspecto que anulava a própria natureza da criptografia: a capacidade de conservar o segredo absoluto sobre a própria comunicação. Conforme exposto por Diffie "*afinal, qual seria a vantagem de desenvolver criptossistemas impenetráveis, se seus usuários fossem forçados a compartilhar suas chaves com um KDC que poderia ser comprometido por roubo ou suborno?*" [Diffie,1988].

O segundo problema refletido por Diffie foi a das assinaturas digitais. Prevendo o uso da criptografia não apenas para fins militares, vislumbrando atender demandas comerciais e particulares, constatou que as mensagens e documentos digitais precisariam de algo que fosse equivalente às assinaturas manuscritas nos documentos em papel. Idealizou a criação de um método que fosse capaz de satisfazer todas as partes, e afirmar que uma mensagem no meio digital tenha sido enviada por determinado indivíduo.

Investindo sobre a resolução destes dois problemas, Diffie e Hellman projetaram um algoritmo revolucionário no campo da criptografia, propuseram um método de cifragem para trocas de chaves de maneira segura realizado em um canal público. Este algoritmo foi publicado em 1976, denominado como método de troca de chaves de Diffie-Hellman. Considerado um dos primeiros exemplos práticos de métodos de troca de chaves implementado dentro da área de criptografia, propulsor da criptografia de chave pública.

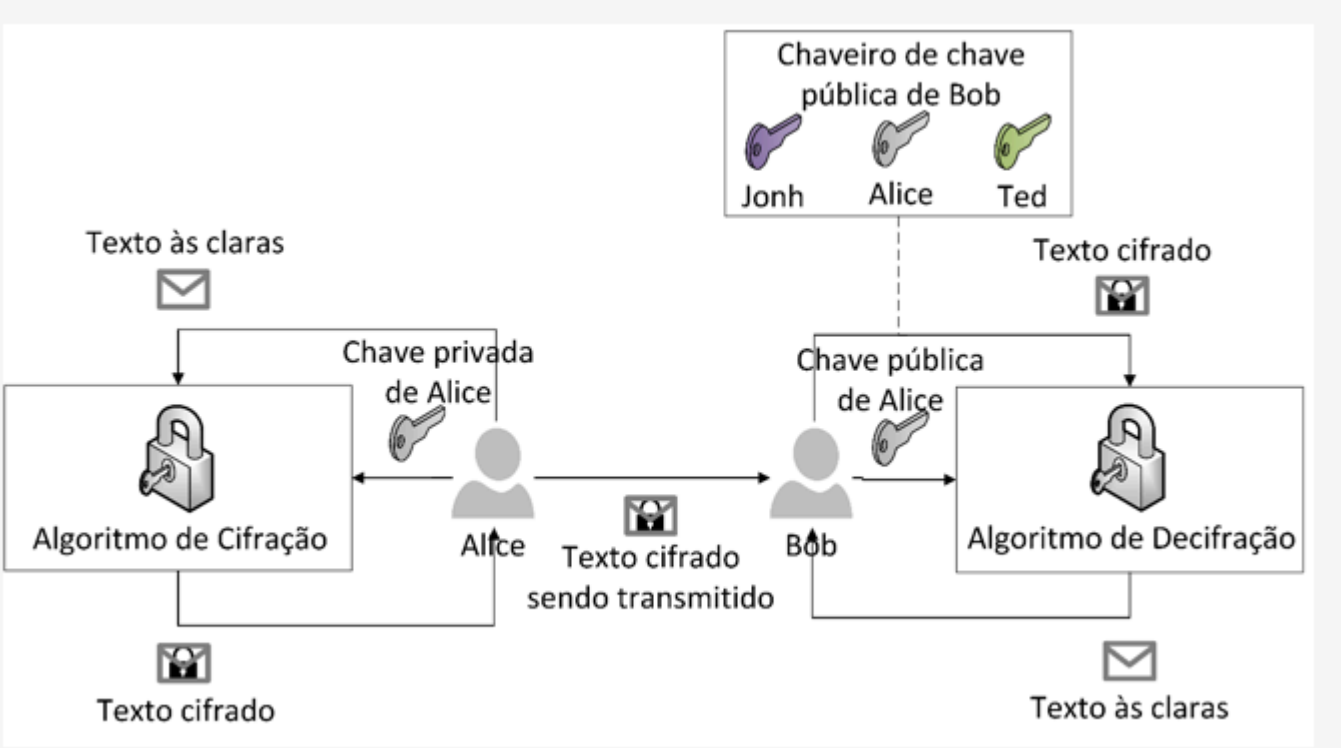
Fundamentos de Cifração Assimétrica

Os algoritmos de criptografia assimétricos trabalham com duas chaves, uma para cifragem dos dados e uma segunda chave para decifragem dos dados. Tais algoritmos possuem uma característica significativa, é computacionalmente inviável especificar a chave de decifragem utilizando apenas o conhecimento do algoritmo e chave de cifragem. Outra característica adicional, específica do algoritmo RSA é a de que qualquer umas das duas chaves podem ser utilizadas para cifragem, como resultado a outra chave deve ser utilizada para decifragem.

A abordagem de criptografia de chave pública dispõe de cinco elementos:

- **Texto às claras**: corresponde à mensagem ou aos dados em formato legível que são disponibilizados como entrada para o algoritmo.
- **Algoritmo de cifraçã**o: é um algoritmo matemático que realiza várias operações e transformações no texto às claras.
- **Chaves pública e privada**: corresponde a um par de chaves secretas, selecionadas de tal modo que se uma das chaves for utilizada para cifrar a outra é utilizada para decifrar. As transformações específicas realizadas pelo algoritmo, variam de acordo com a chave pública ou chave privada que foi concedida como entrada para o algoritmo.
- **Texto cifrado**: é a mensagem codificada produzida como saída. Esta mensagem é embaralhada, ela depende do texto às claras e da chave secreta que foi utilizada. Destaca-se que duas chaves diferentes produzirão como resultado dois textos cifrados distintos.
- **Algoritmo de decifração**: é um algoritmo matemático que recebe como entrada o texto cifrado e a chave correspondente e produz como resultado a mensagem original, ou seja, o texto às claras.

Na figura abaixo é demostrado um esquema típico de criptografia de chave pública:



Fonte: Autor

As etapas fundamentais são demostradas as seguir:

1. Cada usuário deve conceber um par de chaves que será utilizado para o processo de cifragem e decifragem das mensagens.
2. O usuário deve alocar uma das duas chaves em um registrador público ou utilizar outro meio para disponibilizar esta chave, esta chave é denominada como chave pública. A outra chave deve ser mantida em segurança, esta chave é denominada como chave privada. Adicionalmente, cada usuário mantém um conjunto de chaves públicas de outros usuários.
3. Caso Alice deseje enviar uma mensagem secreta para Bob, ela cifra a mensagem utilizando a chave pública de Bob.
4. Quando Bob receber a mensagem, ele utiliza a chave privada para decifrar a mensagem. Destaca-se que nenhum outro indivíduo conseguirá decifrar a mensagem, pois somente Bob conhece a chave privada.

Utilizando esta técnica, todos os envolvidos podem ter acesso às chaves públicas. Ressalta-se que as chaves privadas são geradas localmente por cada uma das partes envolvidas, e essas chaves não podem ser distribuídas. A chave privada deve ser protegida e secreta, isto vai garantir que a comunicação realizada entre as partes esteja protegida. Outro fator interessante é a possibilidade de renovar as chaves sempre que necessário, a qualquer momento um sistema poderá modificar a chave privada e redistribuir uma nova chave pública.

