

Universidade Federal de Campina Grande
Unidade Acadêmica de Matemática e Estatística
Programa de Educação Tutorial
Tutor: Daniel Cordeiro de Morais Filho
Atividade de Iniciação Científica
Orientador Científico: Diogo Diniz Pereira da Silva
Aluno: Alan de Araújo Guimarães

CRIPTOGRAFIA E MATEMÁTICA



Criptografia:

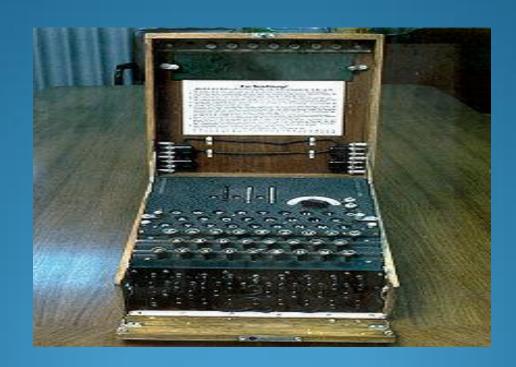
Estuda os métodos de codificação de mensagens.

Exemplos de códigos criptográficos:

- Código de César
- 2. Anagrama
- 3. Máquina ENIGMA



Foto da máquina ENIGMA





Tipos de criptografia

- Criptografia simétrica: Nela, conhecer o procedimento de codificação implica conhecer o procedimento de decodificação.
- Criptografia assimétrica: Nela, conhecer o procedimento de codificação não implica conhecer o procedimento de decodificação.



• Quem é capaz de decifrar o nome de um grupo de matemáticos que tem trabalhado muito nesses últimos tempos?

• O nome do grupo criptografado pelo RSA é:

Algoritmo RSA de criptografia

Inventado em 1977 pelos norte-americanos R. L.
 Rivest, A .Shamir e L. Adleman.



- Código assimétrico
- Forte uso da matemática



Descrição sucinta do RSA

- Para implementar o RSA escolhemos dois primos p e q e calculamos n=p.q
- Para codificar uma mensagem usamos n
- Para decodificar uma mensagem usamos p e q
- n pode ser tornado público
- *p* e *q* precisam ser mantidos em segredo
- Quebrar o RSA consiste em fatorar n, o que leve muito tempo.



Procedimento de codificação

- Transforma-se a mensagem num número por substituição.
- Escolhe-se dois primos p e q tais que:

 $p\Xi_5 \pmod{6}$ e $q\Xi_5 \pmod{6}$



• Seja $a < n = p \ q$ um bloco numérico. Para codificar o bloco a calculamos o número C(a), $o \le C(a) < n$ tal que:

$$a^3 \equiv C(a) \pmod{n}$$

Procedimento de decodificação

Sejam b um bloco codificado e d tal que:

$$d = 4 \left[\frac{(p-1)(q-1) + 2}{6} \right] - 1$$

Para decodificar o bloco b calculamos o número D(b), o $\leq D(b) < n$ tal que:

$$b^d \equiv D(b) (\bmod n)$$



Demonstra-se que :

$$D(C(b))=b$$
Matemática usada:
Pequeno Teorema de Fermat
e
Teorema chinês do resto



 Vamos decodificar os blocos numéricos 5-49-24 e ver qual é o nome do grupo de matemáticos que eles representam!



• Usamos *n*=55 e a correspondência

A	В	C	D	E	F	G	Н	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	О	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35



Bibliografia:

- COUTINHO, S.C. Números inteiros e criptografia RSA. Série de Computação e Matemática n. 2, IMPA e SBM, segunda edição, 2000.
- COUTINHO, S.C. Criptografia (Programa de Iniciação Científica OBMEP);OBMEP. Rio de Janeiro, 2008.