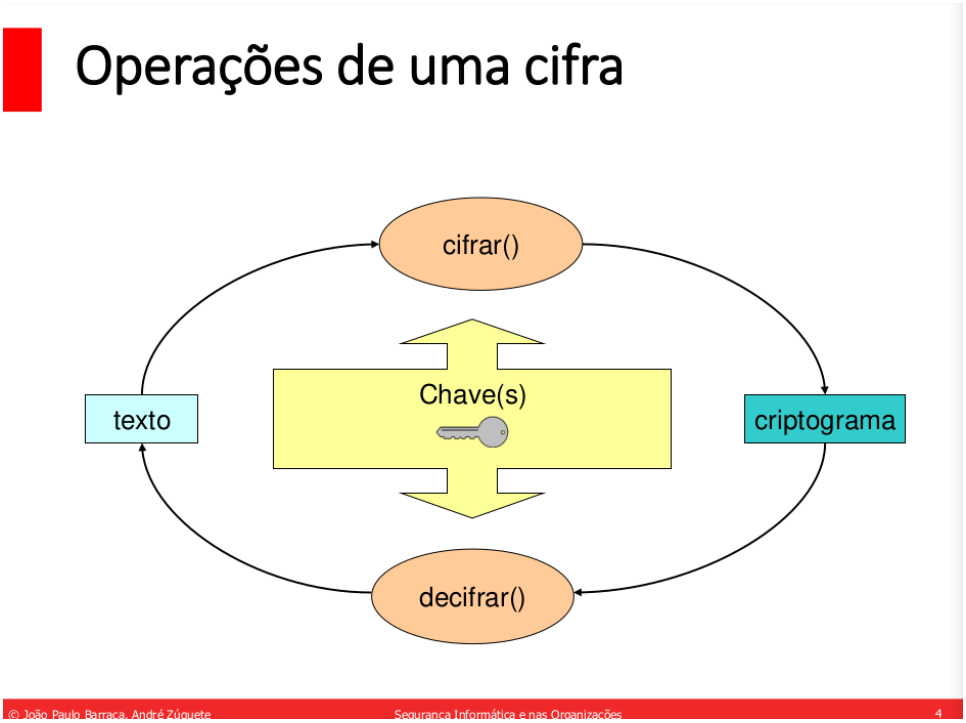
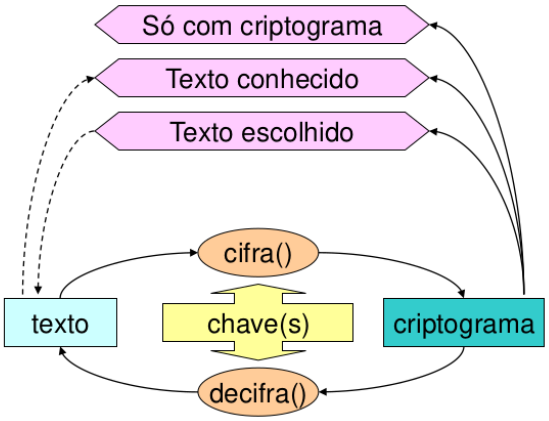
Apontamentos Slides 03

- **Criptografia**
  - Arte de escrever de forma confidencial
- **Criptanálise**
  - Arte ou ciência de quebrar sistemas criptográficos ou inofrmação criptogradafada
- **Criptologia**
  - Criptografia + Criptanálise
- **Cifra**
  - Técnica concreta de criptografia
- **Operação de uma cifra**
  - **Cifra :** texto claro -> criptograma
  - **Decifra:** criptograma -> texto claro
- **Algoritmo**
  - Modo de transformação de dados
- **Chave:** parâmetro do algoritmo
  - Influencia a operação do algoritmo



- **Criptanálise**
  - **Objetivos:**
    - Obtenção do texto original relativo a um criptograma
    - Obtenção de uma chave de cifra ou de uma equivalente
    - Obtenção do algoritmo de cifra
      - Engenharia reversa
      - Normalmente os algoritmos são conhecidos

Ataques por Criptanálise



- **Ataques por Força Bruta (ataque genérico**
  - Pesquisa exaustiva sobre todo o espaço de chaves, até se encontrar uma chave adequada
  - Não é prática oara espaços de dimensão grande
  - É importante que exista aleatoriedade na chave
- **Ataques mais inteligentes**
  - Reduzir o espaço de pesquisa para uma dimensão menos:
    - Palavras
    - Números
    - Conjunto reduzido
    - Alfabeto
  - Identificar padrões em algumas operações, etc...

