Fundamentos de Criptografia

UFRPE

Cifras Clássicas

1ª. Bacon
2ª. Playfair

(1561-1626)

Francis Bacon

Um pouco de história

Francis Bacon foi um filósofo, escritor e político inglês. Estudou no Trinity College, em Cambridge, e mais tarde em Londres. Algumas de suas obras, especialmente os seus *Essays*, estão entre as maiores contribuições feitas ao pensamento humano desde os tempos dos filósofos gregos. Outros livros igualmente importantes são *New Atlantis, Life of Henry VII e The Advancement of Learning*. De especial interesse é o capítulo I do livro VI da obra ***The Advancement of Learning***, onde Bacon descreve minuciosamente a sua cifra, hoje conhecida como codificação binária de 5 bits.

A Cifra de Bacon

Francis Bacon detalha seu sistema de substituição que usa um alfabeto de 24 letras onde I=J e U=V. Para cada uma das letras do alfabeto é atribuído um grupo de 5 caracteres compostos pelas letras "a" e "b". Como são utilizadas apenas duas letras para a formação dos grupos, considera-se esta cifra como sendo de expressão binária. Como os grupos são formados por 5 letras, considera-se a cifra como sendo de 5bits.

O criptograma é preparado em duas etapas, começando pela substituição.

1ª. Etapa: A Substituição:

Vamos utilizar o sistema binário ao invés de "a" e "b" porque ele é menos confuso. Como exemplo, vamos cifrar a mensagem NUMABOA.

Texto claro	N	U	M	A	B	O	A
Binário	01100	10011	01011	00000	00001	01101	00000

2ª. Etapa: Escondendo a mensagem cifrada:

Pode-se usar qualquer texto para camuflar a mensagem cifrada. Tecnicamente esta camuflagem é chamada de cobertura. Como exemplo, uma frase de cobertura fazendo uma brincadeira: "Você sabia que SARS é o contrário de açúcars? "

Cobertura	V o c ê	s a b i a	q u e	S A R S	é	o	c o n t r á r i o	d e	a ç ú c a r s ?
Cobertura	0 1 1 0	0 1 0 0 1	1 0 1	0 1 1 0	0	0	0 0 0 0 0 0 1 0 1	1 0	1 0 0 0 0 0
Cobertura	V **o** **c** ê	s **a** b i **a**	**q** u **e**	S **A** **R** S	é	o	c o n t r á **r** i **o**	**d** e	**a** ç ú c a r s ?

(1802-1875)

Charles Wheatstone

Um pouco de história

Apesar do nome do Barão de Playfair estar associado a uma das cifra clássicas mais conhecidas, foi seu amigo, o cientista Charles Wheatstone, quem a concebeu. A Playfair é uma cifra de bloco primitiva, usando alguns princípios comuns às cifras de bloco atuais. O melhor meio de se proximar da criptologia moderna, sem ter que enfrentar a teoria dos números e a matemática, é entendendo a Playfair.

Basta formar grupos letras são tomadas duas a duas (bloco bigrâmico), Cada bloco recebera um tratamento de acordo com as regras. O texto claro que será cifrado com a playfari é: Criptografia.

CR IP TO GR AF IA

Palavra chave: SEGREDO

Agora Construímos uma grade 5x5 preenchida com alfabeto começando com a palavra chave.

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

Letras repetidas impedem que a cifra possa ser aplicada corretamente. Nestes casos, convenciona-se uma letra de separação. Geralmente são usados o X e/ou o Z. Caso falte uma letra no final, adiciona-se X ou Z.

Cada um dos conjuntos está numa de três categorias, a saber:

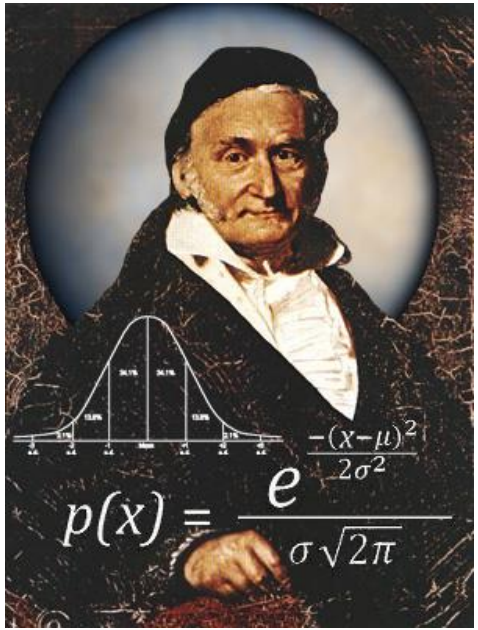
1. As letras estão na mesma linha;
2. As letras estão na mesma coluna;
3. As letras não estão na mesma linha nem na mesma coluna.

Se ocorrer 1), então cada letra é substituída pela letra imediatamente à direita; se uma das letras estiver no final da linha, então é substituída pela letra que está no início da linha. Se ocorrer 2), cada uma das letras é substituída pela letra que se encontra por baixo dela; se uma das letras estiver no final da coluna, será substituída pela primeira letra da coluna. No caso 3), para substituir a primeira letra, seguimos pela linha até encontrar a coluna onde se encontra a segunda letra; a segunda é trocada de forma análoga.

TEXTO EM CIFRA: KCJNM FRDBO NI

Ferramentas

1ª. Congruencia Linear
2ª. Fatoração Rho



Carl Friedrich Gauss

Um pouco de história

Carl Friedrich Gauss foi o grande introdutor da congruência, ele começou a mostrar ao mundo a congruência a partir de um trabalho realizado em 1801, Disquisitiones Arithmeticae, quando tinha apenas 24 anos de idade. Várias ideias usadas na teoria dos números foram introduzidas neste trabalho, até mesmo o símbolo usado na congruência atualmente foi o que Gauss usou naquela época.

Congruência linear

Chamemos de congruência linear em uma variável *x* uma congruência da forma:

a.x = b (mod m)

Propriedade da congruência linear

Tenhamos uma congruência a.x = b (mod m) e seja d o MDC de *a* e *m*, então se *d* não divide *b*, não possuímos nenhuma solução, mas, se *d* divide *b* então temos exatamente *d* soluções incongruentes modulo *m*.

John Pollard

Um pouco de história

O Algoritmo rho de Pollard é um algoritmo de fatoração desenvolvido por Pollard em 1975. O algoritmo rho Pollard é baseado em dois aspectos importantes..

Algoritmo Pollard's rho

1) O algoritmo utiliza uma função módulo n como um gerador de sequência pseudo-aleatória.

2) A detecção do ciclo na sequência é baseada na idéia atribuída a Floyd conhecida como algoritmo da tartaruga e do coelho comparando a sequência $x_{i} com x_{2i}paratodoi. Asequênciax_{i}$ representa a tartaruga e a sequência x2ix2i representa o coelho que move duas vezes mais rápido.

No caso do algoritmo não encontrar um fator, nós vamos utilizar um f(x) diferente. O algoritmo não funciona quando n é primo, uma vez que, d sempre será 1.

Referencia : Criptografia e matemática https://www.facebook.com/Criptografia-e-matem%C3%A1tica-164684333635007/,**Le chiffre Playfair** ttp://www.apprendre-en-ligne.net/crypto/subst/playfair.html, https://comeoncodeon.wordpress.com/2010/09/18/pollard-rho-brent-integer-factorization/