**Criptografia**

É a técnica responsável por cifrar a escrita, de maneira que permita a comunicação segura e confidencial entre duas partes sem que uma terceira tenha acesso a informação.

A palavra criptografia provém dos radicais gregos *kriptos* (oculto) e *grapho* (escrita), citada como uma arte, ciência, os estudos e aplicações destes métodos datam milhares de anos atrás. Como por exemplo a utilização da Cítala(Figura 1) pelos espartanos que consistia em uma tira de couro ou papiro envoltos em um bastão de madeira, de forma que as palavras eram escritas na horizontal. Tal tira era enviada ao outro participante da comunicação que por sua vez possuía um bastão de mesma espessura e enrolava a tira de forma que a cada volta uma letra da palavra iria aparecendo, reconstituindo a mensagem.

Figura 1 – Cítala

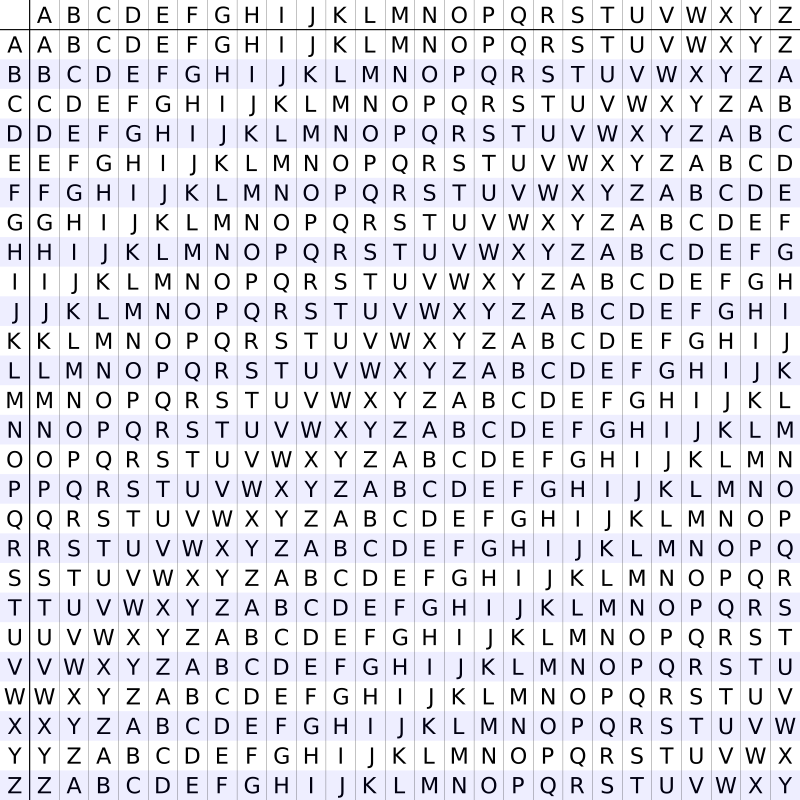


Fonte: Google Imagens - Cítala

Outro exemplo de forma de criptografia utilizada a milhares de anos é a cifra de Júlio César, onde as mensagens escritas pelo próprio imperador se utilizavam da técnica de substituição, onde pode-se trocar uma letra com a outra, embaralhar o alfabeto ou até mesmo criar um novo código para letras ou palavras. No caso de César eram alteradas três posições das letras do alfabeto, tal criptografia possui pouca ou nenhuma segurança nos dias atuais e pode ser facilmente decifrada por identificação de letras comuns e frequência de letras.

Giovan Batista Belaso e Blaise de Vigenére usam como base a cifra de César para no seculo XV criarem cifras mais complexas, utilizando um quadrado com o alfabeto como mostra a figura 2 e possuindo uma palavra-chave, que sera utilizada como base no momento da criptografia, dificultando a utilização da analise de frequência pois a cada letra da palavra-chave o alfabeto é modificado, tal método permaneceu considerado indecifrável por muito tempo.

