SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

CRIPTPGRAFIA E GESTÃO DE CHAVES

LUIS AMORIM

11 Jun 2022

2 AGENDA

- **Noções de criptografia**
- Gestão de chaves

3 NOÇÕES DE CRIPTOGRAFIA

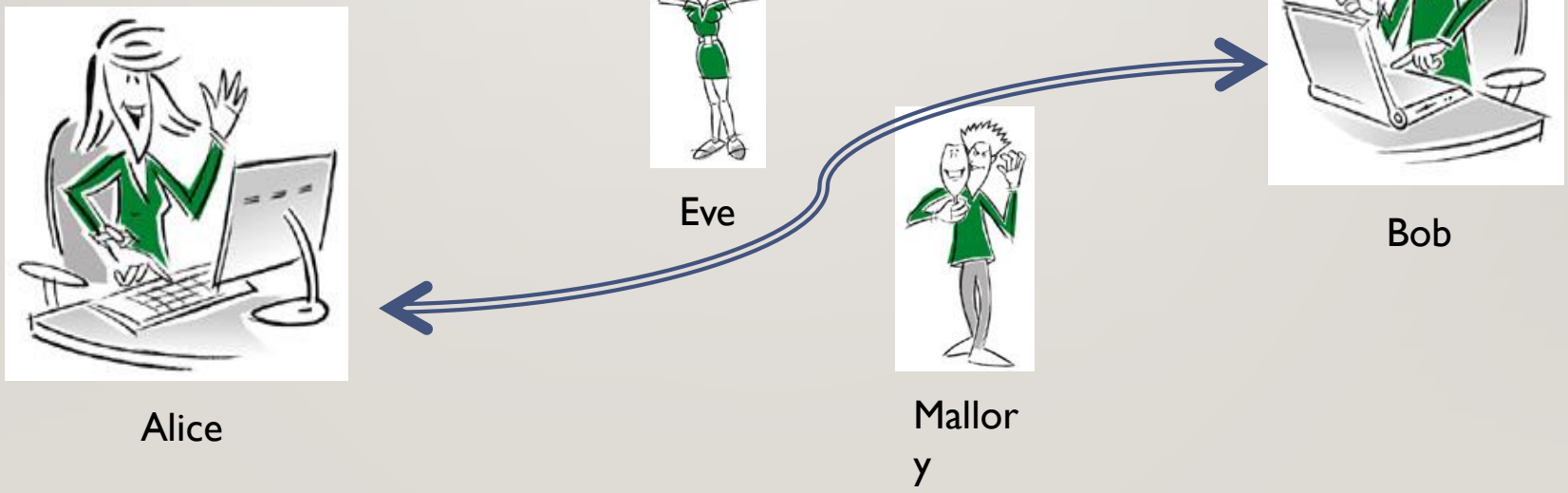
- Criptografia (kryptos=secreto,escondido + gráph0=grafia,escrita)
- O que é?
  - "Escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação"
- Em que consiste?
  - Transformação de textos originais, chamados texto original (plaintext) ou texto claro (cleartext), em informação transformada, chamada texto cifrado (ciphertext), texto código (codetext) ou simplesmente cifra (cipher), que têm a aparência de um texto random ilegível

4 NOÇÕES DE CRIPTOGRAFIA

- O Porquê da Criptografia?
  - Proteger dados (informação)
    - Informações Militares (Tácticas/Estratégias)
    - Informações Científicas (Segurança de Estado)
    - Informações Industriais (Espionagem Industrial)
    - Informações Bancárias (Movimentos Bancários)
    - Informações Comerciais (Comércio Electrónico)
    - Informações Pessoais
    - Etc...

