**Protocolo AES - Advanced Encryption Standard**

**O que é o AES:**

É baseado em uma rede que processo de encriptação de AES que realiza nas operações principais.

Utiliza a mesma chave para encriptar e decifrar os dados. Funciona em blocos de 128 bits para transformar o texto simples. Quanto maior o tamanho da chave, mais intensivo computacionalmente é quebrar a criptografia.

**Como funciona:**

O AES - Advanced Encryption Standard é um algoritmo de criptografia simétrica, o que significa que a mesma chave é utilizada tanto para encriptar como para desencriptar os dados. É usado em sistemas de segurança modernos devido à sua eficiência, rapidez e alto nível de proteção.

O AES é uma cifra de bloco, ou seja, ele divide os dados em blocos de 128 bits ou 16 bytes e processa cada bloco separadamente. Dependendo do tamanho da chave escolhida: 128, 192 ou 256 bits com um algoritmo realiza 10, 12 ou 14 etapas.

#### Como funciona a Expansão da chave :

A chave original não é usada diretamente em todas as etapas. A AES realiza a expansão de chave para gerar várias chaves para várias etapas. Ela usa operações matemáticas para gerar variação e segurança em com a etapa.

**Como funciona a Desencriptação**

A desencriptação da AES segue na mesma etapa, mas aplicá forma inversa utilizando as chaves de etapa na ordem contrária. Os dados são cifrados para transformar um texto original.