Universidade Federal de Viçosa
Instituto de Ciência Exatas e Tecnológicas
CCF 321 - Projeto de Sistemas Para Web

Trabalho 03

Autenticação

Igor Lucas dos Santos Braz Matrícula: 3865
Pedro Cardoso de Carvalho Mundim Matrícula: 3877

Professor:
Jeverson Ricardo Nery Silva dos Santos

24 de junho de 2022

Autenticação e Criptografia

"O termo "criptografia" provém das palavras gregas kryptos (oculto, secreto) e graphos (escrever). Assim, a criptografia foi criada para codificar informações, de forma que somente as pessoas autorizadas pudessem ter acesso ao seu conteúdo."

Atualmente, golpistas estão se tornando cada vez mais presentes, afetando milhões de usuários, no que diz respeito ao uso de tecnologia da informação. Para impedir o roubo de nossos dados, precisamos usufruir da técnica de criptografar. Existem três técnicas de criptografia, a saber, Criptografia simétrica, Criptografia assimétrica e funções Hash (sem chave).

Os dois métodos de criptografia (simétrica e assimétrica) usam chaves para criptografar e descriptografar dados. A **criptografia simétrica** usa a mesma chave para criptografar e descriptografar dados, facilitando o uso. A **criptografia assimétrica** usa uma chave pública para criptografar dados e uma chave privada para descriptografar informações.

Criptografia Simétrica

A **criptografia simétrica**, também conhecida como criptografia de chave secreta, como comentado anteriormente, utiliza uma única chave para criptografar e descriptografar dados. Essa chave precisa ser compartilhada com o destinatário. Exemplo: Suponha que você queira enviar uma mensagem para algum amigo. Primeiramente, você deve escrever a mensagem e definir uma chave secreta para criptografá-la. Em seguida, quando o destinatário receber a mensagem, ele precisará inserir a chave secreta para descriptografar a mensagem. A Figura 1 ilustra esse tipo de criptografia.

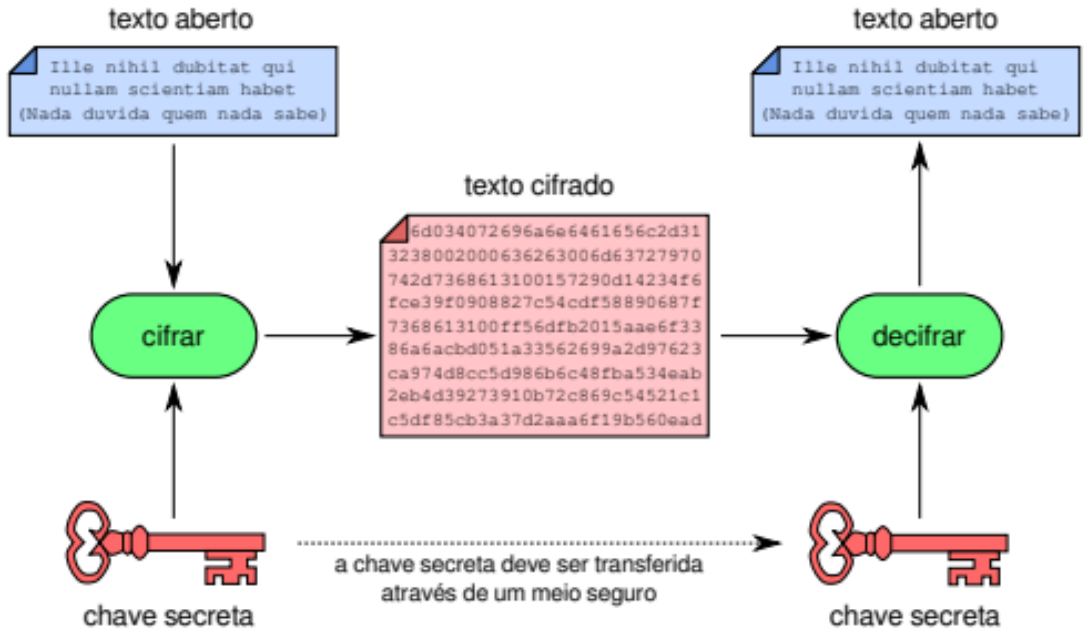

Figura 1: Criptografia Simétrica. Fonte: Livro - Sistemas Operacionais: Conceitos e Mecanismos

Vejamos agora as vantagens e desvantagens desse tipo de criptografia.