Algoritmos de Chave Pública

Nesta seção vamos explorar alguns dos principais algoritmos assimétricos utilizados atualmente, o algoritmo RSA, Diffie-Hellman, DSS e as curva elípticas.

Algoritmo RSA

O RSA foi um dos primeiros algoritmos de cifração assimétrica, desenvolvido em 1977 por Ron Rivest, Adi Shamir e Len Adleman pesquisadores do MIT (Instituto de Tecnologia de Massachusetts), então publicado em 1978 [Rivest et al., 1978]. O algoritmo foi denominado como RSA dado a composição da inicial do nome dos autores. Este esquema de criptografia de chave pública tem sido amplamente aceito e utilizado até os dias de hoje. O RSA é estruturado por uma cifra de bloco onde o texto às claras e o texto cifrado corresponde a um número inteiro entre 0 e *n - 1*, definido algum valor a n.

Em 1977, em uma publicação da revista *Scientific American*, os autores do algoritmo RSA desafiaram seus leitores a decifrar um texto cifrado que foi divulgado na coluna "Jogos matemáticos". Os autores do algoritmo proporcionaram uma recompensa de 100 dólares para quem conseguisse retornar o conteúdo da mensagem em texto às claras. Evento que os autores mensuraram que só poderia ocorrer daqui aproximadamente 40 quatrilhões de anos.

CURIOSIDADE

Quatrilhões – número equivalente a mil bilhões, representado por 10^{15}.

Porém, em 1994 um grupo na internet empenhou-se em decifrar a mensagem, foram utilizados mais de 1600 computadores, então com somente oito meses de trabalho foi reivindicado o prêmio [Leutwyler,1994]. Neste desafio foi utilizado um tamanho de chave de aproximadamente 428 *bits* de comprimento. Ressalta-se que este resultado não anula a utilização do algoritmo RSA, somente enfatiza a necessidade de utilizar chaves com comprimento maiores. Atualmente, as aplicações utilizam um tamanho de chave de 1024 *bits* que é considerado um tamanho adequado e uma chave robusta para maioria dos cenários.

Acordo de chaves de Diffie-Hellman

O algoritmo de Diffie-Hellman foi conhecido como o primeiro algoritmo de chave pública, publicado em 1976. Este algoritmo também é conhecido como troca de chaves ou acordo de chaves de Diffie-Hellman. Existem uma quantidade considerável de produtos no âmbito comercial que utilizam as técnicas empregadas no algoritmo de troca de chaves.

O propósito do algoritmo é permitir que dois indivíduos cheguem em um consenso de como compartilhar um segredo de forma segura, permitindo que este segredo seja utilizado posteriormente como chave secreta em uma aplicação de criptografia simétrica na troca das mensagens. Este algoritmo limita-se somente à troca das chaves secretas.

Digital Signature Standard

O algoritmo *Digital Signature Standard* foi proposto em 1991, publicado pelo NIST em 1994 no FIPS PUB 186, também conhecido como padrão de assinatura digital. Este algoritmo faz uso da função *hash* criptográfica SHA-1 e ainda propõe uma abordagem inovadora para assinatura digital, o algoritmo de assinatura digital conhecido como DSA (*Digital Signature Algorithm*).

Devido algumas menções públicas sobre a segurança do DSS, o algoritmo foi revisado em 1993. Posteriormente, em 1996 houve uma pequena revisão no algoritmo. O algoritmo DSS foi estruturado apenas para fornecer a função de assinatura digital, ou seja, diferente do algoritmo RSA, este algoritmo não pode ser utilizado para realizar trocas de chaves ou ainda para cifragem.

Criptografia de Curvas Elípticas

Devido as propriedades robusta do algoritmo RSA ele tornou-se uma tendência de mercado, atualmente uma grande parte dos produtos e padrões que utilizam criptografia de chave pública ou ainda assinaturas digitais acabam optando por utilizar o algoritmo RSA. Observasse que isto só foi possível porque o algoritmo permite utilizar chaves com tamanho variável. Para manter a robustez do algoritmo em termos de segurança, o comprimento das chaves em *bits* vem sendo ampliado. Contudo, isto reflete em uma carga maior de processamento em relação as aplicações que utilizam o algoritmo RSA.

Este problema possui alguns desdobramentos, em destaque serviços disponibilizados na *web* que realizam um número expressivo de transações seguras por segundo, por exemplo sites de comércio eletrônico. Neste sentido, uma abordagem promissora foi desenvolvida para concorrer

com o algoritmo RSA, a criptografia de curvas elípticas. Conhecida também como ECC, acrônimo do termo inglês (*Elliptic Curve Cryptography*). Existem algumas iniciativas para tornar as curvas elípticas em um padrão, incluindo o padrão de criptografia de chave pública, o *Standard for Public-Key Cryptography P1363* do IEEE (*Institute of Electrical and Electronics Engineers*).

Uma das principais vantagens da curva elíptica em relação a RSA é que ela propõe uma segurança equivalente para um comprimento de bits bem menor, característica que permite reduzir o custo computacional. Em contrapartida, apesar da teoria das curvas elípticas terem sido concebidas há algum tempo, apenas recentemente com a adoção de alguns produtos começaram a ser exploradas. Consequentemente, despertando o interesse criptoanalítico, visando encontrar suas fraquezas. Deste modo, podemos inferir que o nível de confiança das curvas elípticas ainda é inferior quando comparado com um algoritmo RSA.

Aplicações de Chave Pública

Os algoritmos de chave pública são utilizados em diversas aplicações. Em geral, essas aplicações são basicamente categorizadas em duas frentes: assinatura digital; e abordagens de gerenciamento e distribuição de chaves.

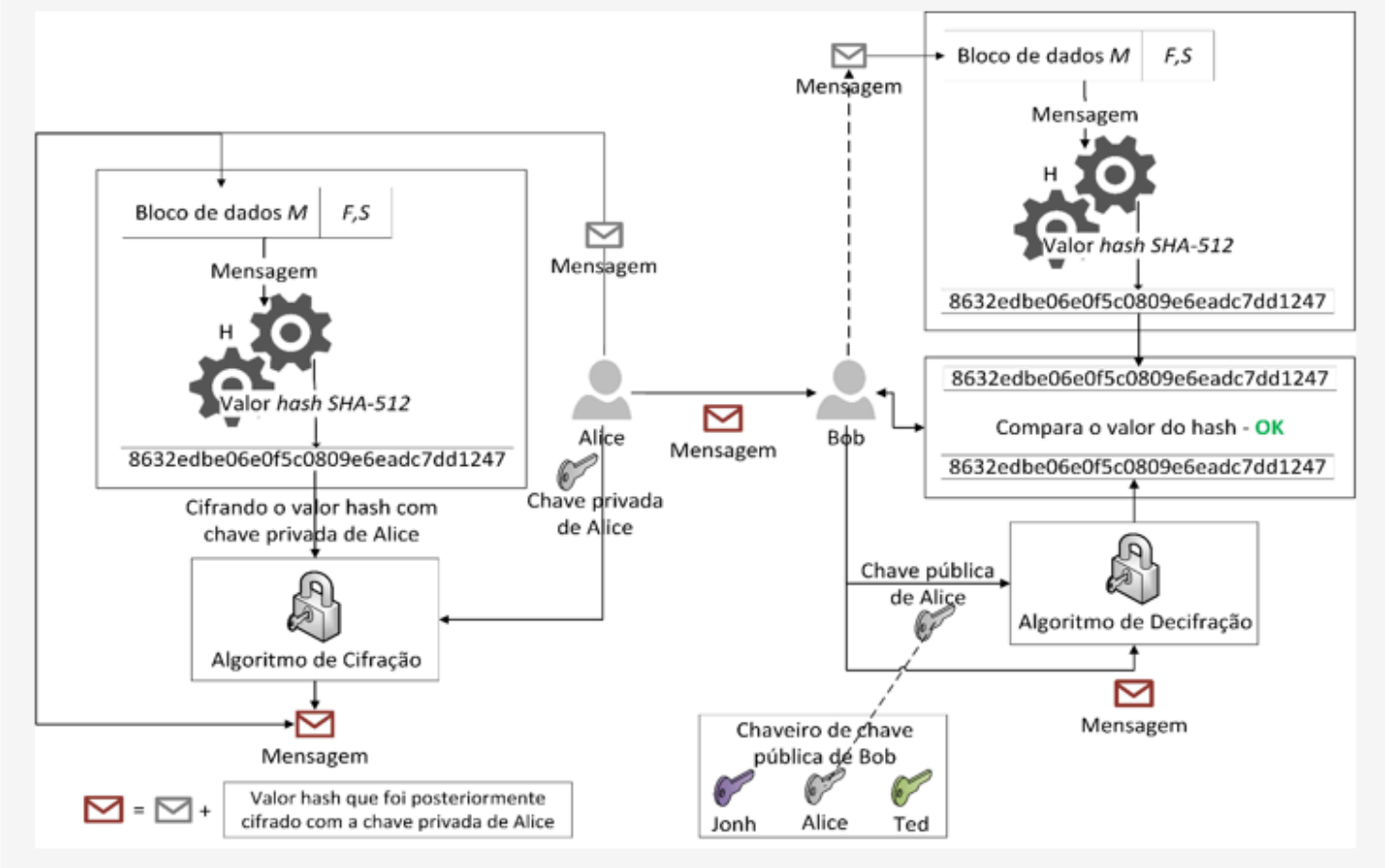
Relacionado ao processo de gerenciamento e distribuição de chaves, alguns fatores fundamentais relacionados à criptografia de chave pública devem ser levados em consideração:

