Segurança em comunicações
Evolução histórica

Redes de Comunicação de Dados

ISEL – DEETC

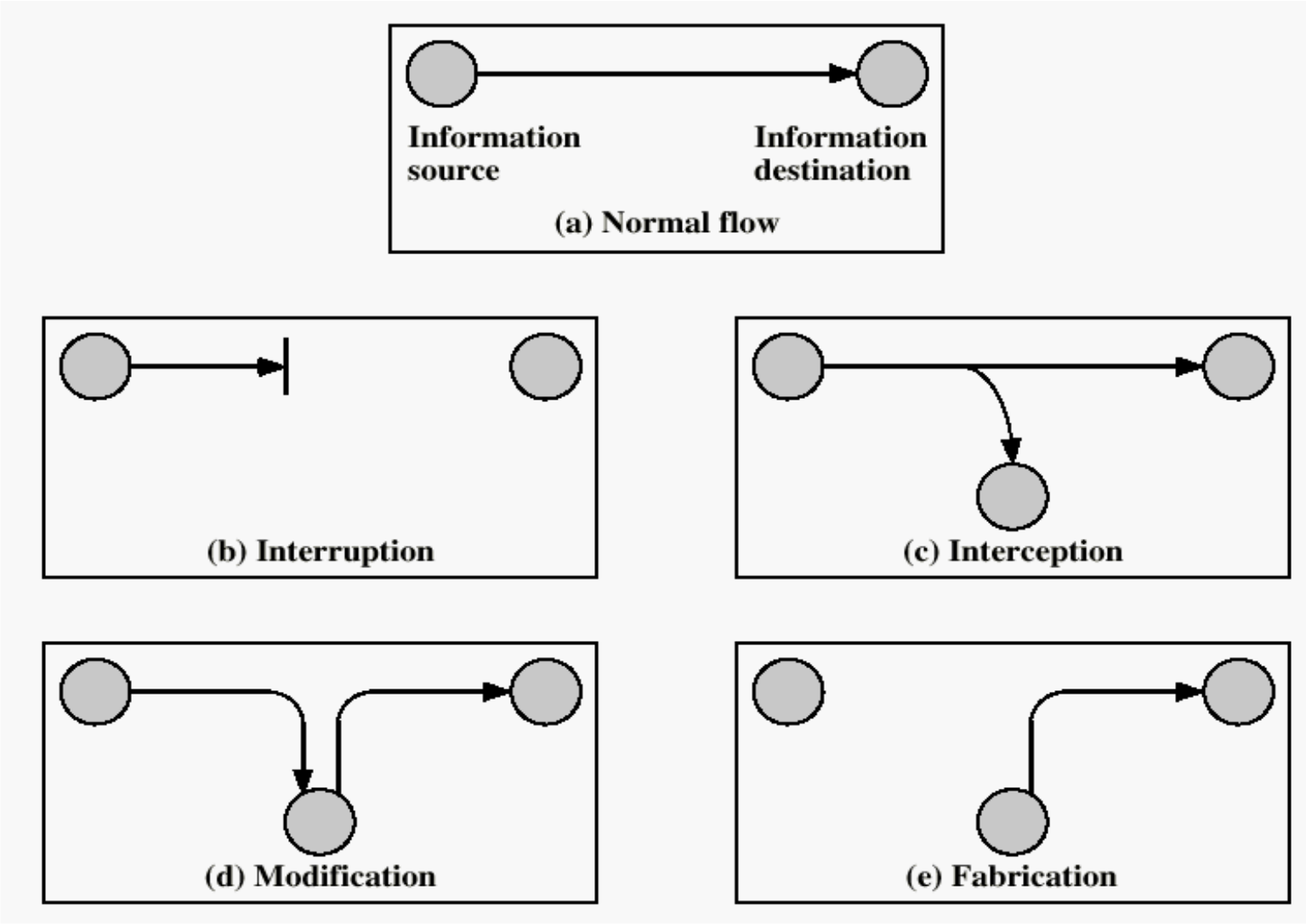
Propriedade curiosa da informação

“Informação é a única coisa que pode ser roubada continuando o seu proprietário na sua posse.”