- **Uso teórico != Exploração prática**
  - Na teoria uma cifra pode ser boa mas usada com más práitacas, como a reutilização de one-time pads, compromete a sua boa utilização

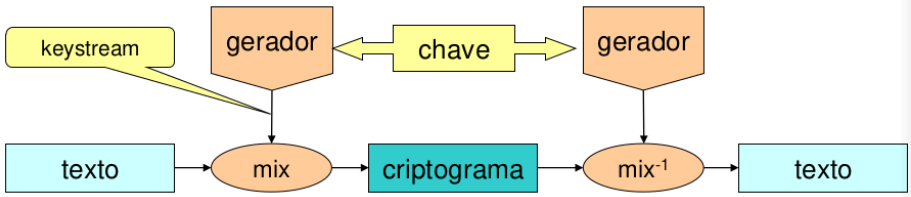
- **Cifras seguras na prática**
    - A segurança é assegurada pela dificuldade computacional de realizar a criptanálise
        - Usando força bruta
    - Têm uma segurança baseada em limites razoáveis:
        - Custo de uma solução técnica de criptanálise
        - Infraestrutura reservada para a criptanálise
        - Tempo útil de criptanálise
    - **5 critérios de Shannon**
        - **Quantidade de secretismo oferecida**
            - Comprimento da chave
        - **A complexidade na escolha das chaves**
            - Geração de chaves, deteção de chaves fracas
        - **A simplicidade da realização**
        - **A propagação de erros**
        - **A dimensão do criptograma**
            - Relativamente aos respetivos textos originais
    - **Confusão**
        - Complexidade na relação entre o texto, a chave e o criptograma
            - Os bits resultantes devem depender dos bits de entrada de uma forma complexa
    - **Difusão**
        - Alteração de **grandes porções** do criptograma em função de uma pequena alteração do texto
            - Se um bit de texto se alterar, então o criptograma deverá **mudar substancialmente,** de forma imprevisível.
            - **Efeito avalanche**
    - **Assumir sempre o pior caso**
        - **O criptanalista conhece o algoritmo**
            - A segurança está na chave
        - **O criptanalista possui grande número de criptogrmas gerados com um algoritmo e chave**
            - Os criptogramas não são secretos
        - **O criptanalista conhece parte dos textos originais**
            - É normal haver alguma noção do texto original
            - Ataques com texto escolhido
            - Ataques com texto conhecido

- **Robustez criptográfica**
    - Não há forma de avaliar a robustez de forma precisa
    - São robustos até que alguêm os quebre
    - Existem orientações públicas do que deve e não ser usado
- **Algoritmos públicos, sem ataques conhecidos, supostamente são mais robustos**
    - Mais investigadores à procura de fraquezas

- **Algoritmos com chaves maiores são tendencionalemente mais robustos**
    - Mas frequentemente são mais lentos

- **Cifras Contínuas (Stream)**
    - Mistura de uma chave contínua (keystream) com o texto ou criptograma
        - **Aleatória - one time pad**
        - **Pseudoaleatória - gerador**
    - **Cifra poli-alfabética**
        - Cada símbolo da chave contínua define um alfabeto

Cifras Contínuas (Stream)



- **Keystream pode ser infinita, mas possui um período (Período depende do gerador)**
- **Questões práticas de segurança**
    - Cada keystream só pode ser **uma vez!!!!!!!**
    - Caso contrário a soma dos criptogramas fornece a soma dos textos
    - Dimensão do texto **tem de ser menor** que período
        - Exposição de keystream é **total com textos escolhidos/conhecidos**
        - Período permitem analistas conhecer partes do texto
    - Controlo de integridade **é mandatório**
        - **Não existe difusão,** apenas confusão
        - Criptogramas podem ser **manipulados livremente**

