Fábrica de Noobs

Criptografia – Cifra de Bifid

A Cifra de Bifid foi criada pelo criptográfico francês Felix Delastelle em 1895,no French Revue du Génie civil. Entretanto, não há registros que ela já tenha sido utilizada para fins militares.

Trata-se de uma combinação entre as cifras de substituição e de fracionamento, o que a torna significativamente mais segura. Neste artigo, você aprenderá a codifica-la e decifra-la manualmente, podendo também utilizar a ferramenta automatizada em http://practicalcryptography.com/ciphers/bifid-cipher/.

O primeiro passo para criptografarmos utilizando a Cifra de Bifid é a criação de uma chave. Essa chave corresponde à uma tabela 5x5, sobre a qual o alfabeto deverá ser escrito.

Para construir sua tabela, primeiramente monte um modelo da seguinte forma, numerando as colunas e linhas de 1 até 5.

	1	2	3	4	5
1					
2					
3					
4					
5					

Em seguida, distribua, de forma aleatória, as letras do alfabeto pelas colunas, com exceção da letra J – já que esta não cabe no alfabeto 5x5. Por exemplo:

	1	2	3	4	5
1	d	b	e	w	k
2	c	z	i	a	h
3	p	y	m	g	f
4	x	v	o	u	s
5	t	n	r	l	q

Uma vez obtida a tabela, marque, em um local a parte, a sequência de letras presentes nela da esquerda para a direita, e de baixo para cima. Nessa situação, ela seria *dbewkcziahpymgfxvoustnrlq*. Essa será a chave de nosso código, e possibilitará sua posterior tradução.

Vamos agora trabalhar com a mensagem a ser codificada. Por exemplo, “defenda a parede leste do castelo”.

Escreva-a de forma a deixar um espaço razoável entre cada uma das letras. Na linha abaixo, escreva “linha” e, mais uma linha abaixo, escreva “coluna”. Ao final, seu espaço de codificação deverá ficar da seguinte forma:

	d	e	f	e	n	d	a		a		p	a	r	e	d	e		l	e	s	t	e		d	o		c	a	s	t	e	l	o
Linha																																			
Coluna																																			

Então, preencha cada espaço com as respectivas linhas e colunas que as letras da mensagem se encontram. Caso a letra J apareça, considere como a letra I em seu lugar.

Por exemplo, a letra E está na 1ª linha e na 3ª coluna. Logo, ela deverá aparecer da forma $\overset{E}{13}$. Faça isso com todas as letras da mensagem. Ao final do processo, você terá algo assim:

	d	e	f	e	n	d	a		a		p	a	r	e	d	e		l	e	s	t	e		d	o		c	a	s	t	e	l	o
Linha	1	1	3	1	5	1	2		2		3	2	5	1	1	1		5	1	4	5	1		1	4		2	2	4	5	1	5	4
Coluna	1	3	5	3	2	1	4		4		1	4	3	3	1	3		4	3	5	1	3		1	3		1	4	5	1	3	4	3

É então o momento de definirmos um período, que servirá como uma espécie de segunda chave e tem a função de melhorar a segurança da cifra. Para tanto, escolha um número, de preferência entre 2 e 6. No exemplo, vamos escolher 5.

Então, agrupe os blocos da mensagem pré-cifrada de 5 em 5, da seguinte forma:

d	e	f	e	n		d	a	a	p	a		r	e	d	e	l		e	s	t	e	d		o	c	a	s	t		e	l	o
1	1	3	1	5		1	2	2	3	2		5	1	1	1	5		1	4	5	1	1		4	2	2	4	5		1	5	4
1	3	5	3	2		1	4	4	1	4		3	3	1	3	4		3	5	1	3	1		3	1	4	5	1		3	4	3

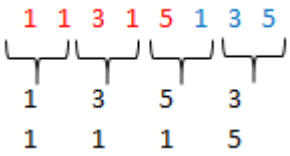
Caso sobrar um número de blocos menor que 5, coloque-os juntos em um bloco final.

