CRIPTOGRAFIA

ALUNOS: EDUARDO L. / MATEUS F. / GUILHERME M./ VICENZO P.

ORIGEM

- A ideia de criptografar mensagens para tais propósitos é muito antiga e remonta à momentos anteriores ao surgimento dos primeiros computadores.
- Podemos citar três métodos antigos de criptografia: -**Tumba de Khnumhotep II** no Egito antigo;
- **-Cifra de César**, utilizado pelo imperador Júlio César;
- -e a máquina **Enigma** que foi utilizada na Segunda Guerra Mundial pelo exército alemão.

CRIPTOGRAFIA HOJE EM DIA

- A criptografia evoluiu e nos dias de hoje, principalmente na computação, se usa o sistema de chaves criptográficas, que consiste em **c**onjunto de bits baseado em determinado algoritmo capaz de decodificar a informação.

CHAVES

- Esta prática é dividida em dois tipos de chaves:
- **chave simétrica**: considerada como mais simples, na qual remetente e destinatário utilizam a mesma chave para codificar e decodificar a informação;
- **chave assimétrica**: é utilizado um par de chaves, a pública e a privada. Nesse sentido, o código público criptografa e o privado descriptografa.

CRIPTOMOEDAS

- Primeiramente, os algoritmos foram desenvolvidos por matemáticos, economistas e cientistas da computação.
- Podemos dizer que seu surgimento aconteceu em meados de 1980. Nesse sentido, o programador David Chaum desenvolveu a primeira espécie de dinheiro eletrônico.
- Mas a primeira moeda digital só surgiu anos mais tarde (2009) com o Bitcoin, criado por Satoshi Nakamoto. Que usou a SHA-256, que é uma função hash criptográfica como esquema de prova de trabalho.

CRIPTOGRAFIA MD5

- A criptografia Hash MD5 não é mais usada para a segurança de transferência de dados. Entretanto, ele conseguiu se manter no mercado de tecnologia para se tornar uma ferramenta de integridade de arquivos. Já que a mudança de apenas um byte de um arquivo já mudaria sua String MD5 por completo.