Elementos e requisitos de segurança

- **Confidencialidade**: Protecção da informação contra descoberta ou intercepção não autorizada; privacidade
- **Integridade**: Impedir a informação/transmissão de ser alterada/danificada de forma não-autorizada, imprevista ou acidental
- **Autenticação e Identificação**: Distinguir, determinar e validar a identidade do utilizador/entidade (se é quem diz ser)
- **Não-repúdio**: Impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação
- **Controle de acesso**: Limitar/controlar nível de autorizações de utilizadores/entidades a uma rede, sistema ou informação
- **Disponibilidade**: Confiabilidade de redes, sistemas e equipamentos para evitar ou recuperar de interrupções

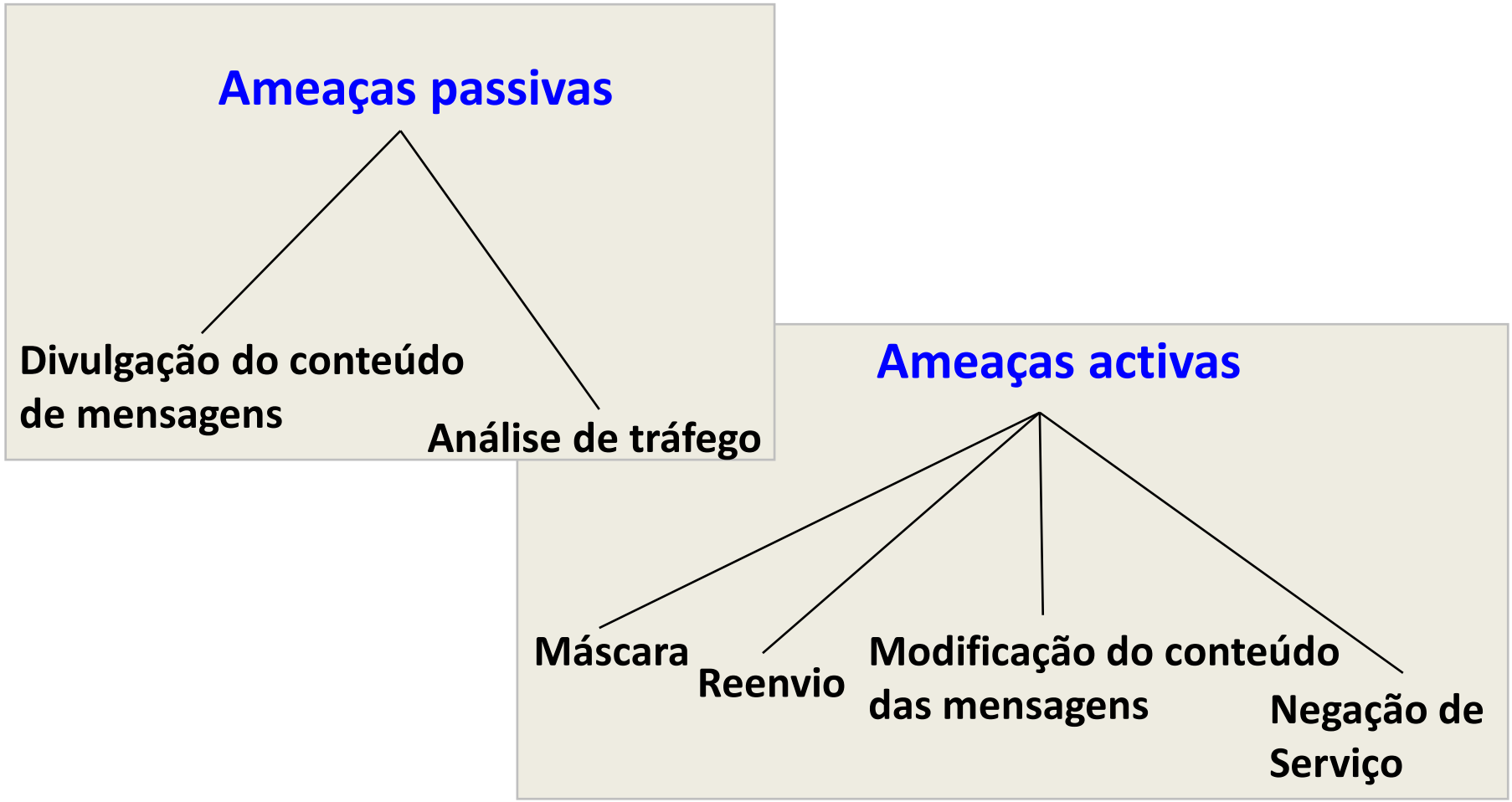
Ataques à segurança



Ataques à segurança

