UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança da Informação I
Segunda Aula

Prof. Frederico Sauer, D.Sc.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptologia e Criptografia

- Criptologia
  - Estudo das técnicas : criptografia e criptoanálise
- Elemento fundamental para os atributos
  - Confidencialidade
  - Integridade
  - Autenticidade

Taxonomia dos Algoritmos

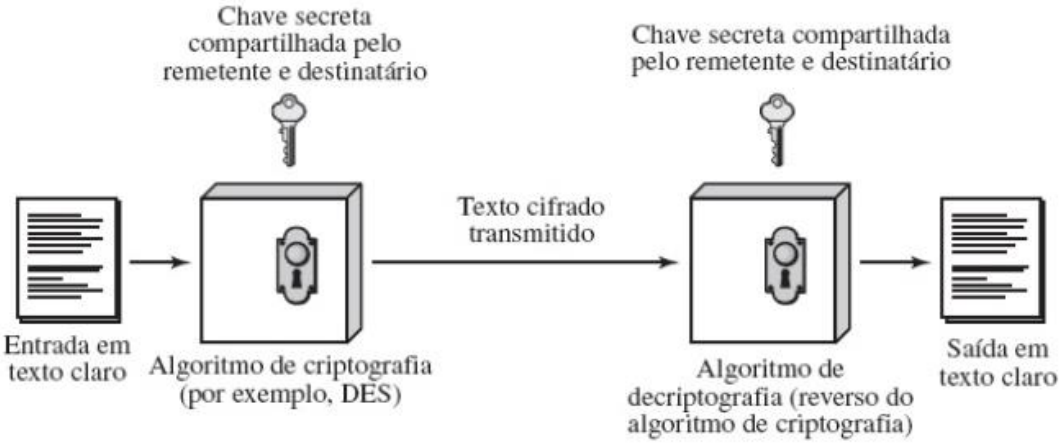
- Sistemas Criptográficos:
  - Tipo de operações criptográficas
    - Substituição e Transposição
    - Operações matemáticas complexas
  - Número de Chaves
    - Chave única ou secreta / par de chaves ou público
  - Forma que o texto original é processado
    - bloco / *stream* (fluxo)

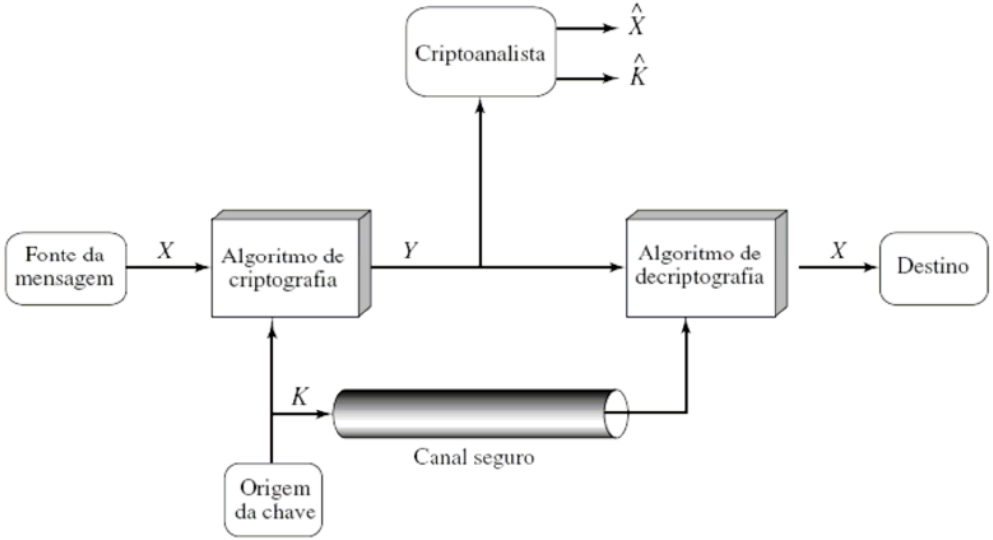
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia Simétrica – Chave Secreta

- Usada desde o tempo de Cristo
- Algoritmos rápidos → uso na confidencialidade do tráfego
- Depende do contato entre as partes
- A Criptografia Assimétrica (anos 70) resolve isso