As **vantagens** do método de criptografia simétrica são: é muito fácil de configurar e pode ser feito rapidamente. Além disso, é bem simples, todas as idades e origens podem entender e usá-lo. A criptografia assimétrica é mais difícil de compreender e usar.

A **desvantagem** é que a chave secreta precisa ser compartilhada com o destinatário. No caso do PEM, a chave secreta é criptografada com a senha do usuário, apenas certifique-se de que a senha não seja facilmente adivinhada. Se você usar a mesma chave secreta para

criptografar todos os seus e-mails e se alguém descobrir essa chave secreta, todos os seus e-mails criptografados serão comprometidos.

Com o que foi exposto em mente, podemos ver agora alguns tipos de criptografias simétricas existentes.

- **IDEA** - O Internacional Encryption Algorithm (IDEA) é uma chave simétrica desenvolvida em 1991, que opera blocos de informações de 64 bits e usa chaves de 128 bits. O algoritmo utilizado atua de forma diferente, pois usa a confusão e difusão para cifrar o texto. Na prática, ele utiliza três grupos algébricos com operações misturadas.
- **SAFER** - SAFER ("mais seguro" em português). Consiste na criptografia de blocos em 64 bits, por isso é conhecido como SAFER SK-64. Entretanto, foram encontradas fraquezas nesse código, o que resultou no desenvolvimento de novas versões.
- **DES** - Data Encryption Standard (DES) é uma das primeiras criptografias utilizadas e é considerada uma proteção básica de poucos bits (cerca de 56). O DES pode ser decifrado com a técnica de força bruta (o programa testa as possibilidades de chave automaticamente durante horas). Por essa razão, os desenvolvedores precisam buscar alternativas de proteção mais complexas além do DES.
- **3DES** O Triple DES foi originalmente desenvolvido para substituir o DES, já que os hackers aprenderam a superá-lo com relativa facilidade. Essa criptografia recebe esse nome pelo fato de trabalhar com três chaves de 56 bits cada, o que gera uma chave com o total de 168 bit. Especialistas no tema argumentam que uma chave de 112 bits é suficiente para proteger os dados.
- **Blowfish** - Esse é outro algoritmo desenvolvido para substituir o DES. É uma cifra simétrica que divide as informações em blocos de 64 bits e criptografa cada um deles individualmente. O Blowfish é conhecido por sua velocidade de encriptação e efetividade em geral. Trata-se de uma tecnologia bastante segura, pois há estudiosos no assunto que afirmam que o código não pode ser quebrado. De forma geral, o Blowfish é usado em plataformas de e-commerce para garantir segurança nos pagamentos e proteger senha de acesso dos usuários.
- **CAST-128 (alternativamente CAST5)** - É uma cifra de bloco de chave simétrica usada em vários produtos, principalmente como a cifra padrão em algumas versões de GPG e PGP. Também foi aprovado para uso do Governo do Canadá pelo Communications Security Establishment.
- **AES** - Advanced Encryption Standard (AES) — ou Padrão de Criptografia Avançada, em português — é o algoritmo padrão do governo dos Estados Unidos e de várias outras organizações. Ele é confiável e excepcionalmente eficiente na sua forma em 128 bits, mas também é possível usar chaves e 192 e 256 bits para informações que precisam de proteção maior. O AES é amplamente considerado imune a todos os ataques, exceto aos ataques de força bruta.
- **OTP** - Consiste em um algoritmo em que o purotexto é combinado, caractere por caractere, a uma chave secreta aleatória que para isso deve ter, no mínimo, o mesmo número de caracteres do purotexto. Para garantir que a criptografia seja imperscrutável, a chave só deve ser usada uma única vez, sendo imediatamente destruída após o uso.

