



Teoria Matemática da Comunicação



Tópicos



- 1) Conceitos básicos Teoria das Probabilidades
- 2) Conceitos básicos Teoria da Informação
 - a) Quantidade de informação
 - b) Capacidade de informação
 - c) Codificação
 - i) Codificação de fonte
 - ii) Codificação de canal
- 3) Papel da Teoria da Informação na Criptografia



Bibliografia



- Douglas **Stinson**, *Cryptography - Theory and Practice*, CRC Press, 1995.
- T. **Cover** and J. Thomas, *Elements of Information Theory*, John Wiley & Sons, 1991.
- A. **Papoulis**, *Probability & Statistics*, Prentice-Hall, 1990.
- M. **Nelson**, *The Data Compression Book*, M&T Publishing Inc., 1991.
- Stephen B. **Wicker**, *Error Control Systems for Digital Communications and Storage*, Prentice-Hall, 1995
- Robert **Lucky**, *Silicon Dreams - Information, Man and Machine*, St. Martin's Press 1991.



Teoria da Informação: o início



- Trabalhos de C. E. Shannon com grande influência no estudo da Criptografia
 - 1948, *A mathematical theory of communication*
 - 1949, *Communication theory of secrecy systems**
- objectivo: estudar a estrutura matemática e propriedades dos sistemas criptográficos

* trabalho realizado em 1945



Tipos de sistemas criptográficos



- Existem 3 tipos de sistemas criptográficos, segundo Shannon :
 - *Concealment systems*
 - Ex.: tinta invisível
 - *Privacy systems*
 - Ex.: equipamentos que implementam a inversão espectral dum sinal de fala
 - “*True*” *secrecy systems*
 - o significado da mensagem é escondido por via da cifra



Sistemas criptográficos discretos



- Shannon no seu estudo considerou apenas os sistemas criptográficos **discretos**, onde as mensagens são, por exemplo:
 - letras/palavras duma linguagem
 - níveis de amplitude quantizados dum sinal de fala ou de vídeo





quintupletto (P, C, K, E, D)

- P - Conjunto finito de possíveis de textos em claro
- C - Conjunto finito de possíveis textos cifrados
- K - Espaço de chaves; Conjunto finito de chaves possíveis
- E - Conjunto de regras de cifra
- D - Conjunto de regras de decifra



- Existem 2 abordagens para discutir a segurança dum sistema criptográfico:
 - **Segurança computacional:** define-se
 - em termos do nº de operações ou do tempo
 - relativamente a um problema conhecido como difícil
 - Ex.: factorização de números inteiros muito grandes
 - **Segurança incondicional**
 - o sistema não pode ser “quebrado”, mesmo com recursos infinitos





- Como desenvolver a teoria dos sistemas criptográficos que são incondicionalmente seguros ?

Usando a **Teoria das Probabilidades** como ferramenta formula-se então o conceito de **Segurança Perfeita**.



- **Probabilidade**
 - conjuntos
 - probabilidade e frequência de ocorrência
 - probabilidade conjunta e probabilidade condicional
 - independência
- **Variáveis aleatórias**
 - função de frequência de ocorrência de X
 - valor médio de X
 - probabilidade conjunta de X e Y
 - probabilidade condicional de X dado Y
 - independência de variáveis aleatórias
 - sequência de variáveis aleatórias



Conjuntos



- Conceitos básicos
 - objectos
 - conjuntos
 - elementos
 - diagramas de Venn
- Operações sobre conjuntos
 - subconjuntos
 - igualdade
 - união e intersecção
 - complementar



Probabilidade e Frequência de Ocorrência



- Experiências, resultados (*outcomes*) e acontecimentos (*events*)

Probabilidade de acontecer A ——— $P(A) = \frac{N_A}{N}$ com $N \rightarrow \infty$