- Estabelecer um processo para distribuição segura das chaves públicas.
- Utilizar a criptografia de chave pública para fornecer um método para distribuição das chaves secretas.
- Utilizar a criptografia de chave pública para fornecer chaves temporárias para serem usadas na cifração de mensagens.

As aplicações de chave pública apresentadas nesta seção, fornecem uma visão geral das assinaturas digitais e alguns exemplos de aplicações do processo de gestão e distribuição de chaves.

Assinatura Digital

A criptografia de chave pública pode ser utilizada como ferramenta de autenticação, observe a representação exposta na figura abaixo:



Fonte: Autor

Supondo que Alice necessite enviar uma mensagem para Bob. Considerando que a mensagem não possui caráter confidencial, ou seja, preservar o sigilo da mensagem não é um requisito importante. Porém, Alice quer garantir que Bob tenha certeza de que a mensagem foi enviada por ela.

Visando garantir a autenticidade, Alice utiliza uma função *hash* criptográfica segura, como algoritmo SHA-512, gerando um valor *hash* para sua mensagem. Posteriormente cifra o código *hash* com sua chave privada, concebendo uma assinatura digital. Então, Alice transmite a mensagem com a assinatura digital anexada. Quando Bob recebe a mensagem encaminhada por Alice ele consegue certificar a origem da mensagem por meio da assinatura digital, para isto Bob deve realizar o seguinte processo:

1. Calcular o valor do *hash* da mensagem;

2. Decifrar a assinatura utilizando a chave pública de Alice;

3. Comparar o código *hash* obtido com o código *hash* disposto na mensagem decifrada.

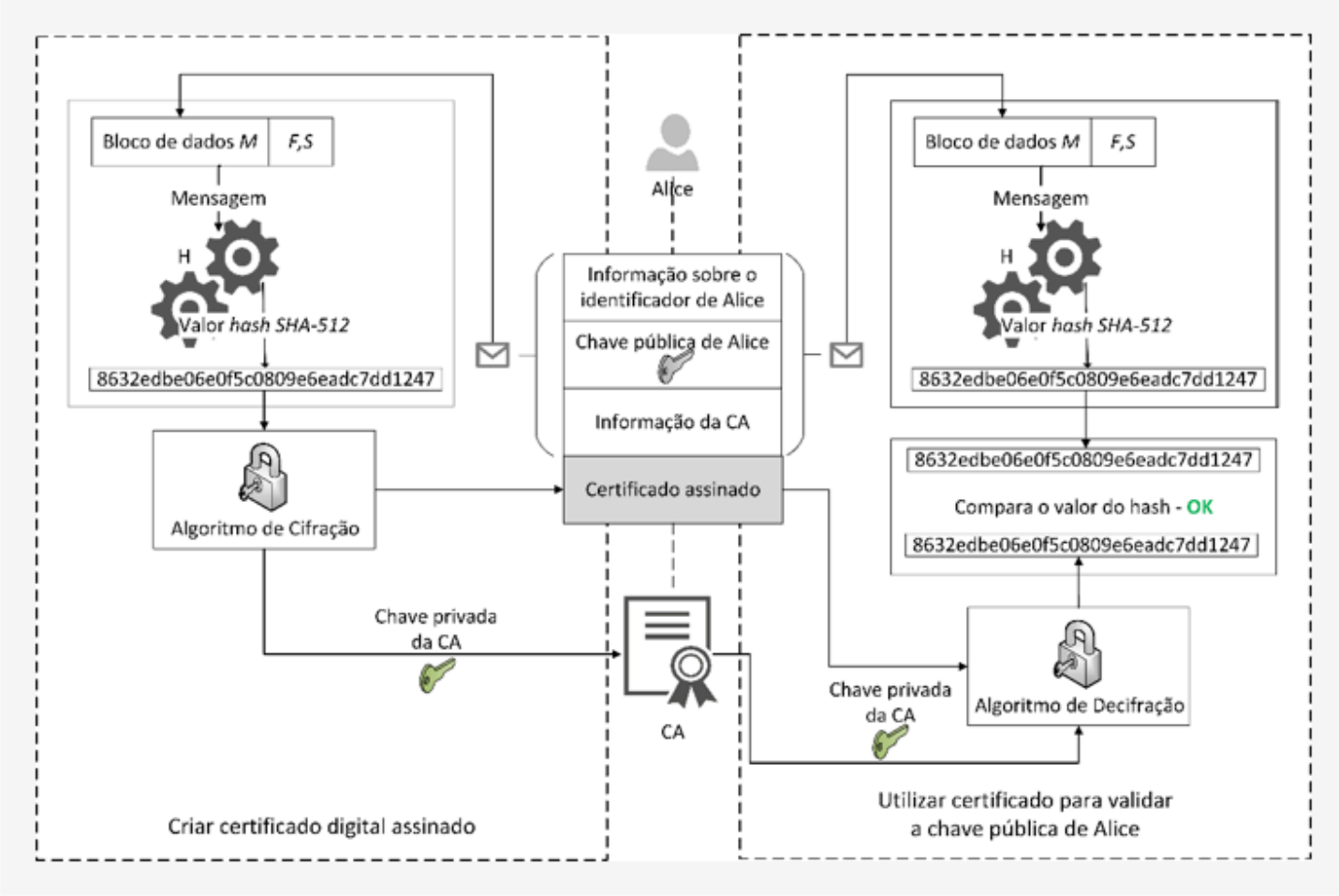
Caso ambos os códigos *hash* forem idênticos, Bob consegue ter certeza de que a mensagem foi assinada com a chave privada de Alice. Sendo que ninguém mais além de Alice possui sua chave privada, ninguém mais poderia ter cifrado o texto que foi decifrado utilizando a chave pública de Alice. Ainda, destaca-se que seria impossível modificar a mensagem sem ter posse da chave privada de Alice, esta propriedade permite autenticar a mensagem, primeiro determinar sua origem, por conseguinte garantir a integridade dos dados transmitidos.