Modelo Simétrico





UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptoanálise

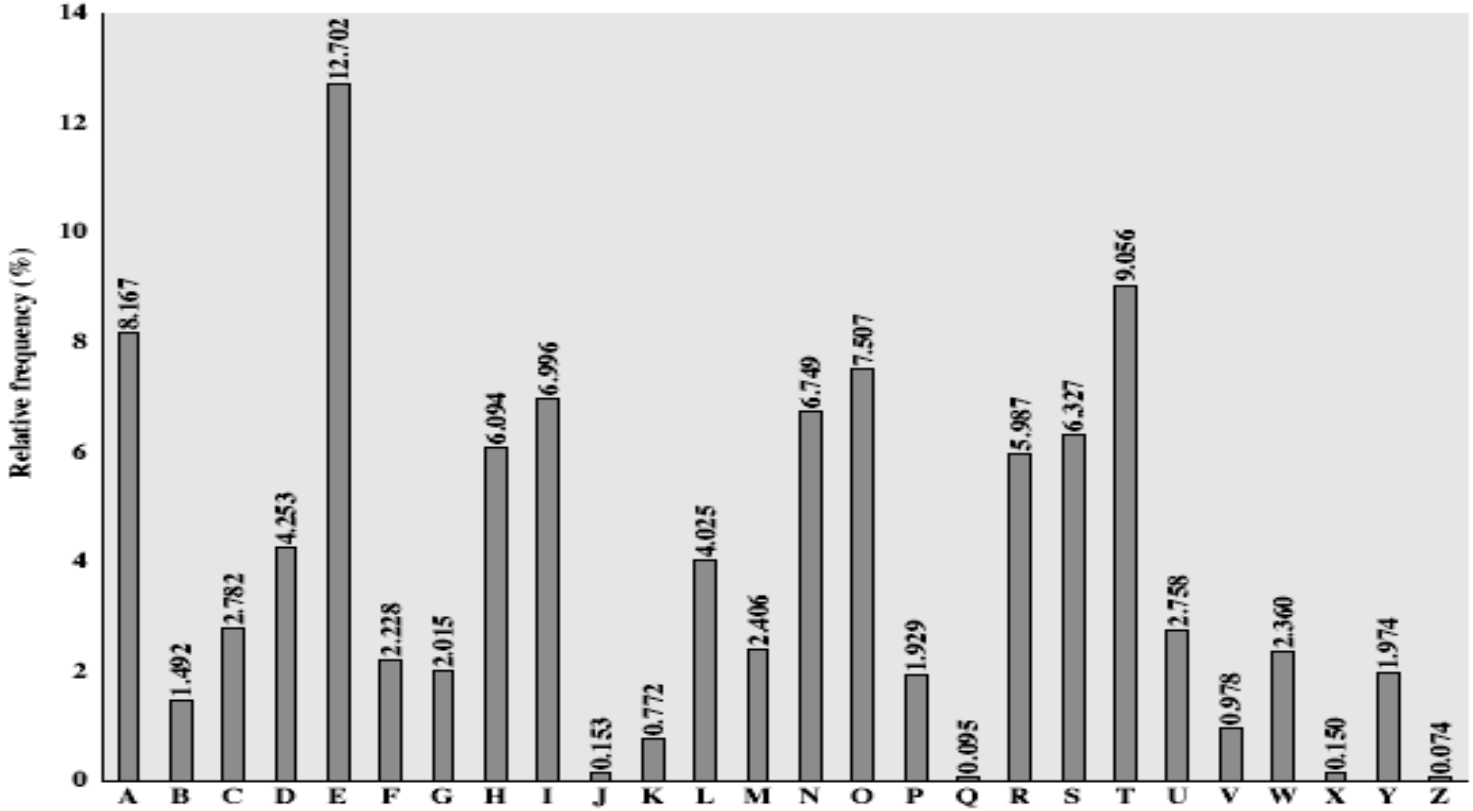
Tipo de ataque	Conhecido ao criptoanalista
Apenas texto cifrado	• Algoritmo de criptografia • Texto cifrado
Texto claro conhecido	• Algoritmo de criptografia • Texto cifrado • Um ou mais pares de texto claro/texto cifrado formados com a chave secreta
Texto claro escolhido	• Algoritmo de criptografia • Texto cifrado • Mensagem de texto claro escolhida pelo criptoanalista, juntamente com seu texto cifrado correspondente, gerado com a chave secreta
Texto cifrado escolhido	• Algoritmo de criptografia • Texto cifrado • Texto cifrado pretendido, escolhido pelo criptoanalista, juntamente com seu texto claro decriptografado correspondente, gerado com a chave secreta
Texto escolhido	• Algoritmo de criptografia • Texto cifrado • Mensagem de texto claro escolhida pelo criptoanalista, juntamente com seu texto cifrado correspondente, gerado com a chave secreta • Texto cifrado pretendido, escolhido pelo criptoanalista, juntamente com seu texto claro decriptografado correspondente, gerado com a chave secreta

