

Exemplos Históricos de Uso de Criptografia

1. **Cifras de Atbash:** Uma cifra de substituição simples que inverte o alfabeto. Por exemplo, 'A' se torna 'Z', 'B' se torna 'Y'. É uma das cifras mais antigas, usada na antiga Israel.
2. **Cifras do Imperador Augusto:** Similar ao Ciframento de César, mas com um deslocamento variável, permitindo uma comunicação mais complexa. Usada por líderes romanos para mensagens secretas.

Algoritmos de Criptografia com Chaves Simétricas

1. **RC4:** Um algoritmo de fluxo amplamente utilizado em protocolos como SSL/TLS e em softwares como o WEP (embora agora considerado inseguro).
2. **CAST-128:** Um algoritmo simétrico de bloco que oferece boa segurança e eficiência, utilizado em várias aplicações comerciais.

Algoritmos de Criptografia com Chaves Assimétricas

1. **PKCS #1:** Um padrão que define o uso do RSA para criptografia e assinaturas digitais, sendo amplamente adotado em sistemas de segurança.
2. **NTRU (N-th Degree Truncated Polynomial Ring):** Um algoritmo de criptografia baseado em polinômios que é resistente a ataques quânticos, tornando-o promissor para o futuro.