**História da Criptografia:**

A história da criptografia é uma narrativa que abrange milênios de anos e reflete a evolução da comunicação segura.

A história da criptografia é escrita desde o antigo Egito, onde hieróglifos eram usados ​​para ocultar mensagens e informações. Os gregos antigos também utilizavam cifras para comunicações secretas, sendo o "Disco de Esparta" um exemplo notável.

Falando de cifras clássicas a “Cipher of Cesar”, desenvolvida por Júlio César, era uma cifra de substituição onde cada letra era deslocada um número fixo de posições no alfabeto. No século XVI, o diplomata Blaise de Vigenère desenvolveu a cifra de Vigenère, que usava uma palavra-chave para variar a substituição de letras.

Durante a Segunda Guerra Mundial, a Alemanha usou a máquina de criptografia Enigma para codificar mensagens militares. O matemático e criptoanalista britânico Alan Turing desempenhou um papel fundamental em quebrar o código enigma.

A era digital viu o desenvolvimento da criptografia moderna, incluindo a cifra de chave simétrica, onde a mesma chave é usada para criptografar e descriptografar dados. E a cifra de chave assimétrica, que envolve um par de chaves (pública e privada), foi introduzida nos anos 1970 com a criação do algoritmo RSA. Em seguida com a internet e a segurança sendo mais desafiada foi criado o protocolo SSL/TLS desenvolvido para criptografar conexões na web, permitindo transações seguras e comunicações online.

Sendo assim a criptografia desempenha um papel crítico na proteção de informações sensíveis, desde transações financeiras online até a segurança de dispositivos IoT.

**FONTES:**

Singh, S. (1999). "**O Livro de Códigos: A Ciência do Sigilo do Antigo Egito à Criptografia Quântica**".

Bauer, F. L. (2000). "**Segredos descriptografados: métodos e máximas da criptologia**"

Kahn, D. (1996). "**Os decifradores: a história abrangente da comunicação secreta desde os tempos antigos até a Internet**".

Stallings, W. (2016). "**Criptografia e segurança de rede: princípios e práticas**".

Schneier, B. (2015). "**Dados e Golias: as batalhas ocultas para coletar seus dados e controlar seu mundo**".

Dierks, T. & Rescorla, E. (2008). "**O protocolo Transport Layer Security (TLS) versão 1.2**".

**Criptografia e Segurança Cibernética:**

A criptografia é um pilar essencial da segurança cibernética, uma vez que visa proteger dados em trânsito e em repouso, garantindo que somente destinatários autorizados possam acessá-los. Este campo interage com vários aspectos da segurança cibernética, incluindo:

1. **Confidencialidade:** A criptografia ajuda a garantir a confidencialidade dos dados, tornando-os ilegíveis para qualquer pessoa que não possua a chave de descriptografia apropriada. Isso é crucial para proteger informações sensíveis, como informações financeiras, médicas e pessoais.
2. **Integridade dos Dados:** Através de algoritmos de hash criptográficos, a criptografia também é usada para verificar a integridade dos dados. Qualquer modificação nos dados resultará em um valor de hash diferente, alertando sobre possíveis alterações não autorizadas.
3. **Autenticação:** A criptografia desempenha um papel fundamental na autenticação, garantindo que os usuários sejam quem dizem ser. Os certificados digitais e os sistemas de autenticação multifatorial frequentemente incorporam técnicas criptográficas para proteger a identidade do usuário.
4. **Proteção de Comunicações:** Na Internet, protocolos como SSL/TLS (criptografia de transporte) são usados para criptografar comunicações entre navegadores e servidores web, garantindo a privacidade das transações online.
5. **Proteção de Dados Armazenados:** A criptografia é usada para proteger dados armazenados em dispositivos, servidores e serviços em nuvem. Isso evita que terceiros acessem informações confidenciais, mesmo se conseguirem acessar fisicamente o hardware.
6. **Prevenção contra Ameaças Internas e Externas:** A criptografia protege contra ameaças internas e externas, incluindo ataques de hackers, acesso não autorizado e vazamentos de dados acidentais.

**"Cryptography and Network Security: Principles and Practice"** William Stallings (2014)

**"Applied Cryptography: Protocols, Algorithms, and Source Code in C"** Bruce Schneier (2017)

**"Security Engineering: A Guide to Building Dependable Distributed Systems"** Ross Anderson (2020)