



### Sessão nº3

# Informação Mútua e Equívocos



## Definição de entropia relativa



- Entropia relativa ou **Distância de Kullback** é uma medida de distância (semelhança) entre duas funções de distribuição  $p(X)$  e  $q(X)$ . Define-se como

$$D(p||q) = \sum_{x_i \in X} p(x_i) \log_2 p(x_i) / q(x_i)$$

- se  $p(X) = q(X)$  (são idênticas) então

$$D(p||q) = 0$$

- por convenção  $0 \log_2 0/q = 0$  e  $p \log_2 p/0 = \infty$



## Definição de informação mútua



- Define-se **informação mútua** das v.a.  $X$  e  $Y$  como

$$I(X;Y) = \sum_{x_i \in X} \sum_{y_j \in Y} p(x_i, y_j) \log_2 p(x_i, y_j) / p(x_i) p(y_j)$$

- Informação mútua é a medida da quantidade de informação que a v.a.  $X$  contém acerca da v.a.  $Y$ ; redução da incerteza de  $X$  por conhecimento de  $Y$

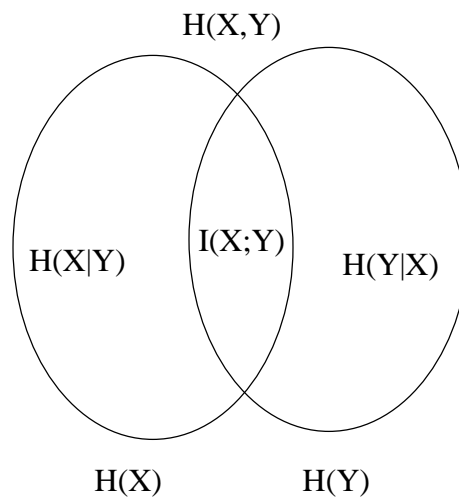
–  $I(X;Y) = H(X) - H(X|Y)$

- se  $X$  e  $Y$  são independentes então

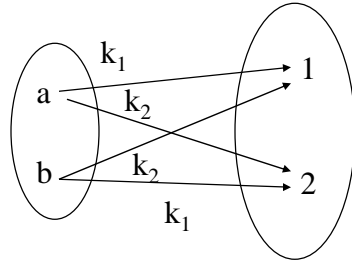
$$I(X;Y) = 0$$



## Relação entre a entropia e a informação mútua



## Análise do sistema *One Time Pad* de Vernam



### Dados:

$$p(a) = 1/4, \quad p(b) = 3/4$$

$$P(k_1) = 1/2, \quad P(k_2) = 1/2$$

### Verifica-se que

$$H(X) \approx 0,81 \text{ [bit/texto]}$$

$$H(K) = 1 \text{ [bit/chave]}$$

$$H(Y) = 1 \text{ [bit/cripto]}$$

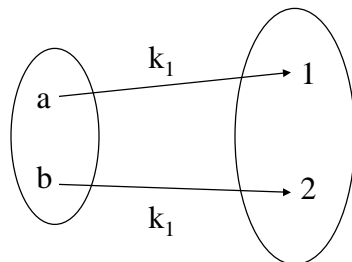
$$I(X;Y) = ?$$

$$I(X;Y) = 0$$

**não se “ganha” informação acerca do texto em claro por observação do criptograma** pois  $X$  e  $Y$  são independentes, uma vez que  $p(x|y) = p(x)$  para todo o  $x$  e para todo o  $y$



## Análise do sistema identidade (chave única $k_1$ )



### Dados:

$$p(a) = 1/4, \quad p(b) = 3/4$$

$$P(k_1) = 1$$

### Verifica-se que

$$H(X) \approx 0,81 \text{ [bit/texto]}$$

$$H(K) = 0 \text{ [bit/chave]}$$

$$H(Y) \approx 0,81 \text{ [bit/cripto]}$$

$$I(X;Y) = ?$$

$$I(X;Y) = H(X) = H(Y)$$

**“ganha-se toda” a informação acerca do texto em claro por observação do criptograma** pois  $X$  e  $Y$  são completamente dependentes;  $Y$  é função de  $X$



## Limites da informação mútua



$$\rightarrow 0 \leq I(X;Y) \leq H(X)$$

- Se X e Y são independentes então

$$H(X|Y) = H(X) \Leftrightarrow I(X;Y) = 0$$

- Se Y é função de X então

$$I(X;Y) = H(X) = H(Y)$$

- Note-se que no sistema de Vernam sempre que  $p(k_1) \neq p(k_2)$  temos  $0 < I(X;Y) \leq H(X)$



## Condição de Segurança Perfeita



$$I(X;Y) = 0 \iff H(X) \leq H(K)$$

- premissas

- $H(X|K.Y) = H(X.K.Y) - H(K.Y) = 0$  ;

- logo  $H(X.K.Y) = H(K.Y)$

- $H(X.K|Y) \stackrel{3}{=} H(X|Y)$

- $H(K|Y) \leq H(K)$



## Equívocos na criptografia



- **Equívoco da mensagem**  $H(X|Y)$  mede a incerteza relativamente ao texto em claro quando se conhece o criptograma.

$$I(X;Y) = H(X) - H(X|Y) \leftarrow$$

- **Equívoco da chave**  $H(K|Y)$  mede a incerteza relativamente à chave quando se conhece o criptograma. É uma medida de quanta informação acerca da chave é revelada pelo criptograma.