Figura 2 – Quadrado de Vigenére



Fonte: Google imagens – Cifra de Vigenére

Por exemplo, se utilizarmos a palavra-chave “unicep” para criptografar a palavra faculdade teríamos o seguinte:

Texto: faculdade

Chave: unicep

Texto cifrado: ZNKWPSUQM

A analise combinatória e as chaves curtas utilizadas para criptografia permitiram tais métodos a serem decifrados manualmente e se tornarem cada vez menos seguros.

A maquina alemã Enigma utilizada durante a segunda guerra mundial dificultava tal atividade, já que utilizava três discos rotores para embaralhar as letras, por exemplo, a letra “A” era cifrada pela letra “K” em sua primeira utilização na frase, na segunda vez já seria uma outra letra, na terceira outra e assim por diante, dificultando muito a analise combinatória sem utilização de computadores, além do que a posição dos discos eram alterados ao fim do dia. Os créditos de quebrar a criptografia da Enigma é dado principalmente a Alan Turing e sua equipe com a construção do computador Bombe que realizava milhões de combinações e possibilitou a descoberta das chaves da Enigma, devido a um padrão conhecido nas mensagens. Feito este que segundo especialistas pode ter encurtado o período da segunda guerra em até um ano, devido a capacidade de interceptação das mensagens por parte dos aliados.

Como visto historicamente a privacidade, integridade e o controle de acesso a informação sempre foi valorizado e de suma importância para diversas atividades. Hoje não se faz diferente, é sempre necessário manter estes e outros aspectos como não-repudio, disponibilidade, autenticidade, na realização de tarefas de comunicação e transações. Um ótimo exemplo da utilização destes pontos em uma simples compra pela internet é dado por Oliveira (2012) “a informação que permite a transação valor e descrição do produto precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (disponibilidade), o valor da transação não pode ser alterado (integridade), somente o cliente que está comprando e o comerciante devem ter acesso à transação (controle de acesso), o cliente que está comprando deve ser realmente quem diz ser (autenticidade), o cliente tem como provar o pagamento e o comerciante não têm como negar o recebimento (não-repúdio) e o conhecimento do conteúdo da transação fica restrito aos envolvidos (privacidade).”

**Criptografia simétrica ou de chave privada**

Até o momento, observou-se a forma de criptografia simétrica ou de chave privada que, segundo Brown e Stallings 2017, era o único tipo em uso antes do desenvolvimento da encriptação por chave pública na década de 1970. Esse continua sendo de longe o mais usado dos dois tipos de encriptação.

Consiste na utilização de uma senha(chave) utilizada em conjunto do algoritmo para cifrar a informação desejada pelo remetente, e por sua vez o destinatário a utiliza para decifrar a informação, como por exemplo a cifra de Vigenére citada acima.

Para utilização do modelo, dois requisitos devem ser levados em consideração, algoritmo forte e chave de segurança não exposta. O primeiro para que mesmo possuindo o algoritmo utilizado e uma serie de textos cifrados e seus respectivos valores reais, não seja possível decifrar a mensagem enviada. O segundo por conta de que caso a chave seja descoberta por um oponente(termo utilizado para quem tenta decifrar a mensagem) a informação pode ser decifrada com uma facilidade enorme, já que os algoritmos geralmente são públicos, todas as mensagens anteriores e posteriores enviadas utilizando tal chave teriam sua segurança comprometida. Já com a segurança desta chave garantida um ataque de força bruta, dependendo o tamanho da chave utilizada seria inviável.

Uma das técnicas utilizadas por cripto analistas é a busca pelo texto claro, uma parte do texto conhecida e que facilitaria no processo de decifrar a mensagem escolhida. Por exemplo um documento que possua sempre o mesmo cabeçalho, o analista pode ser capaz de descobrir a chave através da forma que o texto conhecido é cifrado.

