



## Sessão nº2

# Introdução à Teoria da Informação e Entropias



## Definição de segurança perfeita

- Um sistema tem **segurança perfeita** se, para todo o  $x \in P$  e para todo o  $y \in C$

$$p(x|y) = p(x)$$

– ou seja, não se “ganha” informação acerca do texto em claro por observação do criptograma

- **Como medir o “ganho” de informação?**





- Conceitos básicos

- **Medida de quantidade de informação (entropia).**

- Capacidade de informação dum canal.
- Codificação:
  - codificação de fonte
  - [cifra]
  - codificação de canal



Medida de quantidade de informação (entropia).



### Incerteza = Informação

(antes do acontecimento) (depois da ocorrência)

- Seja  $X$  uma v.a. que toma um conjunto de valores finitos de acordo com uma distribuição de probabilidades  $p(X)$ .
- **Qual é o “ganho” de informação por um acontecimento que pode ocorrer de acordo  $p(X)$ ?**
- **Se o acontecimento não tivesse ocorrido, qual seria a incerteza acerca da sua ocorrência?**

Esta quantidade designa-se por **entropia de  $X$**  e representa-se  **$H(X)$**



## Definição de quantidade de informação



- Seja  $X$  uma v.a. que toma um conjunto de valores finitos de acordo com uma distribuição de probabilidades  $p(X)$ .
- Define-se **quantidade de informação** associada a uma ocorrência (símbolo)  $x_i$  como

$$I(x_i) = \log_2 1/p(x_i)$$

- propriedades:
  - $I(x_i) = 0$  se  $p(x_i) = 1$
  - $I(x_i) \geq 0$  se  $0 \leq p(x_i) \leq 1$
  - $I(x_i) > I(x_k)$  se  $p(x_i) < p(x_k)$
  - $I(x_i, x_k) = I(x_i) + I(x_k)$  se  $x_i$  e  $x_k$  são **independentes**



## Definição de entropia



- Define-se **entropia** da v.a.  $X$  como

$$H(X) = \sum p(x_i) \log_2 1/p(x_i)$$

- no limite quando  $p(x_i) \rightarrow 0$

$$p(x_i) \log_2 1/p(x_i) = 0$$

- Entropia é a medida da quantidade de informação necessária, em média, para descrever a v.a.  $X$ 
  - $0 \leq H(X) \leq \log_2 n$  sendo  $n$  o nº de acontecimentos
  - 1 bit é a quantidade de informação que “ganhamos” quando ocorre 1 de 2 acontecimentos possíveis e equiprováveis.



## Definição de entropia conjunta



- Define-se **entropia conjunta** das v.a.  $X$  e  $Y$  como

$$H(X, Y) = \sum_{x_i \in X} \sum_{y_j \in Y} p(x_i, y_j) \log_2 1/p(x_i, y_j)$$

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

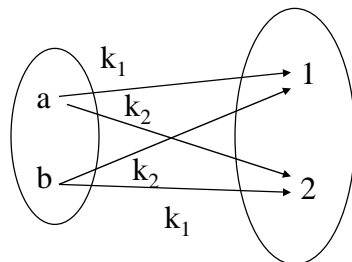
$$H(X, Y) = H(X) + H(Y)$$

- Entropia conjunta é a medida da quantidade de informação necessária, em média, para descrever o par de v.a.  $(X, Y)$

- $H(X, Y) \leq H(X) + H(Y)$  ←



## 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

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

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

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

### Verifica-se ainda que:

$$H(X, Y) = H(X) + H(Y) \approx 1,81$$

pois  $X$  e  $Y$  são independentes, uma vez que  $p(x|y) = p(x)$  para todo o  $x$  e para todo o  $y$



## Entropia condicionada



- Sejam as v.a.  $X$  e  $Y$ ;  
para qualquer valor fixo  $y$  de  $Y$ , dada a distribuição  
(**condicional**) de probabilidade  $p(X|y)$ , define-se

$$H(X|y) = \sum_{x_i \in X} p(x_i|y) \log_2 1/p(x_i|y)$$



## Definição de entropia condicionada (média)



- Define-se **entropia condicionada** (média) da v.a.  $X$  dado  $Y$  como

$$H(X|Y) = \sum_{x_i \in X} \sum_{y_j \in Y} p(x_i, y_j) \log_2 1/p(x_i|y_j)$$

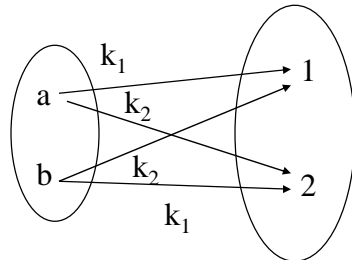
- se  $X$  e  $Y$  são independentes então

$$H(X|Y) = H(X)$$

- Entropia condicionada é a medida da quantidade de informação necessária, em média, para descrever a v.a.  $X$  dado que se conhece  $Y$ 
  - $H(X|Y) = H(X, Y) - H(Y)$
  - $H(X|Y) \leq H(X)$  ←



## 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

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

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

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

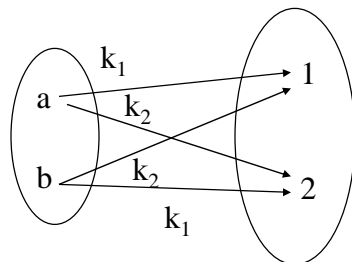
$$H(X|Y) = ?$$

$$H(X|Y) = H(X) \approx 0,81$$

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 *One Time Pad* de Vernam



### Dados (outro exemplo):

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

$$P(k_1) = 1/4, \quad p(k_2) = 3/4$$

### Verifica-se que

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

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

$$H(Y) \approx 0,95 \text{ [bit/cripto]}$$

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

$$H(X|Y) \approx 0,66 < H(X)$$

**dados o criptograma, a incerteza do texto é menor**

pois  $X$  e  $Y$  não são independentes, uma vez que  $p(x|y) \neq p(x)$  para todo o  $x$  e para todo o  $y$  (não existe segurança perfeita)

