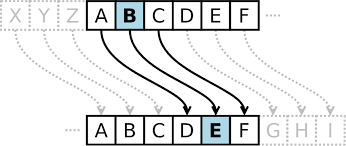
**UC – Sistemas Computacionais e Segurança – Atividade 04**

Exemplos históricos de criptografia:

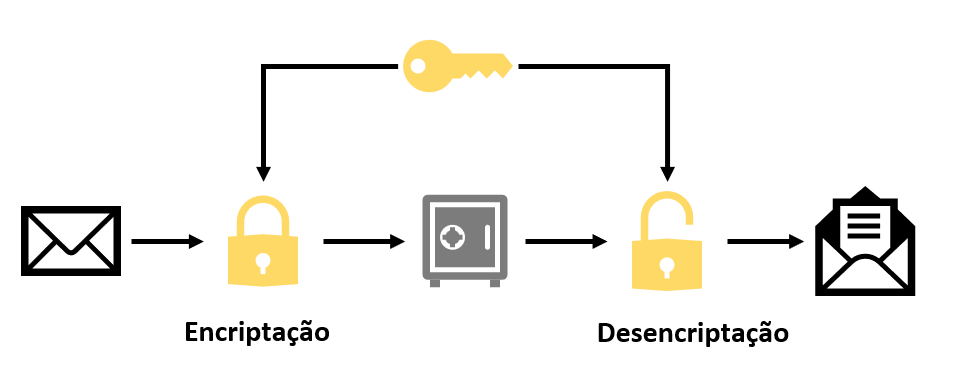
Códigos de substituição no Império Romano: os romanos empregavam não apenas o famoso Cifra de César, mas também códigos de substituição mais complexos. Eles substituíam letras por símbolos ou outros caracteres em arquivos secretos.



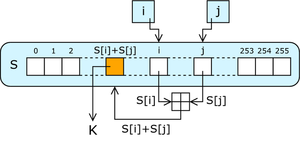
Cifra de Playfair : criada por Charles Wheatstone, mas promovida por Lord Playfair. Foi usada pelos militares britânicos durante a Guerra da Crimeia e a Primeira Guerra Mundial, os pares de letras eram cifrados em letras ao invés de letras individuais, tornando a quebra do código mais complexa.



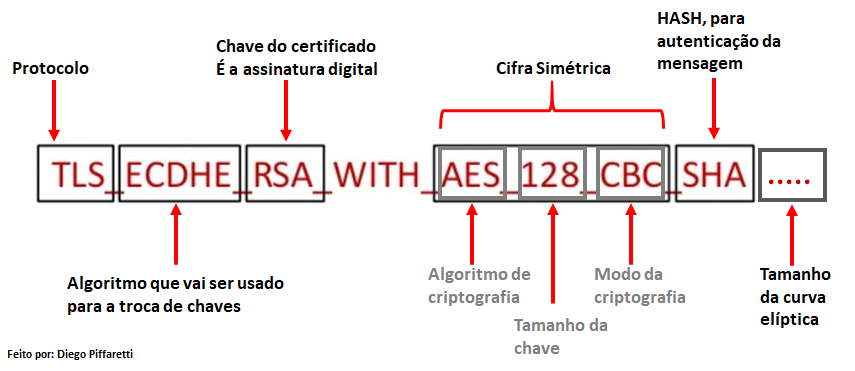
Algoritmos de Criptografia Chave Simétrica:



RC4 : Um algoritmo de criptografia de fluxo que era amplamente utilizado em protocolos como SSL, TLS, WEP e outros. Foi considerado inseguro para algumas aplicações em sistemas modernos, mas ainda é usado em sistemas legados:

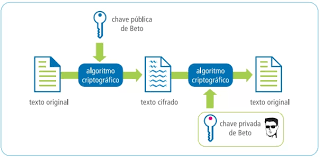


Camellia: Um algoritmo de criptografia de blocos simétrico de alta segurança, projetado para competir com o AES. É usado em redes de telecomunicações e em sistemas de segurança, especialmente na Ásia:

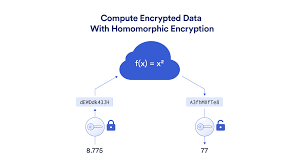


Algoritmos de Criptografia com Chaves Assimétricas:

existem duas chaves, uma pública onde qualquer individuo pode criptografar (chave pública), e outra chave apenas o receptor possui para decriptar a mensagem (chave privada). Percebe-se que esse processo se torna mais seguro e eficaz, resolvendo assim o problema de ter uma mesma chave para as duas pontas da comunicação criptografada.



Paillier: Um algoritmo de criptografia homomórfica que permite operações matemáticas sobre dados criptografados, amplamente utilizado em pesquisa sobre privacidade de dados e computação segura.



NTRU (N-th Degree Truncated Polynomial Ring): Um algoritmo assimétrico baseado em reticulados, usado principalmente em cenários que exigem resistência a ataques quânticos,

sendo uma alternativa promissora para a era da computação quântica.