É importante destacar que assinatura digital não fornece confidencialidade. Em outras palavras, a mensagem que está sendo transmitida permite garantir que não sofreu nenhuma alteração, porém não garante que uma terceira parte tenha acesso ao conteúdo da mensagem.

Certificados de Chave Pública

Analisando a criptografia de chave pública, uma característica exclusiva é dispor da chave pública, onde a chave pode ser distribuída publicamente sem nenhum prejuízo. Deste modo, na utilização de um algoritmo de chave pública, tal como o RSA, qualquer usuário pode disponibilizar sua chave pública para outros usuários. Apesar desta abordagem ser oportuna, ela possui certas limitações: qualquer indivíduo pode falsificar um comunicado público, isto é, um indivíduo mal-intencionado pode se passar pela Alice e enviar uma chave pública a outros participantes, o ainda divulgar a chave pública de forma "aberta" (disponibilizar publicamente). Enquanto Alice não descobrir a farsa e conseguir alertar os participantes, o adversário conseguirá ter acesso ao conteúdo de todas as mensagens cifradas que foram enviadas, ainda pode utilizar as chaves falsificadas para conceber a autenticação.

A ideia do certificado consiste em utilizar uma chave pública associado ao identificador do proprietário da chave em conjunto com um bloco inteiro assinado por uma terceira parte, uma entidade confiável. Em geral, esta terceira entidade corresponde a autoridade certificadora na qual a comunidade tem absoluta confiança. A autoridade certificadora também é conhecida como CA (*Certification Authority*). É bastante comum que uma CA seja uma agência governamental ou uma instituição financeira. Para validar um certificado além da informação da CA é necessário fornecer o período de validade do certificado. Um usuário pode solicitar um certificado assinado pela CA dispondo da sua chave pública de forma segura. Posteriormente, este usuário pode publicar o certificado. Deste modo, quem precisar utilizar a chave pública do usuário poderá obter o certificado e consultar se ele é válido, verificando se a assinatura anexada é confiável. A figura exposta abaixo demonstra este processo.



Fonte: Autor

Para formatar os certificados de chave pública foi adotado um padrão universal, o X.509. Os certificados X.509 são utilizados na grande maioria das aplicações de segurança em rede. Tais aplicações incluem protocolos bastante conhecidos como o IPsec (*IP Security*), TLS (*Transport Layer Security*), SSH (*Secure Shell*) e S/MIME (*Secure / Multipurpose Internet Mail Extension*).

CURIOSIDADE

IPsec - é um protocolo de comunicação segura na internet utilizado para tunelamento, criptografia e autenticação.

S/MIME - é um protocolo amplamente aceito para enviar mensagens assinadas digitalmente e criptografadas.

Distribuição de Chave Simétrica Usando Criptografia de Chave Pública

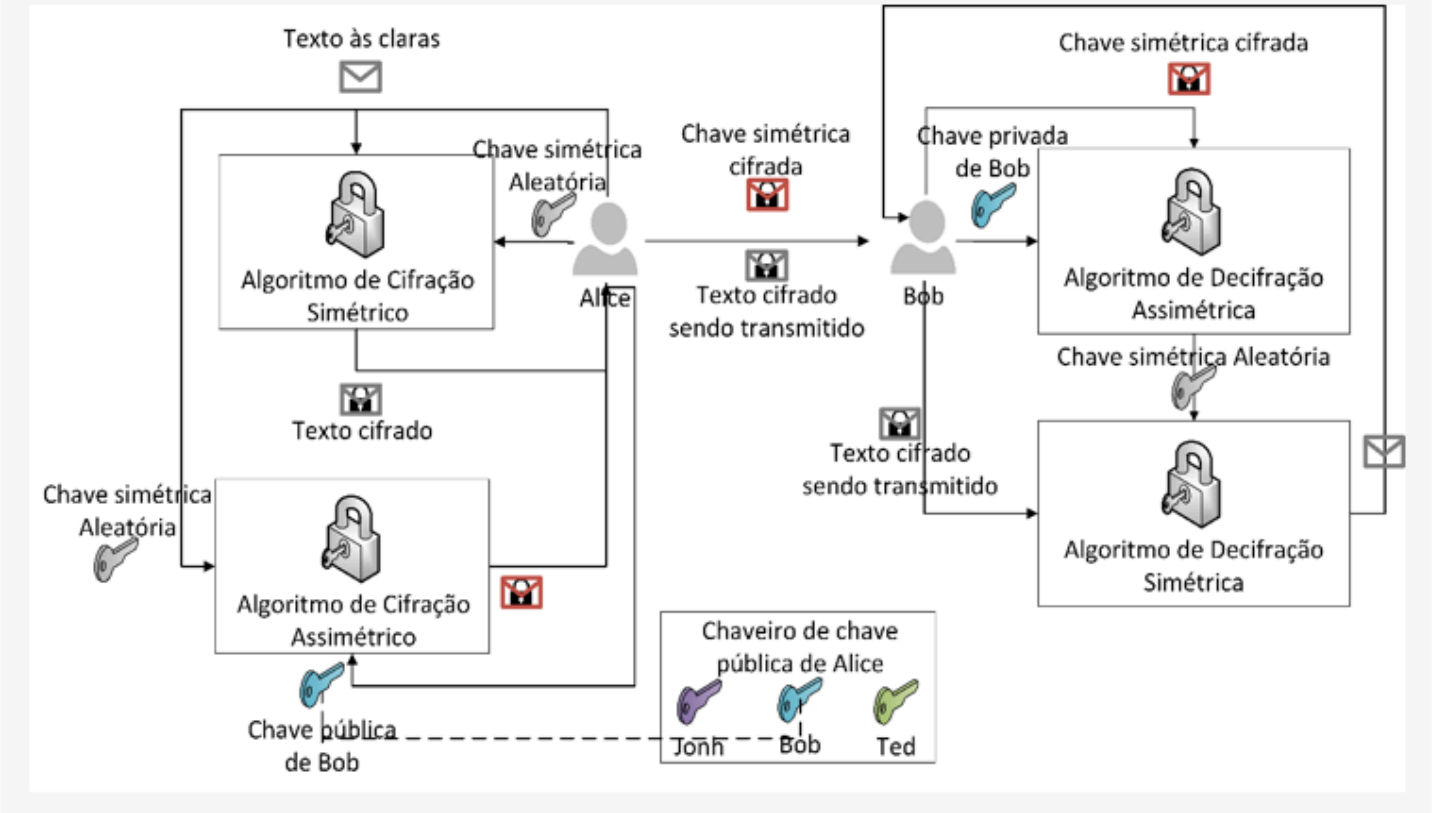
Conforme mencionado, um requisito fundamental da cifração simétrica para possibilitar uma comunicação segura entre duas partes é que elas devem compartilhar uma chave secreta. Para exemplificar, imagine que Alice deseja criar uma aplicação de envio de mensagens. A aplicação deve possibilitar a troca de e-mail de forma segura na internet ou uma rede privada que seja compartilhada entre duas partes. Alice quer utilizar criptografia simétrica na sua aplicação. Utilizando a criptografia simétrica, para que Alice estabeleça uma comunicação segura com alguns dos seus contatos, ela deve encontrar uma maneira segura de compartilhar a chave secreta para que nenhum indivíduo indesejado tenha acesso ao conteúdo das mensagens.