- **Interrupção:** Ataque à disponibilidade
- **Intercepção:** Ataque à confidencialidade.
- **Modificação:** Ataque à integridade.
- **Fabricação:** Ataque à autenticidade.

Ameaças passivas e activas



Criptografia

A criptografia trata da escrita (grafia) secreta (cripto)

Preocupa-se com o desenvolvimento de algoritmos que possam ser utilizados para:

- **Esconder o conteúdo de mensagens** de todos, excepto de quem envia e do destinatário (privacidade ou segredo), e/ou

- **Verificar a correcção de uma mensagem** para um destinatário (integridade e autenticação)

Criptografia

Definição: *A criptografia é o* ***estudo das técnicas matemáticas relacionadas com aspectos da segurança da informação*** *tais como confidencialidade, integridade e autenticação.*

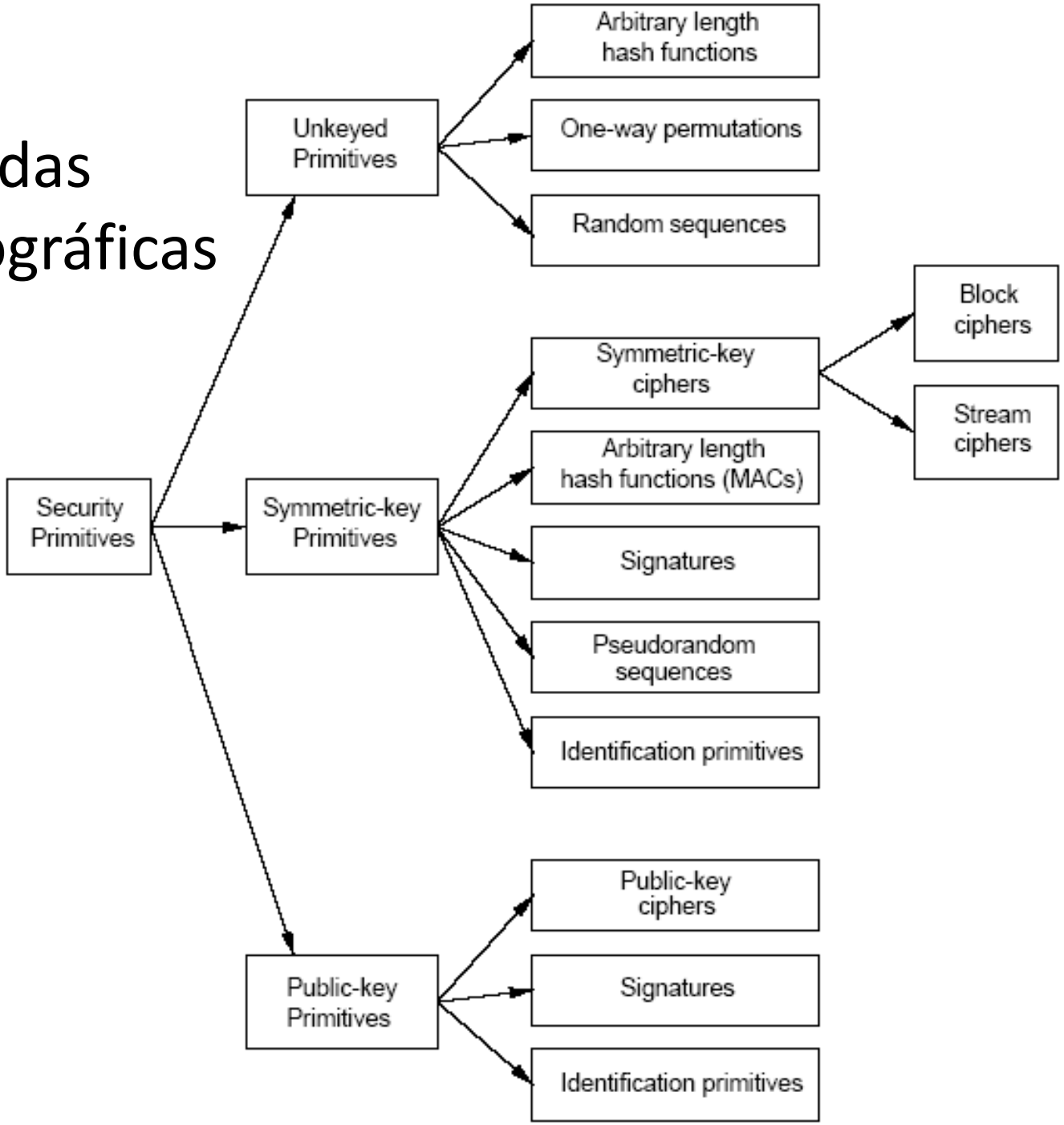
Como conseguir boa cifra?