Diante de técnicas como esta entre outras mais existentes para tentativa de quebra de mensagens cifradas, são definidas duas máximas que os desenvolvedores devem se ater ao desenvolver algum algoritmo de criptografia (BROWN,STALLINGS. 2017):

- O custo para quebrar a cifra ultrapassa o valor da informação encriptada.

- O tempo exigido para quebrar a cifra supera o tempo de vida útil da informação.

Desta forma sendo considerado seguro o algoritmo que conseguir tornar o custo pela informação alto o suficiente para que não seja valido, ou seja, demandar, por exemplo, muito processamento, recursos computacionais e humanos e tecnologia para uma informação que não tenha o mesmo preço. Ou que leve tanto tempo para ser decifrado que a informação já não tenha mais grande valia ao oponente.

**Algoritmos**

*DES(Data Encryption Standard)*

- Criado pela IBM em 1977

- De tamanho 56 bits, o que permite quadrilhões de combinações, porem considerado pequeno pois foi quebrado em 1997 por força bruta

- Um dos mais disseminados no mundo até a padronização do AES

*AES(Advanced Encryption Standard)*

- Cifra de bloco

- Anunciado pelo National Institute of Standards and Technology(NIST) em 2003

- É um dos algoritmos mais populares, desde 2006, usado para criptografia de chave simétrica

- Substituto do DES

- Possui chave de 128, 192 ou 256 bits

- Bloco fixo em 128 bits

- Fácil de executar e rápido, exige pouca memoria

*Twofish*

- Twofish é de uso livre para quem desejar utilizar sem restrição

- Cifra de bloco de 128 bits

- Possui chave variável de 128, 192 ou 256 bits

- Bastante veloz

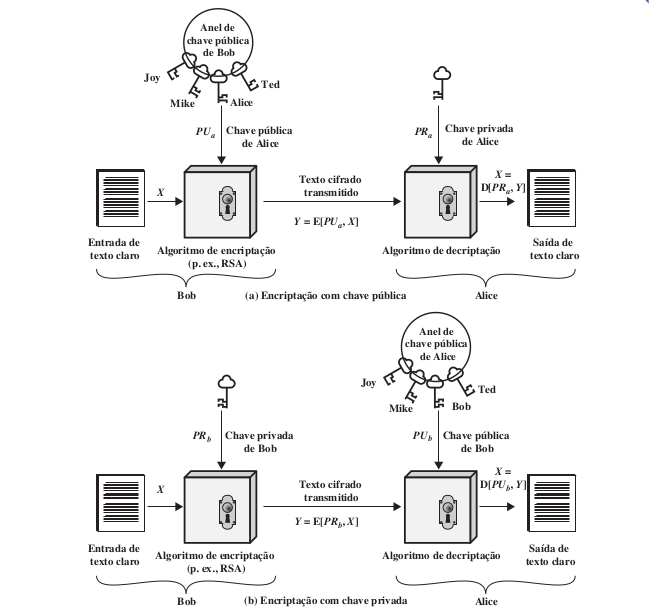
**Criptografia assimétrica ou chave pública**

Como descrito por Oliveira (2012) o método de criptografia assimétrica é onde cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Método este que para Brown e Stallings (2017) talvez represente a maior revolução em milênios das técnicas de criptografia, já que as técnicas utilizadas até então se prendiam a substituição e permutação de caracteres, que detém seus méritos e efetividade. As técnicas assimétricas se utilizam de funções matemáticas, além de que possui duas chaves o que altera concepções nas áreas de distribuição, confiabilidade e autenticação.

Seu funcionamento(Figura3), consiste na elaboração de duas chaves diferentes porém relacionadas, onde uma deve ser publica, ou seja, qualquer pessoa interessada em enviar uma mensagem a este destinatário poderá obtê-la e uma chave privada que sera utilizada para decifrar a mensagem previamente cifrada, esta deve ficar somente em posse de um único dono. Se um oponente obtiver a mensagem e a chave publica não será possível decifrar a mensagem, desta forma nem o remetente real conseguirá decifrá-la posterior processo de encriptação, tornando esta tarefa possível apenas para o detentor da chave privada relacionada a chave publica utilizada em conjunto ao algoritmo para obtenção do texto cifrado.