Criptografia Assimétrica

A **criptografia assimétrica** requer duas chaves para funcionar. Em primeiro lugar, uma chave pública deve ser tornada pública para criptografar os dados. Em segundo lugar, uma chave privada usada para descriptografar os dados.

As chaves pública e privada não são a mesma coisa. Você cria sua mensagem e depois a criptografa com a chave pública do destinatário. Depois disso, se o destinatário quiser descriptografar a mensagem, ele terá que fazer isso com sua chave privada. Ou seja, é necessário um conhecimento maior do que a pessoa comum para fazer isso acontecer. O software de email do destinatário verá se a chave privada corresponde à chave pública e solicitará que o usuário digite a senha para descriptografar a mensagem. A Figura 2 ilustra esse tipo de criptografia.

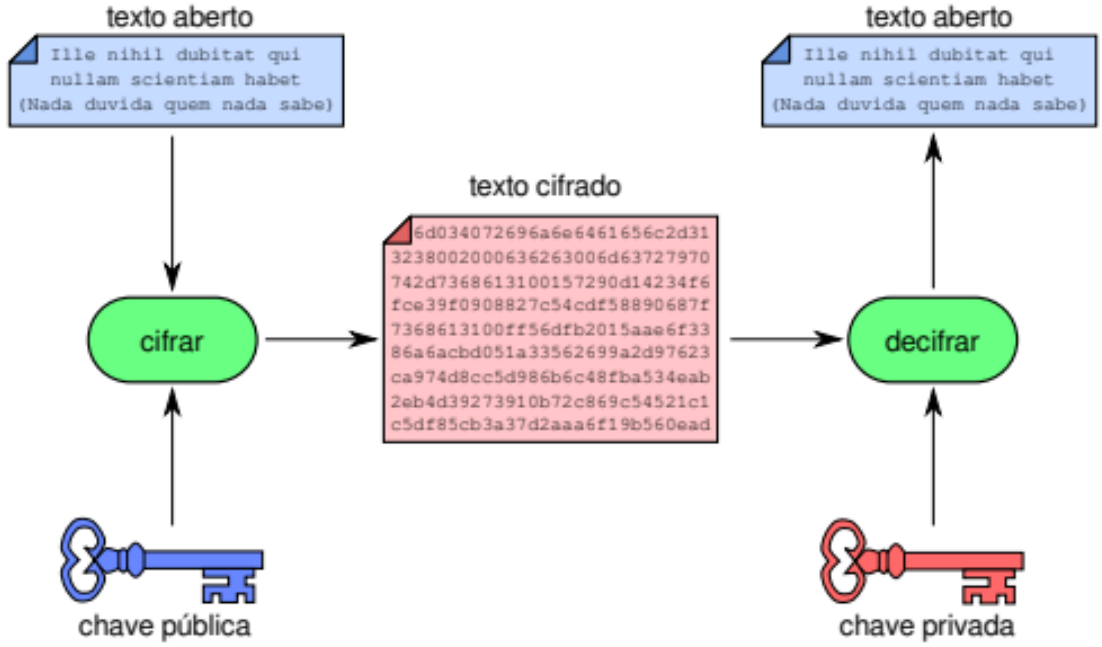

Figura 2: Criptografia Assimétrica. Fonte: Livro - Sistemas Operacionais: Conceitos e Mecanismos

Um exemplo prático de uso da criptografia assimétrica é mostrado na Figura 3 a seguir. Nele, a usuária Alice deseja enviar um documento cifrado ao usuário Bob. Para tal, Alice busca a chave pública de Bob previamente divulgada em um chaveiro público e a usa para cifrar o documento que será enviado a Bob. Somente Bob poderá decifrar esse documento, pois só ele possui a chave privada correspondente à chave pública usada para cifrá-lo. Outros usuários poderão até ter acesso ao documento cifrado, mas não conseguirão decifrá-lo.