- **Algoritmos bem revistos**
  - De maneira a que as fraquezas não se possam “esconder” até depois da implementação
- **Geração e gestão de chaves excelente**
  - Para manter a chave secreta
- **Algoritmos suficientemente complexos** de maneira a não permitirem ataques exaustivos com sucesso

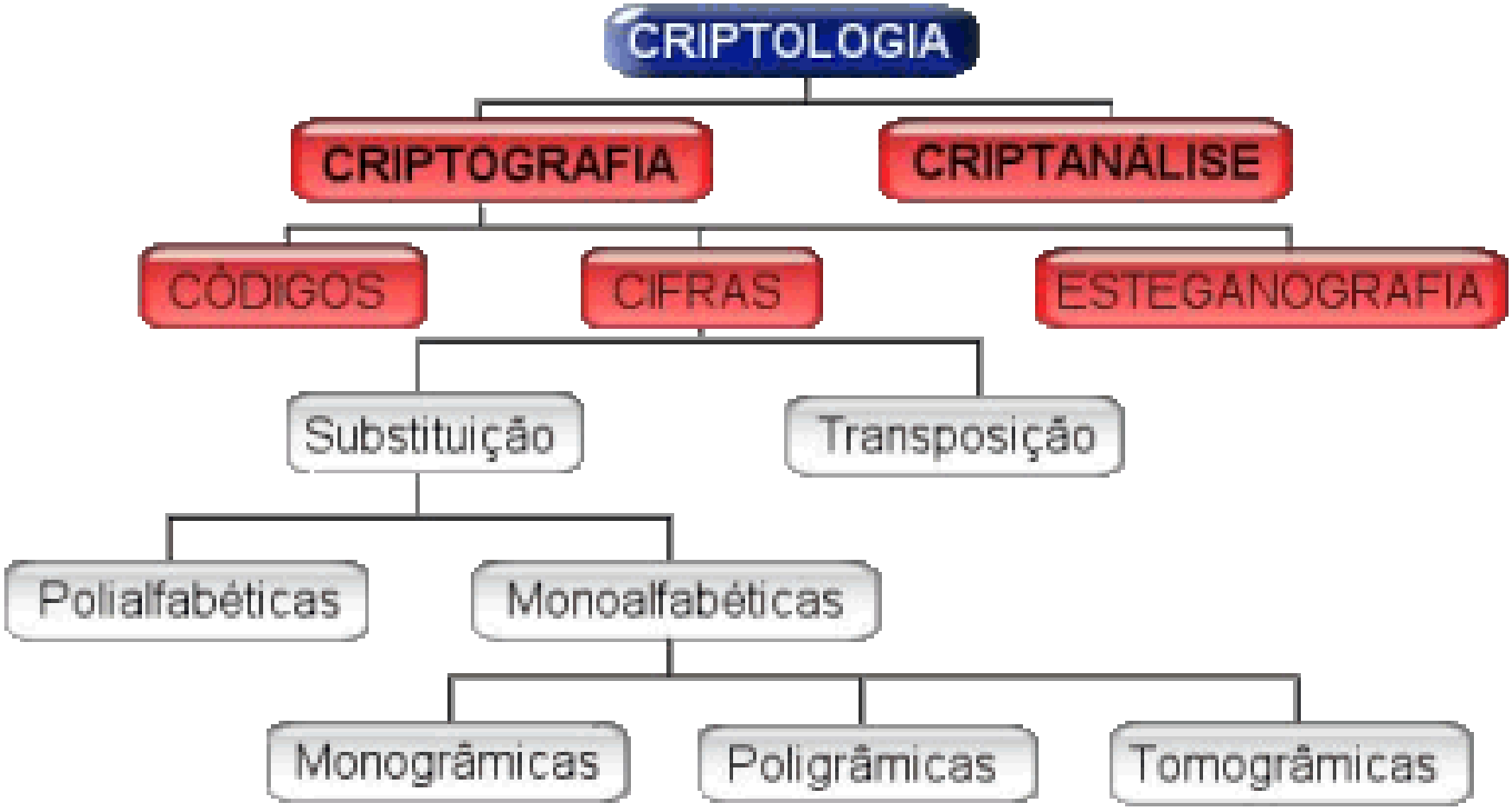
Avaliação das primitivas criptográficas

- As primitivas criptográficas devem ser avaliadas de acordo com vários critérios, nomeadamente:
  - **Nível de segurança**
  - **Funcionalidade**
  - **Métodos de operação**
  - **Eficiência**
  - **Facilidade de implementação**
  - Estes critérios, quando aplicados em conjunto, levaram à não utilização de algoritmos de cifra que em alguns dos critérios eram muito promissores, mas que falhavam noutros.

Taxonomia das primitivas criptográficas



Organograma - Cifra de bloco



[http://www.numaboa.com.br/criptologia/intro.php]

Cifras de substituição

- Substituições Monoalfabetica Simples
  Cifras de substituição monográmica monoalfabética onde cada UM dos caracteres do texto original é substituído por UM outro (daí chamada de monográmica), de acordo com apenas UM alfabeto cifrante pré-estabelecido (ou seja, monoalfabética).
- Substituições Monoalfabetica Homofônicas
  Cifras de substituição que traduzem cada um dos caracteres do texto claro para um dos símbolos de um conjunto de símbolos, ou seja, cada um dos caracteres pode ser substituído por um dos vários existentes no cifrante. Só se conhecem substituições homofônicas monoalfabéticas (que utilizam apenas UM alfabeto cifrante).
- Substituições Monoalfabetica Tomográficas
  Cifras de substituição nas quais cada um dos caracteres da mensagem em claro é substituído por dois ou mais símbolos. Só se conhecem substituições tomográficas monoalfabéticas, ou seja, que utilizam apenas UM alfabeto cifrante.
- Substituições Monoalfabetica Poligrâmicas
  Quando os caracteres do texto claro são tratados em grupos de mais de uma letra e estes grupos são substituídos pelo mesmo número de caracteres cifrados, considera-se a substituição como **poligrâmica**. Se o grupo for de duas letras, ela será digrâmica; se for de três letras, ela será trigrâmica e assim por diante. O comprimento do texto claro e do texto cifrado será igual porque cada grupo de caracteres é substituído por outro com o mesmo número de caracteres.
- Substituições Polialfabéticas
  As cifras de substituição onde mais de um alfabeto cifrante é utilizado são conhecidas como substituições polialfabéticas.