Digamos que Alice precisa compartilhar a chave secreta com Bob. Dado as restrições da localização física isto pode ser tornar um desafio. Alice poderia cifrar a chave utilizando a criptografia simétrica e posteriormente enviar a chave criptografada por e-mail para Bob, porém isto requer que Alice e Bob já possuam uma chave secreta compartilhada entre eles. Ainda, ressalta-se que todos os demais contatos que desejam utilizar o novo aplicativo irão enfrentar esta mesma situação, cada par de correspondente (emissor e receptor) deverão compartilhar uma chave secreta única e exclusiva.

Uma das estratégias é adotar o método de troca de chaves Diffie-Hellman. Esta é uma abordagem amplamente utilizada, contudo possui uma limitação, na implementação mais simples do algoritmo de Diffie-Hellman não é fornecido qualquer tipo de mecanismo de autenticação entre as duas partes comunicantes. Algumas variações do algoritmo de Diffie-Hellman já tratam este problema. Adicionalmente, também existem alguns protocolos que utilizam criptografia de chave pública para este mesmo propósito.

Envelopes Digitais

Os envelopes digitais são um outro tipo de aplicação que envolve o uso de criptografia de chave pública. O conceito do envelope digital é o de proteger uma mensagem sem a necessidade de que o emissor e o receptor compartilhem a mesma chave secreta. Esta técnica seria o equivalente ao criar um envelope selado, porém contém uma carta que não foi assinada. A representação da abordagem é apresentada na figura abaixo.



Fonte: Autor

Imagine que Alice deseja encaminhar uma mensagem confidencial para Bob, contudo eles não possuem uma chave secreta simétrica compartilhada entre eles. Deste modo, Alice pode prosseguir da seguinte forma:

1. Estrutura a mensagem.
2. Cria uma chave simétrica aleatória temporária (deverá ser utilizada somente uma vez).
3. Efetua a cifragem da mensagem utilizando criptografia simétrica com a chave secreta que deverá ser usada uma única vez.
4. Realiza a cifragem da chave secreta de uso único utilizando a criptografia assimétrica com a chave pública de Bob.
5. Por fim, anexa na mensagem a chave secreta (uso único) que está cifrada, então envia a mensagem cifrada para Alice.

Deste modo, apenas Bob conseguirá decifrar a mensagem contendo a chave de uso único, necessária para decifrar a mensagem original. Destaca-se que se Alice conseguiu a chave pública de Bob por meio do certificado de chave pública de Bob, então ela terá certeza de que esta chave pública é válida.

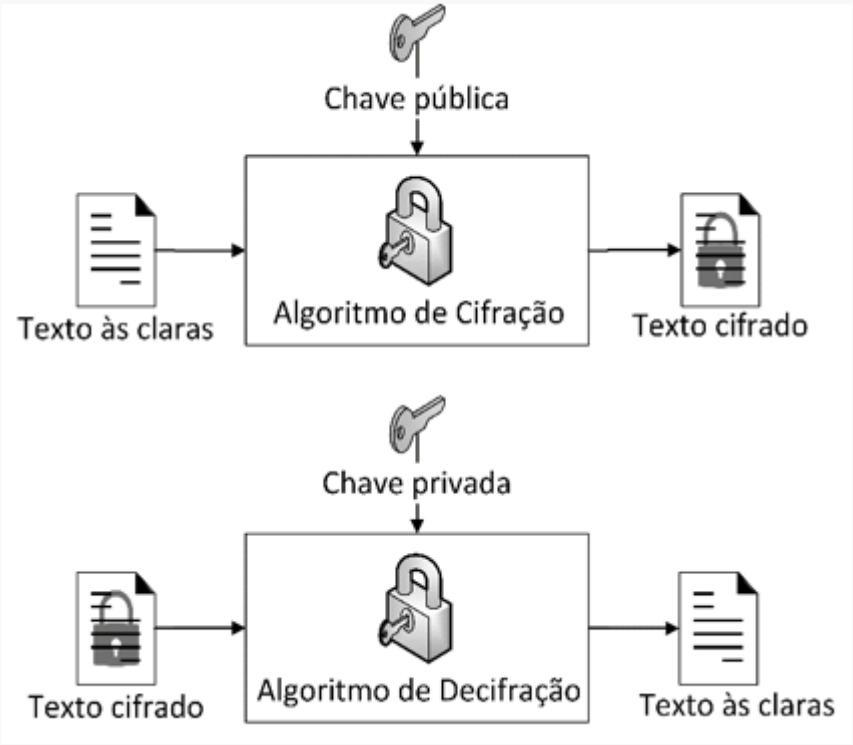
Cifração/Decifração

Os algoritmos de criptografia de chave pública utilizam sempre um par de chaves relacionadas, contudo distintas, uma das chaves utilizada para cifrar e outra por sua vez para decifrar. Destaca-se, que a chave utilizada para decifrar não pode ser obtida a partir da análise da chave de cifragem. Nos algoritmos de chave pública, as chaves são criadas sempre em pares: uma para cifrar e a outra para decifrar.

Conforme já discutido, a chave utilizada para cifrar a mensagem é denominada chave pública, esta chave pode ser divulgada para o transmissor da mensagem. Em contrapartida, a chave utilizada para decifrar a mensagem é conhecida como chave privada, esta chave deve ser guardada em segredo, pertencente ao receptor e não deve ser divulgada.

A característica fundamental do algoritmo assimétrico é que a chave pública pode ser distribuída livremente. A chave privada é a única maneira de decifrar uma mensagem que foi cifrada com a chave pública. Desta maneira, apenas o receptor da mensagem será capaz de decifrar a mensagem de qualquer indivíduo que utilize a sua chave pública para cifrar a mensagem. Assim, cada usuário possui uma chave pública e outra privada.

A figura abaixo demonstra o processo de cifragem e decifragem utilizando um algoritmo de criptografia de chave pública. Observe que na cifragem, o usuário emissor utiliza a chave pública do receptor como entrada para o algoritmo de criptografia, em conjunto com o texto às claras. Em contrapartida, na decifragem, o receptor, ao receber a texto cifrado, utiliza a sua chave privada (chave que apenas ele deve conhecer) como entrada para o algoritmo de criptografia, como resultado obtém o texto às claras.



Fonte: Autor

Os algoritmos de criptografia de chave pública possuem algumas limitações em relação ao desempenho, porque exigem alto nível de processamento, o que os torna muito mais lentos do que os algoritmos simétricos. Neste sentido, uma estratégia bem interessante é utilizar os dois tipos de algoritmos em conjunto, isto permite aproveitar os pontos fortes de cada algoritmo e reduzir os pontos fracos de ambos os tipos de criptografia.

Ao retomar o cenário de estudo do banco de Tóquio (introduzido na Unidade 1) neste ponto, podemos enfatizar a importância de combinar as diferentes abordagens de criptografia para obter um sistema mais seguro. O incidente no banco de Tóquio poderia ter sido evitado se tivessem sido utilizados algoritmos de criptografias adequados ao cenário do banco. O malware disseminado no banco, só conseguiu “quebrar” as senhas dos usuários do sistema de forma rápida, devido os sistemas utilizarem criptografia simétrica com tamanho de chaves de 56 bits, este fator associado com a definição de senhas fracas possibilitou um ataque bem-sucedido.