Em seguida, você deverá escrever os números na sequência de baixo para cima e da esquerda para a direita. Observe no exemplo, com cores:

d	e	f	e	n		d	a	a	p	a		r	e	d	e	l		e	s	t	e	d		o	c	a	s	t		e	l	o
1	1	3	1	5		1	2	2	3	2		5	1	1	1	5		1	4	5	1	1		4	2	2	4	5		1	5	4
1	3	5	3	2		1	4	4	1	4		3	3	1	3	4		3	5	1	3	1		3	1	4	5	1		3	4	3

1 1 3 1 5 1 3 5 3 2 1 2 2 3 2 1 4 4 1 4 5 1 1 1 5 3 3 1 3 4 1 4 5 1 1 3 5 1 3 1 4 2 2 4 5 3 1 4 5 1 1 5 4 3 4 3

O próximo – e penúltimo – passo para a codificação é agrupar os números do novo código, dois a dois. Observe abaixo:



Ao final do processo, você terá uma sequência completa de números escritos na forma $\frac{x}{y}$. É então o momento de transformá-los em letras, conforme a tabela já criada. Por exemplo, um bloco de valor $\frac{5}{3}$ deverá corresponder a letra R, pois essa está na 5ª linha e na 3ª coluna.

Sendo assim, iremos obter o seguinte código após o final do processo. A mensagem codificada assume a forma *dptfybicuwtdrpgwtetpvarwtkoo*.

1	3	5	3	3	1	2	2	4	1	5	1	5	3	3	1	5	1	5	3	4	2	5	1	5	1	4	4
1	1	1	5	2	2	3	1	4	4	1	1	3	1	4	4	1	3	1	1	2	4	3	4	1	5	3	3
d	p	t	f	y	b	i	c	u	w	t	d	r	p	g	w	t	e	t	p	v	a	r	w	t	k	o	o

Sua tradução somente será possível por alguém que possua a tabela de transcrição (que também pode ser representada pelas letras em sequência) e o período.

Para realiza-la, deve-se transcrever, com base na tabela, o valor numérico do bloco de cada letra. Assim, a letra P corresponderia ao bloco $\frac{3}{1}$, por exemplo.

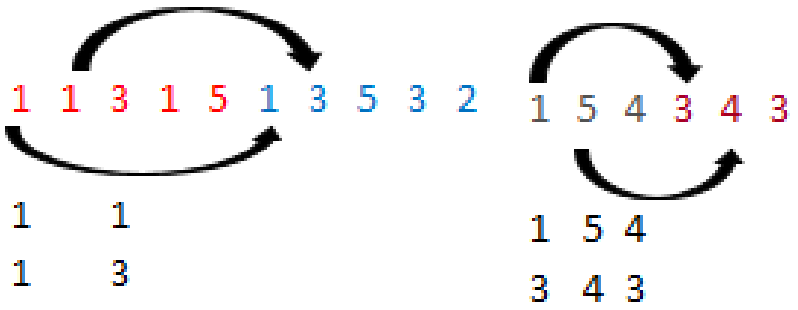
Em seguida, você deverá dividir a nova cadeia em blocos de 5, e marca-los de formas distintas. Por exemplo:

1 1 3 1 5 1 3 5 3 2

Lembre-se que, obrigatoriamente, cada bloco que você marcar deverá ter um correspondente, sempre aos pares. Quando você terminar de marcar um par e notar que restam menos que o dobro do período de números para serem marcados, interrompa o processo, divida o total de números restantes por 2 e crie blocos com essa extensão. Por exemplo:

4 2 2 4 5 3 1 4 5 1 1 5 4 3 4 3

Para compor os blocos correspondentes, você deverá unir o primeiro elemento do primeiro bloco com o primeiro elemento do segundo bloco, e assim por diante. No caso:



Finalmente, basta você utilizar a tabela para verificar as correspondências de letras e regressar à mensagem original. Por exemplo, um bloco de valores $\begin{matrix}5\\4\end{matrix}$ deverá corresponder a letra L, pois esta está na 5ª linha e na 4ª coluna.