http://www.numaboa.com/criptografia)

História da criptografia

Antiguidade (ver http://www.hu60.com/Criptologia.htm)

1900 a.C. - Khnumhotep II - Os egípcios documentaram os planos das suas pirâmides em placas de argila substituindo palavras ou trechos por outros. Isto de maneira a despistar os possíveis ladrões.

600 a 500 a.C. - O Livro de Jeremias e as **Cifras Hebraicas** (substituição simples)

487 a.C. - Tucídides e o **Bastão de Licurgo** (transposição)

± 300 a.C. - Euclides e os Elementos (Teoria dos Números e Números Primos)

276 a 194 a.C. - O Crivo de Erastótenes (Números Primos)

204 a 122 a.C. - O Código de Políbio - Telégrafo óptico (substituição poligrâmica)

50 a.C. - O **Código de César** (substituição simples)

História da criptografia

79 d.C. - A **Fórmula Sator ou Quadrado Latino** (transposição)

400 d.C. - **Cifra do Kama-Sutra** (substituição simples)

Idade Média

801 a 873 d.C. - **al-Kindi** e a **criptoanálise**

Apesar de não se saber quem foi o primeiro a perceber que a **variação na frequência de letras poderia ser explorada para se quebrar cifras**, a descrição mais antiga de que se tem conhecimento e que descreve esta técnica data do século IX e é devida ao cientista Abu Yusuf Ya 'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi.

1119 a 1311 d.C. - Templários (substituição simples por símbolos)

História da criptografia

Renascença

1466 d.C. - Leon Battista **Alberti** (inventor da substituição polialfabética)

1518 d.C. - Johannes **Trithemius** (esteganografia, tabela de substituição, primeiro livro impresso)

[Esteganografia é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra.]

1533 d.C. - **Pig Pen** (substituição simples por símbolos)

1550 d.C. - Girolamo **Cardano** (esteganografia e substituição com auto-chave)

1553 d.C. - Giovanni Battista **Bellaso** (substituição polialfabética com palavra-chave)

1558 d.C. - Philibert **Babou** (substituição homofónica)

História da criptografia

1563 d.C. - Giambattista **Della Porta** (substituição polialfabética com palavra-chave)

Foi o inventor do primeiro sistema literal de chave dupla, ou seja, da primeira cifra onde se altera o alfabeto cifrante a cada letra cifrada. Dificultou a aplicação da análise de frequência de ocorrência das letras.

Della Porta descreve a primeira substituição bigrâmica da história da criptologia. Este método caracteriza-se pela substituição de duas letras por um símbolo único.

História da criptografia

1586 d.C. - Blaise de **Vigenère** (substituição polialfabética com palavra-chave)

A cifra de Vigenère é uma **cifra de substituição polialfabética**. Seu método pode ser considerado como uma **generalização do Código de César**, só que, ao invés de deslocar cada letra um número fixo de posições para obter a letra cifrada, o deslocamento é variável e determinado por uma frase ou **palavra-chave**.

A grande força da cifra de Vigenère é que **letras iguais são cifradas de maneiras diferentes**.

Por exemplo, um E do texto claro pode ser cifrado por qualquer uma das letras do alfabeto, como M, V, L ou P. Isto inviabiliza a aplicação da análise de frequência de ocorrência das letras dificultando a criptoanálise.

Esta cifra **resistiu à criptoanálise por quase três séculos**, apesar de ser relativamente fácil quebrá-la.