Vejamos agora as vantagens e desvantagens desse tipo de criptografia.

A **vantagem** da Criptografia assimétrica é que ela não força o usuário a compartilhar chaves (secretas) como a criptografia simétrica, removendo, portanto, a necessidade de distribuição de chaves. A criptografia assimétrica oferece suporte à assinatura digital, que autentica a identidade do destinatário e garante que a mensagem não seja violada em trânsito.

Com o que foi exposto em mente, podemos ver agora alguns tipos de criptografias assimétricas existentes.

- **RSA** - Rivest-Shamir-Adleman (RSA) é considerado um dos algoritmos mais seguros do mercado, por essa razão também foi o primeiro a possibilitar a criptografia na assinatura digital. O RSA funciona da seguinte forma: ele cria duas chaves diferentes, uma pública e outra privada (que deve ser mantida em sigilo). Todas as mensagens podem ser cifradas pela pública, mas somente decifradas pela privada.
- **ElGamal** - É um algoritmo de criptografia de chave assimétrica para criptografia de chave pública que é baseado na troca de chaves Diffie-Hellman. A criptografia ElGamal é usada no software gratuito GNU Privacy Guard, nas versões recentes do PGP e em outros sistemas criptográficos. O Algoritmo de Assinatura Digital (DSA) é uma variante do esquema de assinatura ElGamal, que não deve ser confundido com a criptografia ElGamal.

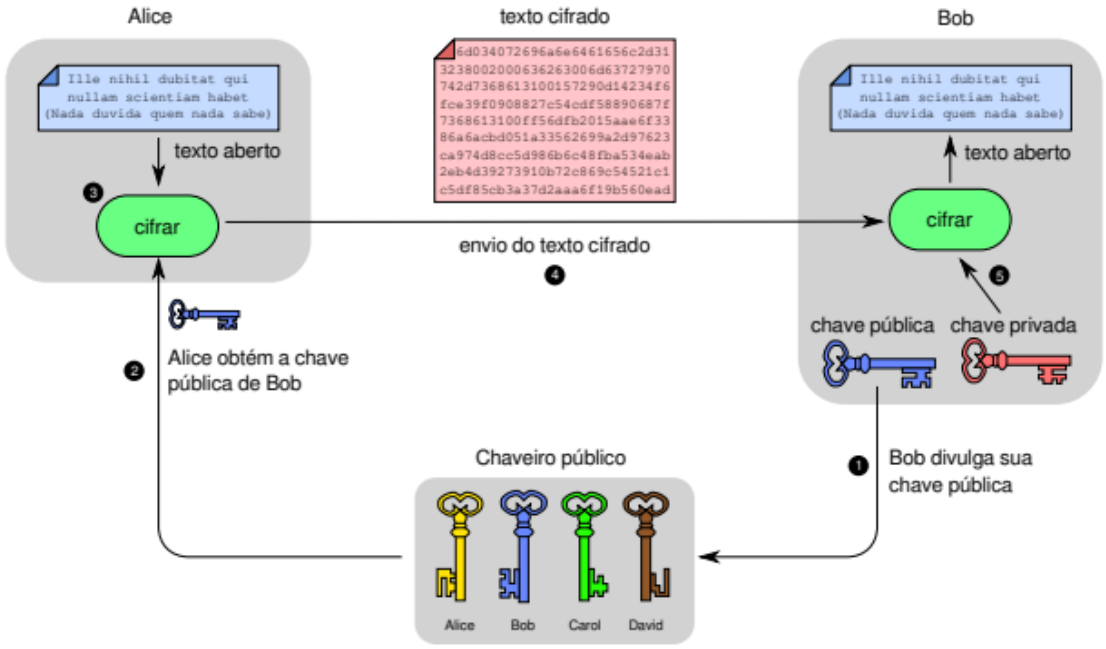

Figura 3: Criptografia Assimétrica. Fonte: Livro - Sistemas Operacionais: Conceitos e Mecanismos

Funções de Hash

Uma função de hash criptográfico, muitas vezes é conhecida simplesmente como **hash** – é um algoritmo matemático que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo. Independentemente do comprimento dos dados de entrada, o mesmo tipo de hash de saída será sempre um valor hash do mesmo comprimento. A Figura 4 ilustra o hash.