Distribuição de Chaves Pública

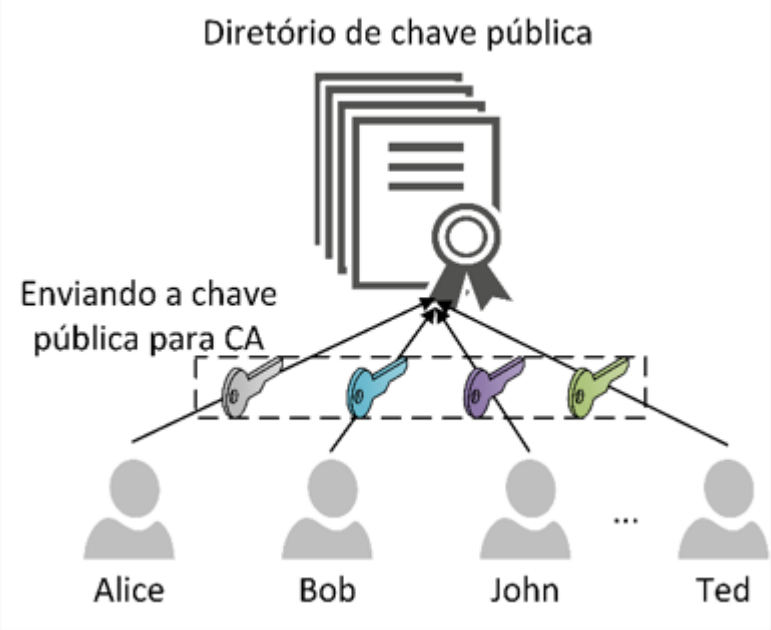
Existem algumas abordagens utilizando a criptografia assimétrica projetada para fornecer um esquema de distribuição de chaves públicas. Em geral, tais abordagens podem ser classificadas em um dos seguintes grupos:

- Diretório de chaves disponível publicamente;

- Autoridade de chave pública (CA);
- Certificados de chave pública;
- Anúncio público.

Diretório de Chaves Disponível Publicamente

A estratégia de utilizar um diretório dinâmico para conceder as chaves públicas fornece um nível maior de segurança. Contudo, o processo de gerenciamento e distribuição das chaves no diretório público deve ser atribuído a uma entidade confiável de fé pública, em geral uma instituição governamental ou financeira. A abordagem de um diretório da distribuição de chaves públicas é representada na figura abaixo:



Fonte: Autor

As etapas fundamentais são demostradas as seguir:

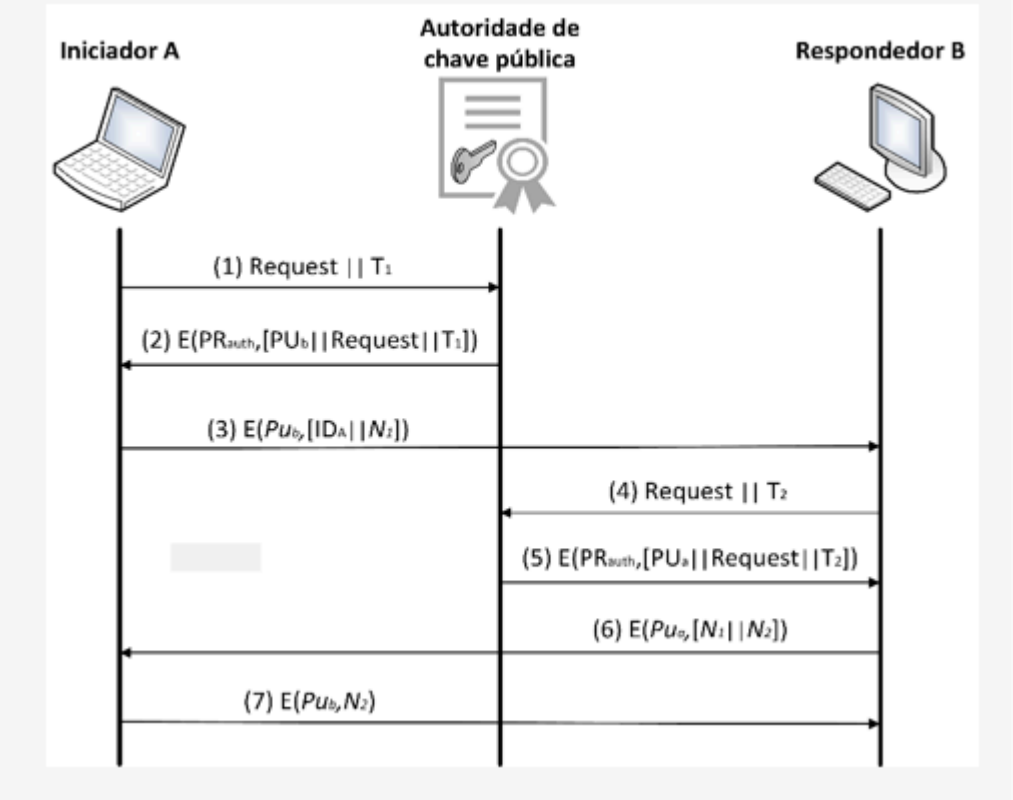
1. Cada usuário deve conceber um par de chaves que será utilizado para o processo de cifragem e decifragem das mensagens.
2. O usuário deve alocar uma das duas chaves em um registrador público ou utilizar outro meio para disponibilizar esta chave, esta chave é denominada como chave pública. A outra chave deve ser mantida em segurança, esta chave é denominada como chave privada. Adicionalmente, cada usuário mantém um conjunto de chaves públicas de outros usuários.
3. Caso Alice deseje enviar uma mensagem secreta para Bob, ela cifra a mensagem utilizando a chave pública de Bob.

4. Quando Bob receber a mensagem, ele utiliza a chave privada para decifrar a mensagem. Destaca-se que nenhum outro indivíduo conseguirá decifrar a mensagem, pois somente Bob conhece a chave privada.

Esta abordagem fornece um nível considerável de segurança, contudo ainda assim este esquema possui fraquezas. Caso um adversário consiga obter acesso a chave privada da autoridade do diretório, a comunicação entre todos os participantes estaria comprometida. O adversário poderia falsificar a chave pública de qualquer um dos participantes além de espionar as mensagens enviadas pelos demais participantes. Ainda, outra vulnerabilidade que o adversário poderia explorar, são os registros mantidos pela autoridade.

Autoridade de Chave Pública

Um mecanismo de segurança mais forte para distribuição de chave pública pode ser alcançado com a adoção de controles mais rigorosos no processo de distribuição de chaves públicas utilizando um diretório. Um cenário típico foi apresentado por Popek, esquematizado na figura adaptada de [Popek e Kline,1979] a seguir:



Fonte: Adaptado de: Popek e Kline, 1979

O cenário exposto considera que uma autoridade central gerencia um diretório de chaves públicas. Ainda, é necessário que cada participante tem acesso seguro a chave pública da autoridade responsável, enfatizando que somente a autoridade responsável deve ter acesso a

chave privada correspondente. As seguintes etapas são expostas por Popek:

1. O usuário A envia uma mensagem com *timestamp* à autoridade de chave pública, solicitando a chave pública do usuário B.

2. A autoridade responde com uma mensagem que é cifrada utilizando a chave privada da autoridade. Assim, o usuário A é capaz de decifra a mensagem utilizando a chave pública da autoridade. Desse modo, o usuário A tem certeza de que a mensagem foi originada pela autoridade. A mensagem inclui o seguinte:

- A chave pública do usuário B, que o usuário A pode utilizar para cifrar a mensagens destinadas ao usuário B.
- A solicitação original, para permitir que o usuário A compare essa resposta com a solicitação anterior, verificando se a solicitação original não foi modificada antes do recebimento pela autoridade.
- O *timestamp* original, para que o usuário A possa determinar que essa mensagem não é antiga da autoridade, contendo uma chave diferente da chave pública atual do usuário B.

3. O usuário A armazena a chave pública do usuário B utilizada para cifrar uma mensagem para o usuário B, contendo um identificador do usuário A e um *nonce*, utilizada para identificar essa transmissão exclusivamente.