História da criptografia

Idade moderna

1901 d.C. - Guglielmo **Marconi** - Comunicação sem fios

Prémio Nobel da Física em 1909

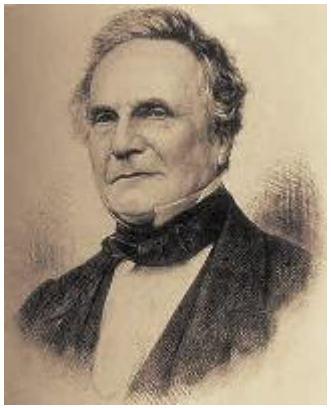
1917 d.C. - **William F. Friedman -** "Pai da criptoanálise norte-americana".

1917 d.C. - **Gilbert Sandford Vernam** - Um funcionário da AT&T inventa uma máquina de cifragem polialfabética capaz de usar uma chave totalmente aleatória e que nunca se repete. Esta máquina foi oferecida ao governo dos EUA para ser usada na Primeira Guerra Mundial, porém foi rejeitada. Foi colocada no mercado comercial em 1920.

Vernam desenvolveu uma cifra inviolável, baseada na cifra de Vigenère, e que leva seu nome. Com o aperfeiçoamento feito por Mauborgne, nasce o **One-Time-Pad**.

História da criptografia

Máquinas cifrantes



1854 d.C. - Charles Babbage e as **Máquinas de Diferenças.**

Projectou a primeira máquina a que podemos chamar computador.

A sua máquina foi construída recentemente, 200 anos após a data do seu nascimento, e funcionou.

1920 d.C. - **A cifra de Bazeries** .

Criação de um cilindro cifrante.

História da criptografia

1915 – 1960 d.C.

Máquinas de rotor famosas

- Estados Unidos da América: Converter M-209
- Reino Unido: TYPEX
- Japão: Red, Purple
- Alemanha: Enigma

http://www.codesandciphers.org.uk/enigma/index.htm

História da criptografia

Criptografia moderna

1948 d.C. - Claude Elwood **Shannon** – "Uma Teoria Matemática da Comunicação". Grande impulso à teoria da informação.

1960 d.C. … - O Dr. **Horst Feistel**, liderando um projecto de pesquisa no IBM Watson Research Lab, desenvolve a **cifra Lucifer**.

Alguns anos mais tarde, esta cifra servirá de base para o **DES** e outros produtos de cifra, criando uma família conhecida como "cifras Feistel".

1974 d.C.– A cifra de bloco **DES** (*Data Encryption System*) - O NBS (*National Bureau of Standards*) publica a norma nos EUA.

História da criptografia

1976 d.C. - **Diffie-Hellman**

Revolução iniciada com a publicação de um método que permitia **trocar chaves sem estas necessitarem passar em claro na rede**. A partir daqui foi desenvolvido um novo tipo de criptografia designada por criptografia de chave assimétrica.

História da criptografia

1978 d.C. – **RSA** (Ron **R**ivest, Adi **S**hamir, Len **A**delman)

- Deu origem à **criptografia de chave pública ou assimétrica** (*public key cryptography*)
- Publicado pela primeira vez em 1978, no MIT (serviços secretos referiram que já conheciam o método anteriormente).
- Baseada na teoria dos números/aritmética modular



História da criptografia

1986 d.C. – Miller - Curvas elipticas

A criptografia usando o algoritmo da curva elíptica é sugerida por Miller.

1980 d.C. – Evolução dos **algoritmos de *hash* (*message digest*)** para ajudar a garantir de integridade

1990 d.C. … – **Comunicação quântica**

Trabalhos com computadores quânticos e criptografia quântica.

1993 d.C. - Biham e Shamir - **Criptoanálise diferencial**

2000 d.C. - O algoritmo Rijndael é seleccionado para substituir o DES e é denominado **AES - Advanced Encryption Standard**

2008 d.C.– Governo dos EUA procura **sucessor** para os algoritmos de *hash* existentes, nomeadamente da família **SHA256** e outros.

FIM