## Equívoco da chave



- Seja um sistema criptográfico  $(P,C,K,E,D)$ , então

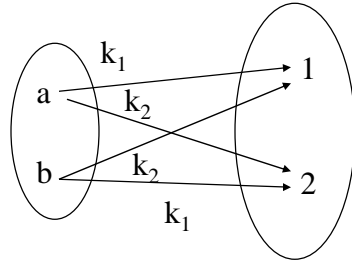
$$H(K|Y) = H(K) + H(X) - H(Y)$$

– **assume-se que:**

- $K$  e  $X$  determinam um único  $Y$ , i.e.  $H(Y|K,X) = 0$ , e
- $K$  e  $Y$  determinam um único  $X$ , i.e.  $H(X|K,Y) = 0$



## Análise do sistema *One Time Pad* de Vernam



### Dados:

$$p(a) = 1/4, \quad p(b) = 3/4$$

$$P(k_1) = 1/2, \quad p(k_2) = 1/2$$

### Verifica-se que

$$H(X) \approx 0,81 \text{ [bit/texto]}$$

$$H(K) = 1 \text{ [bit/chave]}$$

$$H(Y) = 1 \text{ [bit/cripto]}$$

$$H(K|Y) = ?$$

$$H(K|Y) = 1 + 0,81 - 1 = 0,81 \text{ é menor !!!}$$

(Mas se maximizarmos  $H(X)$  temos que  $H(K|Y)=H(K)$ )



## Exemplo: cifra de substituição

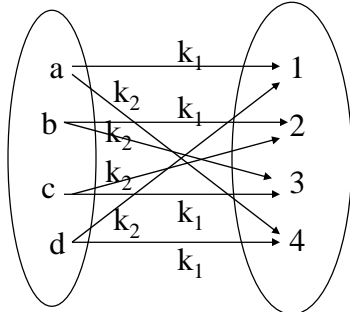


- Considere o sistema criptográfico  $(P, C, K, E, D)$  onde  $P=C=K=\mathbf{Z}_2=\{0,1\}$ , as regras  $E$  e  $D$  correspondem à **cifra de substituição** e a mesma chave é usada na cifra de vários textos.

– Como varia o equívoco da chave  $H(K|Y)$  com o número de criptogramas observados?



Análise do sistema Vernam usando a mesma chave para dois textos



Seja  $a \circ 00$   $b \circ 01$   $c \circ 10$   $d \circ 11$

$1 \circ 00$   $2 \circ 01$   $3 \circ 10$   $4 \circ 11$

Sabendo que

$$p(0) = 1/4, \quad p(1) = 3/4$$

$$P(k_1) = 1/2, \quad p(k_2) = 1/2$$

Verifica-se que

$$H(K) = 1 \text{ [bit/chave]}$$

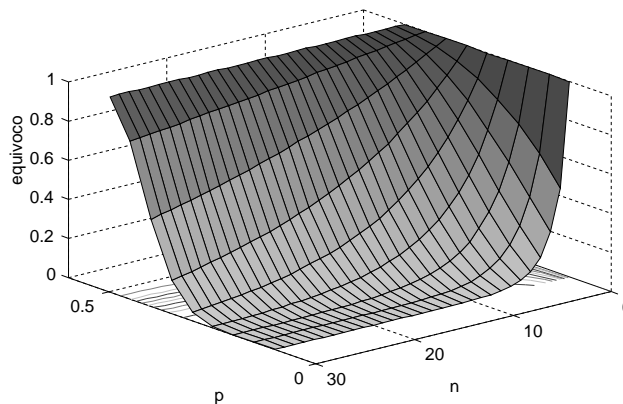
Depois de observarmos dois criptogramas,  $H(K|Y) = ?$

$$H(K|Y) \approx 0,67$$

**é ainda menor do que  $H(K|Y)$  observando um só criptograma!**



Equívoco da chave na criptoanálise



- Equívoco na criptoanálise de uma **cifra de substituição** aplicada a um conjunto de 2 textos em claro (**p** é probabilidade dum dos textos e **n** é o número de criptogramas observados).