4. O usuário B obtém a chave pública do usuário A na autoridade da mesma forma como o usuário A obteve a chave pública do usuário B.

5. Idem as etapas realizadas pelo usuário A para obter a chave (passos 1 e 2).

Até este ponto, as chaves públicas foram fornecidas com segurança ao usuário A e usuário B, agora eles podem iniciar a troca de mensagens de forma segura. Entretanto, duas etapas adicionais apresentadas na sequência são desejadas:

6. O usuário B envia uma mensagem ao usuário A (cifrada com a chave pública do usuário A) e contendo o *nonce* do usuário A, além de um novo *nonce* gerado pelo usuário B. Como somente o usuário B poderia ter decifrado a mensagem (etapa 3), a presença de primeiro *nonce* na mensagem (etapa 6) permite garantir ao usuário A que o seu correspondente (com quem está trocando mensagem) é o usuário B.

7. O retorno do segundo *nonce* cifrado, utilizando a chave pública do usuário B, permite garantir ao usuário B que o seu correspondente é o usuário A.

CURIOSIDADE

Timestamp - é um instante único de tempo que permite determinar a ocorrência de um evento.

Nonce - é um número arbitrário que só pode ser usado uma vez.

Observe que para realizar uma comunicação segura são necessários um total de troca de sete mensagens. Contudo, as primeiras quatro mensagens são utilizadas com pouca frequência, pois tanto o usuário A quanto o usuário B podem salvar a chave pública um do outro para utilização futura, esta técnica é conhecida como *caching*. Devemos ressaltar, que os usuários devem solicitar periodicamente cópias recentes das chaves públicas de seus correspondentes, visando garantir sempre que as chaves públicas sejam atuais.

Certificados de Chave Pública

O aumento na quantidade de usuário e requisições realizadas na autoridade de chave pública pode ocasionar um gargalo no sistema, pois cada usuário deverá contatar a autoridade responsável a fim de obter a chave pública do usuário com quem pretende se comunicar. Ressalta-se que o diretório de nomes e chaves pública também pode ser vulnerável à violação. Como alternativa, é possível utilizar certificados para possibilitar que os usuários troquem as chaves públicas sem a necessidade de participar a autoridade de chave pública, propondo uma maneira para realizar as trocas de chaves que seja tão confiável quanto se a troca fosse realizada com a autoridade de chave pública.

Observando que um certificado consiste basicamente em três partes: a chave pública, um identificador do proprietário da chave (informações do usuário), e um bloco inteiro assinado por uma autoridade certificadora. Um determinado usuário pode solicitar um certificado para uma autoridade certificadora, para isto o usuário deve apresentar a sua chave pública de uma

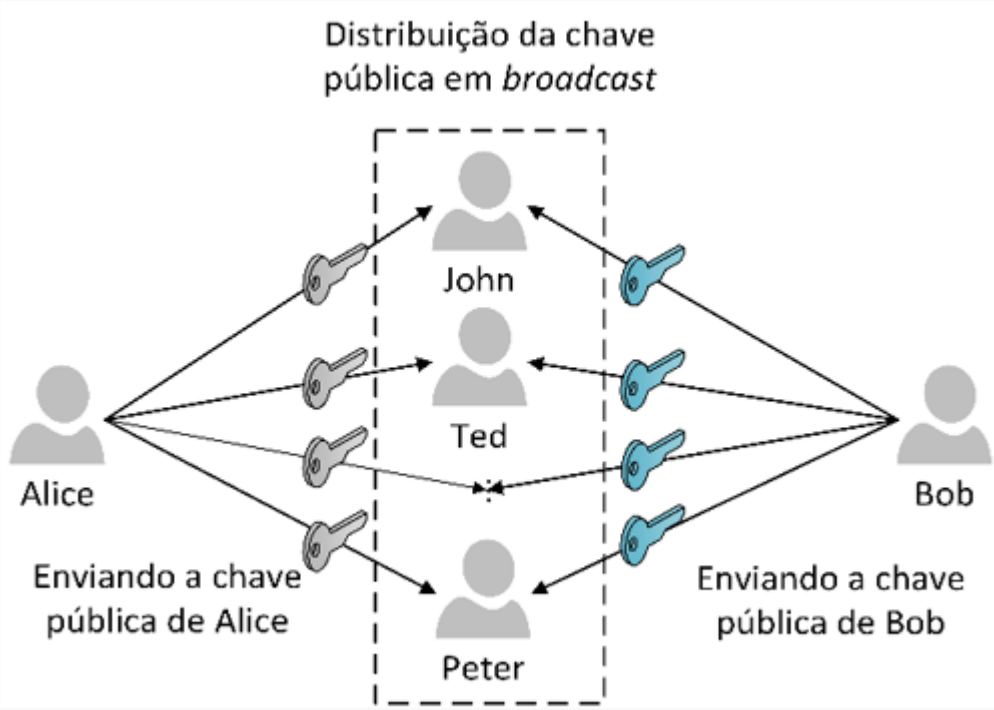
forma segura. Posteriormente, o usuário torna público este certificado. Deste modo, qualquer outro usuário que necessite utilizar a chave pública desse usuário poderá verificar se a chave é válida por meio da assinatura confiável a ele anexado. Os demais participantes também podem gerar seus próprios certificados junto a autoridade certificadora. Consequentemente, cada participante pode consultar se as demais chaves públicas são válidas verificando se o certificado foi realmente criado por uma autoridade confiável. Alguns requisitos devem ser avaliados neste processo:

1. Todos os participantes podem ler o certificado para validar a identidade e a chave pública do proprietário do certificado;
2. Todos os participantes podem verificar se um determinado certificado foi gerado pela autoridade certificadora, garantindo que o certificado não foi falsificado;
3. Apenas a autoridade certificadora deve criar e atualizar os certificados;
4. Todos os participantes podem verificar se os certificados ainda são válidos.

Para que esta abordagem seja efetiva é necessário que cada participante solicite seu certificado válido junto a autoridade certificadora. Ressalta-se que esta demanda é imprescindível que seja realizada de forma segura, feita pessoalmente ou utilizando uma comunicação segura.

Anúncio Público

Utilizando um algoritmo de chave pública como o RSA, qualquer participante pode encaminhar sua chave pública para outro participante, ou ainda poderá transmitir as chaves por meio de *broadcast*, ou seja, enviar a chave pública para todos os participantes da comunidade. Na figura a seguir é demonstrada a distribuição da chave pública utilizando *broadcast*.



Fonte: Autor

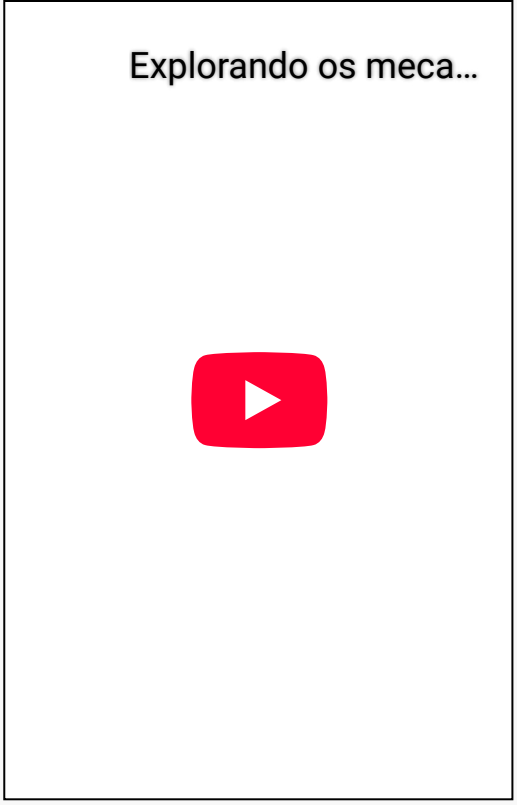
Uma ferramenta bastante popular que utiliza o algoritmo RSA é o PGP (*Pretty Good Privacy*), diversos usuários adotam a prática de disponibilizar sua chave pública em anexo em *posts* em fóruns públicos apropriados.