Freq. Ocorrência de A

$$0 \leq P(A) \leq 1$$

$$P(S) = 1$$

↑
Espaço de acontecimentos possíveis



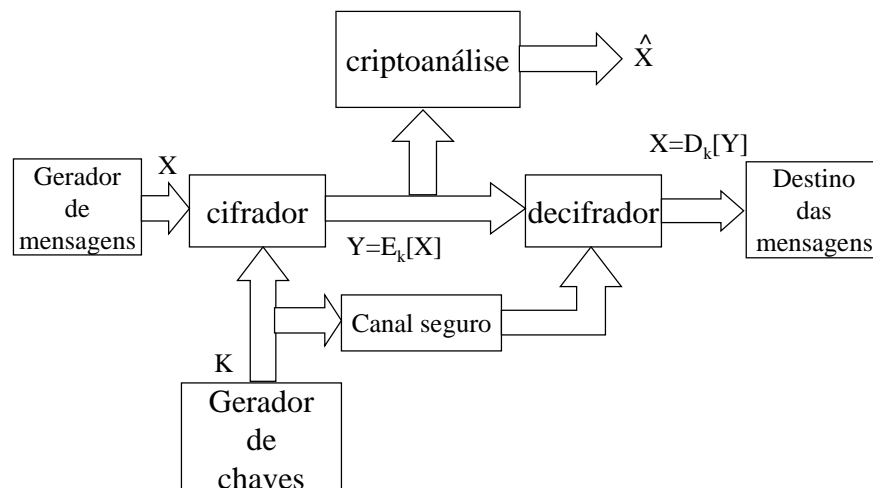
Teorema de Bayes



- A probabilidade conjunta relaciona-se com a probabilidade condicionada da seguinte forma:
 - $P(A,B) = P(A|B) \cdot P(B)$
 - $P(A,B) = P(B|A) \cdot P(A)$
- **Teorema de Bayes**
 - $P(A|B) = P(B|A) \cdot P(A) / P(B)$ se $P(B) > 0$
- **Corolário**
 - A e B **são independentes** sse $P(A|B) = P(A)$



Modelo de sistema criptográfico





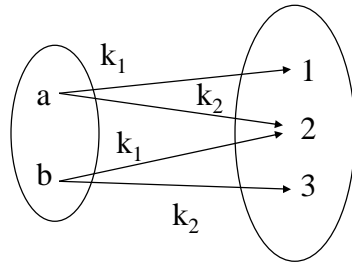
- v.a. X : conjunto de textos em claro $\in P$
- v.a. K : conjunto de chaves $\in K$
- v.a. Y : conjunto de criptogramas $\in C$
- Assume-se que:
 - a chave k é escolhida antes dos textos de acordo com $P(K=k) \equiv p(k)$, logo X e K são independentes.
 - 1 chave é usada apenas para 1 texto



- Probabilidades **a priori**:
 - $p(x) \equiv P(X=x)$: Probabilidade de X tomar o valor x
 - $p(k) \equiv P(K=k)$: Probabilidade de K tomar o valor k
- $p(x)$ e $p(k)$ induzem a distribuição de probabilidades de y
 - $p(y)$: probabilidade do criptograma y ter sido transmitido
- Probabilidades **a posteriori**:
 - $p(x|y) \equiv P(X=x|Y=y)$: Prob. condicionada de X tomar o valor x dado que Y toma o valor y



Análise do sistema A



Dados:

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

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

Pretende-se determinar:

$$p(y), p(k|y), p(y|x), p(x|y).$$



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





- **Sequência de variáveis aleatórias i.i.d.**

- $\mathbf{X} = [X_1 \ X_2 \ X_3 \ \dots \ X_n]$

- $\mathbf{x} = [x_1 \ x_2 \ x_3 \ \dots \ x_n]$
 - Concretização de X_1
 - Concretização de \mathbf{X}

- $p(\mathbf{x})$: Probabilidade da sequência \mathbf{x}

- $p(\mathbf{x}) = p(x_1) \times p(x_2) \times p(x_3) \times \dots \times p(x_n)$ Indep.