Ataques por Força Bruta

- Mais importante que o número de caracteres é a sua entropia (senha “forte”)

Cifras de Substituição

- Cifra de César
  - Um caracter substituído pelo shift + 3
  - O Infnet é o melhor = RLQIQHXHRPHOKRU
  - Possui a óbvia repetição de padrão
  - Poderia ser aprimorado com substituição mono alfabética, mas...



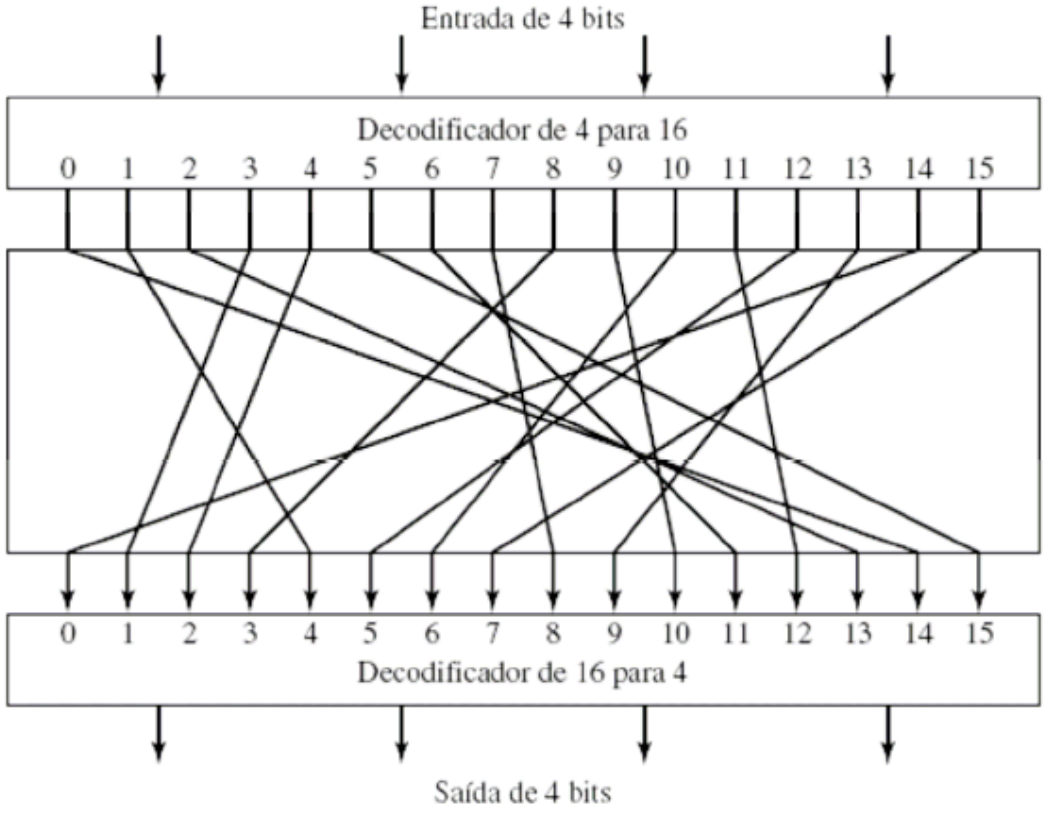
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Esteganografia

- Voltou a ser discutida por relatos de uso em atividades terroristas
- Ocultação de mensagens em arquivos de texto, imagens ou sons
  - Veja http://www.steganos.com e http://www.jjtc.com/Steganography/tools.html

