[illegible] Murao - 186837

Lista 01

01) Playfair → chave = naocompartilhe → resultado = COMOBERNTIBFMEBWDA

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

↳ ODCAEMPARTEDAFEXEC

↳ O DCA é parte da FEEC

02) N = 4 rotores com K = 10 letras

a) fixos → $K^N = 10^4$

b) móveis → $N! \cdot K^N = 4! \cdot 10^4 = 2{,}4 \cdot 10^5$

c) todas combinações possíveis → $\frac{K!}{(K!-N)!} \cdot K^N = 10!9!8!7! \cdot 10^4 \cong 2 \cdot 10^{24}$

03) O efeito Avalanche é quando uma pequena mudança na entrada muda muito o resultado da criptografia. Ele sendo bom para aumentar a imprevisibilidade do algoritmo, para ser mais difícil de ser descoberto a entrada a partir somente da saída.

04) Supondo a frase "só sei que nada sei" = SOSEIQUENADASEI

↳ com a chave → ABCDEABCDEABCDE

↳ temos o resultado → TQVINRWHRFECVIN

- Pode-se notar 2 vezes a sequência VIN, logo, supondo que são 2 palavras iguais podemos concluir que a chave se repete a cada
  - 10 letras → TQVINRWHRF , ECVIN
  - 5 letras → TQVIN , RWHRF , ECVIN
  - 1 letra → seria um algoritmo monoalfabético

- Conhecido o tamanho da chave é possível fazer uma análise estatística com caracteres em colunas correspondentes com a mesma letra da chave.

05) O one-time pad é uma variação do código de Vigenère que usa uma chave aleatória de mesmo tamanho da palavra de entrada, assim criando uma saída com distribuição uniforme impossibilitando uma análize estatística.

06) Uma máquina de rotores possui:

- N rotores
- Cada rotor direciona K letras para outras K letras, tendo K! combinações possíveis
- O rotor N só anda 1 letra quando o rotor N-1 anda K letras
- Os rotores podem ser reposicionados de $\frac{M!}{(M-N)!}$ formas, sendo M o número de rotores disponíveis, no pior caso $M = NK!$
- A entrada vai no primeiro rotor, que por sua vez tem sua saída na entrada do próximo, assim fazendo a quantidade de possíveis alfabetos $\frac{M!}{(M-N)!} K^N$

07) Confusão é usado para obscurecer a relação entre a cifra e a chave, usando métodos de substituição para fazer com que cada bit da cifra dependa de vários bits da chave, aumentando a ambiguidade da cifra. Enquanto difusão é a relação de cada bit da cifra com vários do texto da entrada, usando transposição para aumentar a redundância da cifra.

08) É visto a maior ocorrência de letras, ou caracteres que acredita que vêm da mesma letra, e contado suas frequências para ser comparado com as letras mais ocórrentes nessa língua, assim mapeando a cifra para o texto inicial.

Para impedir análizes estatísticas é preciso fazer com que a distribuição de caracteres seja uniforme, assim como no one-time pad

09) P = RODRIGOSEIJIPIUBELIHIRAO

$k_1 = 1$, $k_2 = 3\ 1\ 2\ 4$

Matrix =

R	O	D	R
I	G	O	S
E	I	J	I
P	I	U	B
E	L	I	H
I	R	A	O
X	X	X	X

2 3 1 4

OGIILRX|DOJUIAX|RIEPEIX|RSIBHOX

R	O	D	R
I	G	O	S
E	I	J	I
P	I	U	B
E	L	I	H
I	R	A	O
X	X	X	X

↓

RODRIGOSEIJIPIUBELIHIRAO

(01) Caso ele tenha conhecimento do algoritmo usado, a cifra é:

- a chave → ele pode simplesmente executar o algoritmo ao contrário
- o texto de entrada → ver como foi mapeado a substituição ou transposição seguindo o algoritmo para descobrir a chave

Caso não seja conhecido o algoritmo, deverá ser feito uma análize estatistica