Apesar desta técnica ser conveniente, de uma certa maneira, ela possui vulnerabilidades, pois, qualquer indivíduo mal-intencionado pode falsificar este anúncio público. Para o adversário seria tarefa simples, ele poderia fingir ser um determinado usuário e enviar uma chave pública falsificada para outro participante ou ainda em *broadcast*. Até que o usuário autêntico que possui aquela identidade que está sendo falsificada descubra a falsificação e avise os demais participantes, o adversário já teve acesso as mensagens que foram enviadas cifradas para este usuário, além do adversário poder utilizar a chave falsificada para fins de autenticação.

Explorando os mecanismos de criptografia simétrica e assimétrica

Este vídeo fornecerá uma visão mais ampla sobre os mecanismos de criptografias simétricos e assimétricos, vamos apresentar os elementos fundamentais associados a cada um dos algoritmos, quais as vantagens e

desvantagens de utilizar estas abordagens, dicas e boas práticas para implementação destes mecanismos de segurança.



EXERCÍCIO

Exercícios de Fixação

Descreva com suas palavras como funciona o algoritmo de criptografia simétrica.

Quais os elementos fundamentais da criptografia simétrica?

Quais os dois requisitos necessários para utilização da criptografia simétrica de forma segura?

Quais os principais tipos de ataques direcionados a criptografia simétrica?

Cite 3 algoritmos de criptografia simétrica.

Quais os problemas relacionados a distribuição das chaves na criptografia simétrica?

O que é um KDC, e para que é utilizado?

Qual a diferença da chave mestra e chave de sessão no KDC?

Descreva com suas palavras como funciona o algoritmo de criptografia assimétrica.

Quais os elementos fundamentais da criptografia assimétrica?

Cite 3 algoritmos de criptografia assimétrica.

Cite 3 aplicações para criptografia de chave pública.

Para que é utilizado a assinatura digital?

O que é uma CA?

Para que é utilizado um certificado de chave pública?

Para que serve os envelopes digitais?

Quais são as principais abordagens para distribuição das chaves públicas?

Conclusão

Esta unidade abordou os mecanismos de criptografia simétrica e assimétrica. Descobrimos que na criptografia simétrica o emissor e receptor compartilham a mesma chave secreta. Conforme discutido, esta chave é utilizada tanto para cifrar como decifrar uma mensagem. Destacamos a importância de proteger e preservar a chave secreta. Exploramos os princípios da cifração simétrica, onde foram apresentados os cinco elementos fundamentais da criptografia simétrica, o texto às claras, algoritmo de cifração, chave secreta, algoritmo de decifração e texto cifrado. Ainda, foi apresentado as principais características do algoritmo de cifração simétrica. Constatamos que o adversário pode explorar duas técnicas para atacar um sistema de criptografia simétrica, através de um ataque de criptoanálise ou utilizando um ataque de força bruta, então mostramos quais as contramedidas necessárias.

Por conseguinte, apresentamos os principais algoritmos de criptografia simétrica adotados como padrão pelo NIST, o algoritmo DES, Triplo DES e AES. Demonstramos a evolução dos algoritmos de criptografia simétrica e as limitações de cada algoritmo. Ainda, mostramos que o tamanho da chave secreta utilizada para cifrar uma mensagem reflete no tempo necessário para "quebrar" a mensagem que foi cifrada com essa chave. Enfatizamos a importância de proteger e armazenar corretamente a chave secreta. De acordo com o que estudamos, uma das grandes limitações da criptografia simétrica é justamente a distribuição das chaves secretas. Discutimos o cuidado que devemos ter para compartilhar esta chave de maneira segura. Conforme estudamos o KDC é considerado a melhor opção para compartilhar a chave secreta na rede. Adicionalmente, abordamos a hierarquia de chaves necessária para troca de chaves utilizando o KDC.

Exploramos também a criptografia de chave pública, as principais características e os elementos fundamentais deste mecanismo. Conforme discutido, verificamos que a criptografia assimétrica trabalha com um par de chaves, uma chave pública e a outra privada. Verificamos que um texto cifrado com uma das chaves somente poderá ser decifrado pela outra chave correspondente. Descobrimos que a chave privada é exclusiva do proprietário, não deve ser divulgada, apenas ele deve ter acesso a esta chave. Por sua vez, a chave pública pode ser distribuída para os participantes. Adicionalmente, apresentamos os principais algoritmos de criptografia de chave pública, o algoritmo RSA, Diffie-Hellman, DSS e as Curvas elípticas. Entre as aplicações de criptografia, mostramos como é estruturado os algoritmos assinatura digital, autenticação de mensagens, certificados de chave pública, envelopes digitais, e outras aplicações.

Por fim, demonstramos vulnerabilidades que os adversários podem explorar, associadas ao uso dos mecanismos de criptografia, mas sobretudo as estratégias e boas práticas para contorná-las. Descobrimos as vantagens e desvantagens de utilizar as criptografias simétrica e assimétrica. Discutimos sobre os desafios do profissional de segurança da informação para implementar tais mecanismos. Deste modo, demonstramos como podemos combinar diferentes algoritmos de criptografia para propor um cenário de segurança mais robusto e adequado ao contexto de cada organização.

Referências Bibliográficas

DIFFIE, W. **The First Ten Years of Public-Key Cryptography**. Proceedings of the IEEE, mai. de 1988.

LEUTWYLER, K. **Superhack**. Scientific American, jul. 1994.

NIST. **FIPS PUB 171 - Federal Information Processing Standards Publication**. National Institute of Standards and Technology (NIST), 1992. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>. Acesso em: 21 de jul. de 2021.

NIST. **FIPS PUB 186 - Federal Information Processing Standards Publication**. National Institute of Standards and Technology (NIST), 1994. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub186.pdf>. Acesso em: 21 de jul. de 2021.

NIST. **FIPS PUB 197 - Federal Information Processing Standards Publication**. National Institute of Standards and Technology (NIST), 2001. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>. Acesso em: 21 de jul. de 2021.

NIST. **FIPS PUB 46 - Federal Information Processing Standards Publication**. National Institute of Standards and Technology (NIST), 1988. Disponível em: <https://csrc.nist.gov/CSRC/media/Publications/fips/46/1/archive/1988-01-

22/documents/NBS.FIPS.46-1.pdf>. Acesso em: 21 de jul. de 2021.

NIST. **FIPS PUB 46-2 - Federal Information Processing Standards Publication**. National Institute of Standards and Technology (NIST), 1993. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub46-2.pdf>. Acesso em: 21 de jul. de 2021.

NIST. **FIPS PUB 46-3 - Federal Information Processing Standards Publication**. National Institute of Standards and Technology (NIST), 1999. Disponível em: <https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf>. Acesso em: 21 de jul. de 2021.

POPEK, G.; KLINE, C. **Encryption and Secure Computer Networks**. ACM Computing Surveys, dez 1979.

RIVEST, R. SHAMIR, A. ADLEMAN, L. A **Method for Obtaining Digital Signatures and Public Key Cryptosystems**. Communications of the ACM, fev. 1978.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas**. São Paulo: Pearson Prentice Hall, 2008.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores: princípios e práticas**. Rio de Janeiro: Elsevier Campus, 2014.