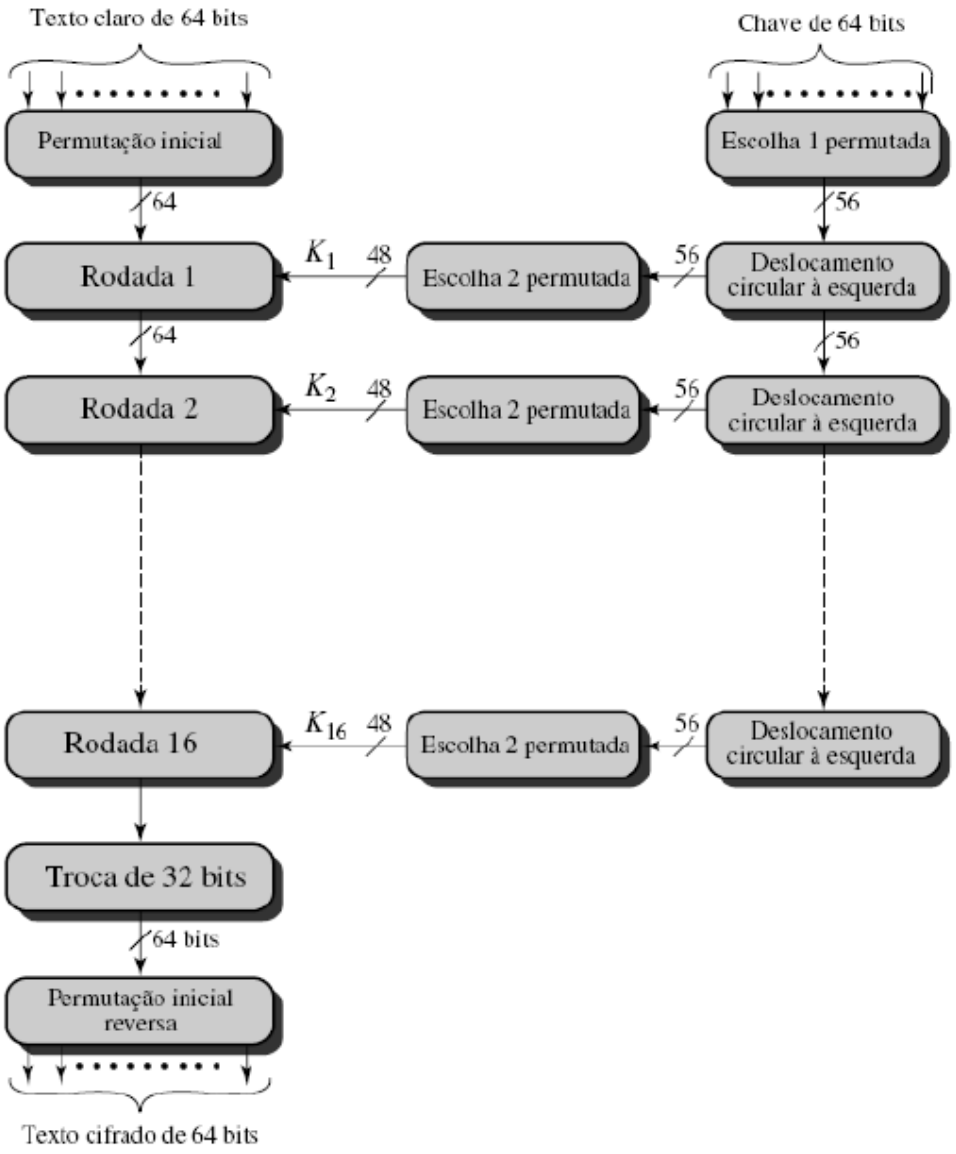
Cifras de Bloco e Fluxo

- As cifras de fluxo não são mais usadas
- As cifras de bloco substituem grupos de bits



DES – Data Encryption Standard

- O uso de permutações e substituições
- Chave de 56 bits
- Facilidade de implementação em hardware



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptoanálise do DES

- Com o algoritmo conhecido, a robustez recai na chave
- Efeito Avalanche – alteração de um bit na chave altera aproximadamente metade da cifra – adivinhação inviável
- Bruta Força é bem sucedida em algumas horas
- Veja: http://www.cryptography.com/resources/whitepapers/DES.html