A história da criptografia começa há milhares de anos. Até décadas recentes, ela havia sido a história do que poderia ser chamado de criptografia clássica — isto é, de métodos de criptografia que usam caneta e papel, ou talvez auxílios mecânicos simples. No começo do século XX, a invenção de complexas máquinas mecânicas e electro-mecânicas, tais como a máquina com rotores Enigma, providenciou meios mais sofisticados e eficientes de encriptação; e a posterior introdução da eletrônica e computação permitiu elaborar esquemas de ainda maior complexidade, muitos completamente inadequáveis ao papel e caneta.

**O que é criptografia?**

Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

Na computação. A técnica usada são a de chaves as “chaves criptográficas”, trata-se de um conjunto de bit’s baseado em um algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave diferente e incompatível com a do emissor ela não conseguirá ter a informação.

A primeira técnica de criptografia usava apenas um algoritmo de decodificação, assim bastava o receptor de o algoritmo para decifrá-la, porém se um intruso conhecesse esse algoritmo poderia decifrar a informações caso capturasse os dados criptografados. Ainda existe outro problema imagine:

Se a pessoa “X” tivesse que enviar uma informação para a pessoa “Y”, e a pessoa “Z” tivesse que receber uma informação da pessoa “X”, mas a pessoa “Z” não pode saber a informação passada a pessoa “Y”, mas para a pessoa “Y” e a pessoa “Z” obterem a informação precisaria ter o algoritmo, assim teríamos que ter mais que um algoritmo.



**Qual seria a função da criptografia?**

Trata de um conjunto de regras que mostra codificar a informação de forma que só o emissor e o receptor consigam decifrá-la. Para isso são feitas várias técnicas são usadas, e ao passar do tempo modificada e o surgimento de novas outras de maneira que fiquem mais seguras.

**Como uma criptografia protege os usuários?**

Em geral, você geralmente tem contato com a criptografia de dados quando precisa inserir informações de identificação pessoal em um formulário da Web. Sites financeiros, do governo, de escolas e de compras costumam criptografar seus dados para ajudar na proteção contra roubo e fraude.

O princípio geral de funcionamento da criptografia é o embaralhamento do conteúdo de uma mensagem ou de um arquivo. Esse desarranjo oculta os dados por meio da reorganização de informações a partir de um código. Nesse processo, o emissor e o receptor da informação criptografada dispõem de uma determinada chave, ou seja, a linguagem correta para decifrar o código usado na ocultação do dado.

Assim, a criptografia protege os dados dos usuários tornando essas informações ilegíveis a aqueles que não possuem o código correto para lê-las, além de evitarem a exploração por malware, ações que impedem que aconteçam roubos de arquivos e fraudes.

**Cifra de César**

A Cifra de César é uma das mais fáceis e conhecidas técnicas de criptografia. Tratasse de um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto (26 Letras), porém transportada um certo número de posições à esquerda ou à direita.

O processo de criptografia de uma cifra de César é frequentemente incorporado como parte de esquemas mais complexos tendo aplicações modernas, como no sistema ROT13. Como todas as cifras de substituição monoalfabéticas, a cifra de César é facilmente decifrada e na prática não oferece essencialmente nenhuma segurança na comunicação.

**Benefícios em relação às técnicas anteriores**

As técnicas anteriores utilizavam o mesmo método substituição, que é o método usado pelos hebreus, mas substituíam a primeira letra do alfabeto pela última, a segunda pela penúltima e assim sucessivamente invertendo o alfabeto por completo. E que a técnica de César era razoavelmente segura e melhor.

Uma das técnicas anteriores seria a cifra de Vigenère que se trata de uma versão simplificada de uma mais geral cifra de substituição polialfabética. Para cifrar, é usada uma tabela de alfabetos que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição. As 26 linhas correspondem às 26 possíveis cifras de César. Uma palavra é escolhida como “palavra-chave”, e cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem.

**Vulnerabilidade e falhas**

A principal vulnerabilidade desse método de criptografia consiste na possibilidade de desincriptação ao se analisar o padrão de frequência dos símbolos. Essa questão já havia sido avaliada antes mesmo da existência do primeiro computador.

Fontes:<https://www.kaspersky.com.br/blog/vigenere-cipher-history/5688/> ,<https://www.passeidireto.com/arquivo/39716459/aps-2-semestre-ciencia-da-computacao-as-tecnicas-criptograficas-conceitos-usos-e> , <https://www.docusign.com.br/blog/criptografia-o-que-e-e-quando-ela-deve-ser-usada>,<https://www.passeidireto.com/arquivo/39716459/aps-2-semestre-ciencia-da-computacao-as-tecnicas-criptograficas-conceitos-usos-e>, <http://blog.mastermaq.com.br/criptografia-em-aplicativos/#:~:text=Como%20a%20criptografia%20protege%20os%20usu%C3%A1rios%3F,ser%20lidos%20por%20qualquer%20pessoa>. , <http://visonet.com.br/2019/03/29/criptografia-e-seguranca-de-dados-como-funciona/> ,