

LUCAS BENITE DE ALCANTARA

RA: 824157974

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 descryptografada, 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.

PDF Converter

Only two pages were converted.

Please **Sign Up** to convert the full document.

www.freepdfconvert.com/membership