- **Cifras Simétricas**
  - **Chave secreta única,** partilhada por 2 ou mais interlocutores
  - Permite:
    - Confidencialidade para todos os conhecedores da chave
    - Autenticação de mensagens (cifra por blocos)
  - Muito eficiente
  - Demasiadas chaves
  - Distribuição de chaves
- **Cifras Simétricas Contínuas**
  - Obriga que os emissores/recetores estejam sincronizados
  - Normalmente sem possibilidade de acesso aleatório rápido
- **Cifras Simétricas por blocos**
  - Blocos de grande dimensão, >128bits
  - Difusão, confusão
  - Exemplos de algoritmos:
    - **DES**
    - **IDEA**
    - **AES**
  - **S-Box (Substituição):** bit de entrada troca bits da saída**;** alteração de um bit provoca a alteração de pelo menos metade dos bits
  - **S-Box (Permutação):** permuta a posição de bits entre a entrada e saída
- **DES**
  - A maioria dos valores de 56 bits são adequados
  - Fáceis de identificar e de evitar
  - Pesquisa exaustiva
  - 56 bits são atualmente insuficientes
  - **Solução:**
    - Cifra tripla, porque cifra dupla não é segura
- **ECB**
  - Cifra direta e decifra direta de cada bloco
  - Blocos são independentes
  - **T1=T2 então C1=C2...**
- **CBC**
  - Cifra e decifra com feedback do anterior
  - Bloco inicial usa IV
- CBC não propaga tantos padrões
- **Problemas de alinhamento ECB/CBC**
  - Necessitam de textos com dimensão múltipla da dimensão do bloco
  - Blocos incompletos necessitam de tratamento diferenciado
  - Resultado é um bloco
    - Criptograma pode ser maior que o texto em claro
  - Alternativa: Padding
  - **Ciphertext Stealing**
    - Troca ordem de cifra/decifra dos dois últimos blocos

- Usa parte do criptograma do penúltimo para preencher o último
- Usa Padding fixo e cifra contínua antes de cifra por blocos

Modos: Comparação

	Bloco		Contínua (Stream)			
	ECB	CBC	OFB	CFB	CTR	GCM
Ocultação de padrões no texto		✓	✓	✓	✓	✓
Confusão na entrada da cifra		✓		✓	Contador Secreto	Contador Secreto
Mesma chava para mensagens diferentes	✓	✓	Outro IV	Outro IV	Outro IV	Outro IV
Dificuldade de alteração	✓	✓ (...)				✓
Pré-processamento			✓		✓	✓
Paralelização	✓	decifra	com pré. proc.	decifra	✓	✓
Acesso aleatório uniforme						
Propagação de erros		próximo bloco		alguns bits seguintes		detetado
Capacidade de re-sincronização	perda de blocos	perda de blocos		perda de múltiplos n-bits		detetado

---

- **Ataque Meet in the Middle**
  - Cifra dupla
  - Se C e T forem conhecidos, podem-se calcular a Decifra e a Cifra
    - Db(kb, C), variando Kb
    - Ea(ka, T), variando Ka
  - Chaves encontradas quando se verificar a igualdade Db(kb, C) = Ea(ka, T)

- **Cifras assimétricas por blocos**
  - **Para de chaves**
    - Privada
    - Pública
  - Permitem:
    - Confidencialidade na troca de segredos
    - Autenticação de conteúdos (integridade) e de autoria (assinaturas digitais)
  - São pouco eficientes
  - Interação com N interlocutores requer apenas N pares de chaves
    - Cifra por blocos simétrica iria requerer N^2

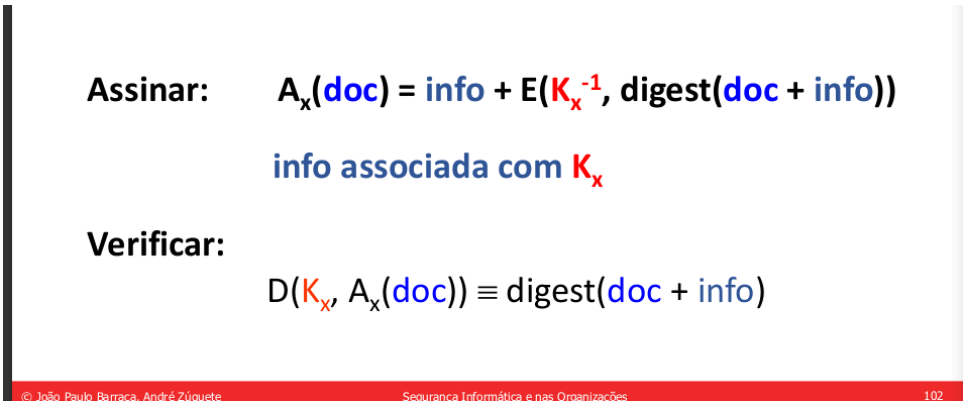
    - Chaves públicas têm de ser distribuídas à priori
    - Tempo de vida dos pares de chaves (têm de expirar)
    - **Algoritmos usados**
        - **RSA**
        - ElGamal
        - Curvas elípticas
        - Diffie-Hellman
    - Confidencialidade
        - Publica cifra
        - Privada decifra
    - Autenticidade
        - Publica decifra
        - Privada cifra
    - O resultado da cifra de uma chave pública não deverá ser previsível
        - Concatenação do valor a cifrar com dois valores
            - Fixo
            - Aleatório
- **Cifra Híbrida**
    - Juntar as duas Cifras
- Digest
    - Fingerprint
    - Resultados muito diferentes para entradas similares
    - Resistência à descoberta de um texto
    - Resistência à descoberta de um 2ºtexto
    - Resistência à colisão
- Hash algorithmic
    - MD5
    - SHA

