**CASO 1:**

O Quadrado de Polybius era uma técnica de criptografia utilizada na antiguidade. Consiste em associar de uma maneira fácil letras com números. Utilizando o formato de tabela de dimensão 5x5, as letras do alfabeto eram ali colocadas, sendo que o I e o J ocupam a mesma posição. O método de criptografar utilizando esse quadrado consiste em associar uma letra a dois números formados pelo número da linha e coluna de cada letra. Deste modo basta trocar a letra pelo respectivo número, para dificultar que a mensagem fosse decifrada, a numeração das linhas e colunas não era fixa.

**CASO 2**

No início do século 19, quando tudo se tornou elétrico, Hebern projetou uma engenhoca eletromecânica chamada de "máquina de rotores de Hebern". Ela usa um único rotor, no qual a chave secreta é incorporada a um disco rotativo. A chave codificava uma tabela de substituição, e cada tecla pressionada no teclado resultava em texto cifrado. Isso também fazia o disco girar em um entalhe e uma tabela diferente era usada para o próximo caractere de texto simples. Esse sistema deu origem à famosa máquina Enigma.

**CRIPTOGRAFIA COM CHAVES SIMETRICAS:**

**Advanced Encryption Standard – AES:** AES é uma variante da família Rijndael de algoritmos de criptografia de bloco simétrico, que é uma combinação dos nomes de dois criptógrafos belgas, Joan Daemen e Vincent Rijmen. O AES provou ser muito eficaz e eficiente e, dada a chave correta, adiciona pouca ou nenhuma diferença perceptível na sobrecarga de qualquer processo em que é utilizado. Essencialmente, o AES é uma forma de criptografia rápida e altamente segura, favorita de empresas e governos em todo o mundo.

As soluções Advanced Encryption Standard criptografam dados usando diferentes técnicas de criptografia. As seguintes técnicas são usadas:

SubBytes: usando uma tabela de substituição, também conhecida como caixa S, esse algoritmo substitui cada byte nos dados de entrada por um byte relacionado.

ShiftRows: nesta técnica, as linhas da matriz de dados são deslocadas um certo número de vezes, seguindo um padrão específico do AES.

MixColumns: trata-se uma técnica que usa uma matriz fixa para misturar as colunas da matriz de dados. Especificamente, manipulando cada byte de uma coluna usando uma função.

AddRoundKey: o método utiliza uma chave de rodada para fazer uma operação XOR com a saída dos três passos anteriores.

**IDEA (International Data Encryption Algorithm):** É uma chave simétrica desenvolvida em 1991. Caracterizado como um algoritmo com chave secreta de 128 bits. Foi projetado para ser eficiente em implementações de software. Possui um número fixo de iterações de uma mesma função que utiliza subchaves distintas. É conhecido publicamente desde 1991 e até agora não há notícia de ter sido revelado qualquer vulnerabilidade.

O algoritmo utilizado atua de forma diferente, pois usa a confusão e difusão para cifrar o texto. Na prática, ele utiliza três grupos algébricos com operações misturadas, e é dessa forma que o IDEA consegue proteger as informações.

**CRIPTOGRAFIA COM CHAVES ASSIMETRICAS:**

**RSA:** O algoritmo RSA é um dos mais seguros que existem na atualidade. Ele foi desenvolvido pelos fundadores da empresa RSA Data Security, Inc., o Ron Rivest, Adi Shamir e Leonard Adleman. Devido a isso, a sigla leva a inicial do sobrenome de cada um deles. A criptografia RSA é considerada uma das mais seguras e seu algoritmo foi o primeiro a possibilitar a assinatura digital. Por se tratar de uma criptografia muito eficiente, é possível utilizá-la hoje, diretamente na internet, como no caso de e-mail, e-commerce e outros recursos. A assinatura digital, por exemplo, garante que o documento é uma cópia verdadeira e legítima do original, além de assegurar sua autoria.

**Criptografia de curva elíptica (ECC):** Criptografia de curva elíptica (CEC) usa as propriedades matemáticas de curvas elípticas para produzir sistemas criptográficos de chave pública. Como toda criptografia de chave pública, a ECC é baseada em funções matemáticas que são simples de calcular em uma direção, mas muito difíceis de reverter. No caso de ECC, esta dificuldade reside na inviabilidade de calcular o logaritmo discreto de um elemento de curva elíptica aleatório em relação a um ponto de base conhecido publicamente, ou o "problema de logaritmo discreto de curva elíptica" (ECDLP). O Algoritmo de assinatura digital de curva elíptica (ECDSA) é um algoritmo de assinatura amplamente usado para criptografia de chave pública que usa ECC.