1 – Quadrado de Políbio

Políbio foi um geógrafo e historiador da Grécia antiga e atribui-se a ele, a invenção de um sistema criptográfico que permite com facilidade transformar letras em números e, através de uma chave numérica simples, recriar o texto inicial. Este sistema simples de criptografia foi usado até o século XIX. 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 descriptografada, a numeração das linhas e colunas não era fixa.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Usando o quadrado acima como exemplo, a mensagem “Bom Dia” seria B=12 O=34 M=32 D=41 I=42 A=11. Assim, a mensagem cifrada obtida é 123432414211.

2 – Cifra ADFGX

A invenção do telégrafo no século XIX possibilitou a comunicação entre grandes distâncias sem a necessidade de um mensageiro. Isto fez com que as trocas de mensagens entre remetente e destinatário se tornassem mais seguras. Entretanto, o uso desta tecnologia trouxe alguns inconvenientes, como o vazamento de informações pelos operadores dos telégrafos ou ainda a possibilidade da linha telegráfica ser “grampeada” por parte dos inimigos. Com o intuito de evitar os problemas obtidos com a invasão da comunicação à distância, os alemães desenvolveram uma cifra com base no Quadrado de Políbio, o qual substitui os números 12345 pelas letras ADFGX, como poder ser visto na figura abaixo.

	A	**D**	**F**	**G**	**X**
A	A	B	C	D	E
D	F	G	H	I/J	k
F	L	M	N	O	P
G	Q	R	S	T	U
X	V	W	X	Y	Z

Usando o quadrado acima como exemplo, neste caso, a mensagem “Boa Tarde” seria B=AD O=FG A=AA T=GG A=AA R=GD D=AG E=AX. Assim, a mensagem cifrada obtida é AD FG AA GG AA GD AG AX.

A mensagem cifrada é então organizada numa tabela baseada numa chave de tamanho variável de acordo com a dimensão da mensagem, podendo ser de qualquer tamanho, mas que não contenha letras repetidas. O passo seguinte é ordenar a chave por ordem alfabética e transpôr a mensagem cifrada.

Supondo que a chave criptográfica é a palavra "FRIO", obtém-se:

F	**R**	**I**	**O**	**-->**	**F**	**I**	**O**	**R**
A	D	F	G		A	F	G	D
A	A	G	G		A	G	G	A
A	A	G	D		A	G	D	A
A	G	A	X		A	A	X	G

A mensagem final, a ser transmitida via rádio será então lida por colunas:

AA AA FG GA GG DX DA AG

Para ler a mensagem, o destinatário terá somente que inverter o processo, sabendo a chave utilizada e a composição do diagrama de substituição em uso.

3 - Exemplos de algoritmos de criptografia com chaves simétricas utilizados atualmente:

3.1 - ChaCha20: É uma cifra de fluxo de 256 bits, leve e de alto desempenho, frequentemente usada para proteger dados transmitidos online, como e-mails, mensagens, tráfego da web e arquivos sendo carregados para a nuvem. Desenvolvido por Daniel J. Bernstein, um criptologista matemático, o ChaCha20 é projetado para corrigir os pontos fracos de seu antecessor, o Salsa20, oferecendo segurança aprimorada e, ao mesmo tempo, mantém o desempenho ideal. O ChaCha20 criptografa informações usando uma chave exclusiva e um nonce (um número usado apenas uma vez) para garantir que cada mensagem seja criptografada de forma diferente. Esse método torna extremamente difícil para os invasores descriptografar os dados sem a chave secreta.

3.1 - Blowfish: Um algoritmo de bloco que foi projetado para ser rápido e eficiente, especialmente em sistemas embarcados. Ele usa tamanhos de chave variáveis de até 448 bits e é popular em aplicações de criptografia de dados. ornando-o ideal para aplicações tanto domésticas, quanto comerciais. O Blowfish foi desenvolvido em 1993 por Bruce Schneier como uma alternativa grátis mais rápida para os algoritmos criptográficos existentes.

4 - Exemplos de algoritmos de criptografia com chaves assimétricas utilizados atualmente:

4.1 - Troca de chaves de Diffie–Hellman: É um método de criptografia que estabelece um compartilhamento de chaves secreto que pode ser usado para troca de mensagens secretas dentro de um canal de comunicação público. Desenvolvido por Whitfield Diffie e Martin Hellman, foi um dos primeiros exemplos práticos de métodos de troca de chaves implementado dentro do campo da criptografia, tendo sido publicado em 1976. O método permite que duas partes que não possuem conhecimento prévio uma da outra, compartilhem uma chave secreta sob um canal de comunicação inseguro.

4.2 - NTRU: NTRU é um sistema de criptografia de chave pública assimétrica pós-quântica que usa criptografia baseada em redes para encriptar e desencriptar dados. Foi desenvolvido em 1996 pelos matemáticos J. Hoffstein, J. Pipher e Silverman. O NTRU é composto por dois algoritmos: NTRUEncrypt, para encriptação, e NTRUSign, para assinaturas digitais. O NTRU é resistente a ataques e tem um design que facilita a segurança prática e é considerado um sistema probabilístico porque usa um elemento aleatório para encriptar uma mensagem.