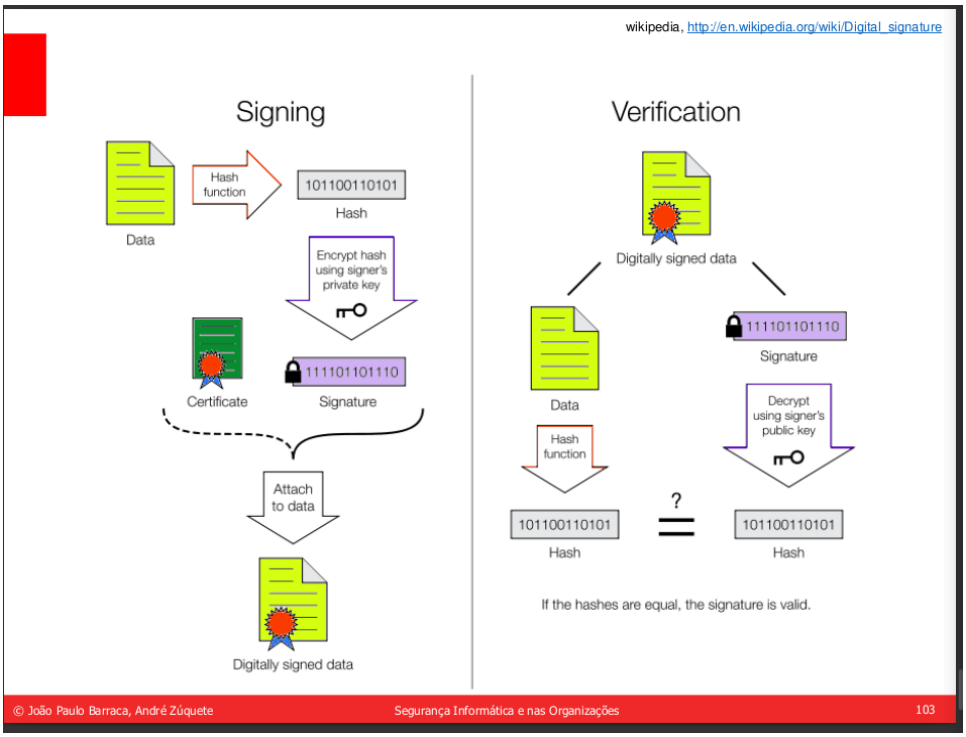
- **MIC**
    - Fornecem capacidade de detetar alterações por máquinas
    - Envio:
        - Calcular Mic (sintese) e enviar T+Mic
    - Receção:
        - Receber dados e verificar se S(T) = MIC
    - Não protege contra alterações deliberadas
- MAC
    - Sintese/HAsh/digest gerada com recurso a uma chave
    - Utilizada para garantir autenticidade/integridadade

- Enviar:
  - M+Mac, Mac=F(K,M)
- Receber:
  - Calcular F(K,M') e comparar com MAC

- **Encrypt then Mac: Mac calculado do criptograma**
  - **Não pode ser calculado a partir do texto**

- **Assinaturas Digitais**
  - Autenticam o conteúdo de documentos
    - Garantem a sua integridade
  - Autenticam o autor
    - Garantem a identidade do autor/criador
  - Previnem repudiação do conteúdo
    - Autor não pode negar a sua criação
      - Só ele tem acesso à chave privada
  - **Cifra assimétrica sobre Síntese**
    - Síntese usada por questões de desempenho
    - Cifra assimétrica para garantir autenticidade





- **Assinaturas cegas**
  - Garante o anonimato e não alteração da informação assinada
  - Assinante não consegue observar os conteúdos assinados