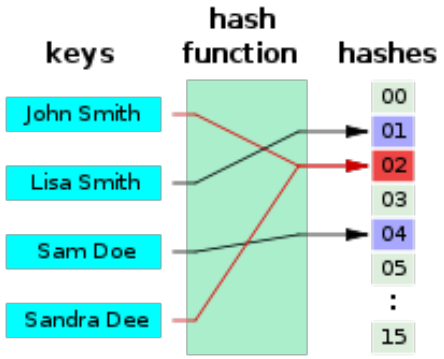

Figura 4: Criptografia por Hash. Fonte: wikipedia

O algoritmo Hash é conhecido como uma função matemática criptográfica, na qual você possui dados de entrada e, após passar pela criptografia, eles apresentam valores de saída "padronizados", ou seja, as saídas devem possuir o mesmo tamanho (geralmente entre 128 e 512 bits) e o mesmo número de caracteres alfanuméricos.

A função hash criptográfica é utilizada, principalmente, para resumir uma grande quantidade de informações em arquivos.

Imagine um banco de dados com muitas informações podendo ser resumido em uma única sequência de letras e números! Isso traz uma praticidade gigantesca dentro do mundo digital e da tecnologia da informação.

Uma função hash é caracterizada por:

- **Saída de tamanho fixo:** independente do valor de entrada, as saídas possuem a mesma quantidade de letras e números.
- **Eficiência de operação:** a função não pode ser complexa ao ponto de comprometer a velocidade de processamento.
- **Determinística:** um valor de entrada sempre possuirá a mesma saída.

Com o que foi exposto em mente, podemos ver agora alguns tipos de criptografias hash existentes.

- **MD5** - O MD5 (Message-Digest algorithm 5) é uma função de dispersão criptográfica de 128 bits unidirecional desenvolvido pela RSA Data Security, muito utilizado por softwares com protocolo ponto-a-ponto na verificação de integridade de arquivos e logins.
- **SHA1** - Produz um valor de dispersão de 160 bits (20 bytes) conhecido como resumo da mensagem. Um valor de dispersão SHA-1 é normalmente tratado como um número hexadecimal de 40 dígitos.
- **SHA2** - A função hash SHA-2 é implementada em algumas aplicações de segurança e protocolos amplamente usados, incluindo TLS e SSL. A família SHA-2 é composta por seis funções hash com resumos (valores de hash) que são de 224, 256, 384 ou 512 bits: SHA224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA512/256.
- **SHA-512** - É parte de um sistema para autenticar vídeos de arquivos do Tribunal Penal Internacional para o genocídio de Ruanda.
- **RIPEMD** - É uma versão melhorada das funções MD. As saídas do RIPEMD possuem 160 bits de tamanho, enquanto as saídas MD possuem 128 bits.

Nossa Experiência com Autenticação no Curso

Durante o curso de ciência da computação tivemos pouca experiência com criptografia. Atualmente, na disciplina de Sistemas Distribuídos, o conceito está sendo aplicado para o desenvolvimento de um sistema de escambo, para deixá-lo mais seguro contra agentes externos. Fora isso, no primeiro período tivemos um pouco de contato com a teoria sobre criptografia na disciplina de Matemática Discreta, mas nenhuma prática de implementação até o presente momento.

Referências

[Maziero,] Maziero, C. A. Sistemas operacionais: Conceitos e mecanismos i-conceitos básicos.