Algumas observações errôneas a respeito da criptografia assimétrica são feitas comumente, uma delas é de que este método é mais seguro contra criptoanalise em comparação a metodologia simétrica, o que não é verdade, já que depende do tamanho da chave e também do trabalho computacional envolvido, em ponto algum conseguimos apontar benefícios de uma sobre a outra em relação a criptoanalise.

A segunda seria em relação ao fim da utilização das técnicas simétricas devido a criação das assimétricas pois possuirão uso geral, mas ao contrario do que se parece devido ao grande necessidade computacional das técnicas assimétricas, não existe probabilidade previsível de que a criptografia simétrica seja abandonada e como citado inclusive por um dos criadores da técnica, “a restrição da criptografia de chave pública às aplicações de gerenciamento de chave e assinatura é aceita quase universalmente”(BROWN, STALLINGS,2017).

Figura 3 – Etapas da criptografia de chave publica

Fonte: Segurança de computadores: princípios e práticas (2017)

**Algoritmos**

*RSA*

- Tem este nome devido as iniciais do sobrenome de seus criadores Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT

- Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento

- Para gerar as chaves se utiliza multiplicação de números primos grandes, o que é fácil, porém para a chave privada exige-se fatoração deste numero absurdamente grande, o que impossibilita sua execução em tempo razoável

- Muito utilizada para emissão de certificados digitais

*ElGamal*

- Envolve manipulação de grandes quantidades numéricas

- Se utiliza de problemas matemáticos complexos, porém diferentemente do RSA, se aproveita da dificuldade de se calcular logaritmos discretos em um corpo finito.

*Diffie-Hellman*

- Também utiliza o problema dos logaritmos discretos, porém não é utilizada para cifra, mas sim para dois indivíduos entrarem em acordo ao compartilharem um segredo tal como uma chave

**Certificados e Assinaturas Digitais**

A criptografia de chave publica também atua em métodos para emissão de certificados digitais, que são chaves publicas assinadas por alguém de confiança. Tal aplicação tem a função de evitar problemas onde um oponente pode tentar convencer dois interlocutores de que uma chave publica falsa gerada por ele é a chave de uma das pessoas que querem estabelecer comunicação, interceptando assim a informação. Geralmente são gerenciados por órgãos como, por exemplo, ICP-Brasil(AC-Raiz), erasa Experian (AC-SERASA), Caixa Econômica Federal (AC-CAIXA), entre outros no Brasil.

Já a assinatura digital, é a técnica de criptografar uma mensagem conhecida com a chave privada de uma pessoa, de forma que alguém que necessite desta assinatura se utilize de sua chave publica para decifrar a mensagem e realmente garantir que foi assinada por aquele indivíduo.

**Conclusão**

Foi observado que o uso da criptografia data de milhares de anos atrás e continua sendo de suma importância para garantir confidencialidade, confiabilidade entre as comunicações atuais. Existem diversas aplicações para seus algoritmos e técnicas, tais como, utilização hibrida de chaves simétrica e assimétrica, hashing, entre outros aspectos matemáticos que não foram citados neste sumário, também fazem parte da ciência da criptografia.

A escolha do melhor método, melhor algoritmo depende da aplicação que será feita com a técnica, deve-se sempre lembrar de dois princípios acima citados, referente ao custo computacional, de dinheiro e de tempo empenhados para decifrar uma mensagem criptografada, sua técnica deve ter segurança suficiente para demandar muito esforço para se decifrar uma mensagem.

**Referencia bibliográfica**

BROWN, Lawrie; STALLINGS, William. **Segurança de computadores: princípios e práticas**. Elsevier Brasil, 2017.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, v. 31, p. 11-15, 2012.

Criptografia | Nerdologia Tech. Disponivel em: https://www.youtube.com/watch?v=\_Eeg1LxVWa8&t=365s. Acessado em: 22 de Abril de 2019