5 NOÇÕES DE CRIPTOGRAFIA

- Utilização de criptografia para protecção
  - Concorrentes ou Inimigos;
  - Hackers;
  - …



6 NOÇÕES DE CRIPTOGRAFIA

- A International Association for Cryptologic Research (IACR) é uma organização científica internacional que mantém a pesquisa nesta área.
  - Organiza conferências
    - **Crypto 2022**, 13 - 18 August 2022, Santa Barbara, USA.
    - **Eurocrypt 2022**, 23 - 27 April 2023, Lyon, France.
  - Workshops
    - **Real World Crypto Symposium,** 13 - 15 April 2022, Amsterdam, The Netherlands
    - **Cryptographic Hardware and Embedded Systems (CHES),**

      18 - 21 September 2022, Leuven, Belgium.
    - **Fast Software Encryption,** 20 - 24 March 2023, Beijing, China
  - Publicações

7 NOÇÕES DE CRIPTOGRAFIA

- Protecção da informação
  - **O foco da segurança da informação deve ser**
    - **protegê-la de algum mal (roubo, alteração, acesso não autorizado)**
    - **ao mesmo tempo que mantém a informação disponível para quem**

  - As técnicas criptográficas estão já disponíveis há alguns anos, mas só por questões de conformidade ou utilização de boas práticas se tem incrementado a sua utilização.
  - A cifra tem-se tornado uma comodidade, vindo já embebida em aplicações ou bases de dados.

8 NOÇÕES DE CRIPTOGRAFIA

- As ameaças que a informação enfrenta:
  - Perda ou Roubo de Media - Tapes ou discos de bakup armazenados ou em transito
  - Roubo de Informação por utilizadores com acesso
  - Distribuição não intencional (envio para um destinatário diferente)
  - Hacking (aplicacional), alterando aplicações ou configurações com impacto nos dados
  - Roubo de dispositivos móveis

9 NOÇÕES DE CRIPTOGRAFIA

- Utilização de criptografia
  - Numa primeira fase generalizou-se a protecção dos dados em transito:
    - SSL
    - VPNs
  - Mas devemos também considerar os riscos da informação permanecer em claro nas origem e no destino
    - roubar um carro no parque ou garagem é muito mais fácil do que tentar roubá-lo numa auto-estrada

10 NOÇÕES DE CRIPTOGRAFIA

- **Protecção da informação em vários pontos**
  - **Segurança de dados armazenados**
    - Cifrar dados armazenados - em disco, tape,..
      - Mas podemos estar a aplicar uma medida desnecessária à maioria dos dados.
      - Necessário pensar como partilhar alguns dos dados com utilizadores que não têm acesso a chaves ou por razões de auditoria
  - **Segurança nos Servidores**
    - A utilização de dispositivos cifrados (tudo cifrado) pode não ser a melhor opção para atacantes internos.
    - Segurança a nível aplicacional
      - Os dados quando utilizados pelas aplicações ganham contexto e significado, quem e como deve aceder
      - Para além do controlo de acessos que já está vulgarizado, existem já soluções ao nível aplicacional que fazem uso de PKIs:
        - gestão documental;
        - e-mail;
        - autenticação de utilizadores;
        - software publishing.

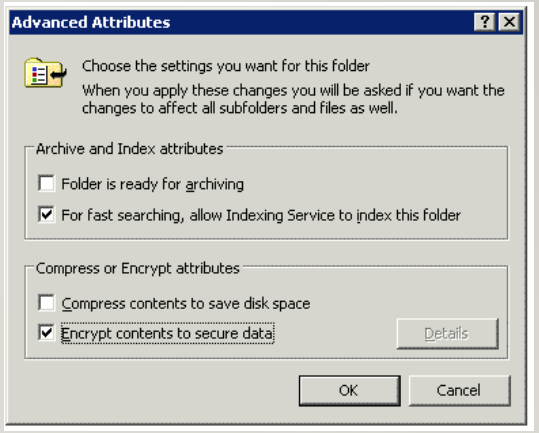
11 NOÇÕES DE CRIPTOGRAFIA

- Protecção da informação em vários pontos
  - **Segurança dos Terminais de utilizador**
    - Considerando como forte ameaça causada pelo Teletrabalho
      - onde o acesso remoto a informação
      - cópia dessa informação para pastas locais, nos PCs ou Portáteis
      - e-mails com attachs em claro para contas pessoais
      - acumulação durante largos anos de informação desnecessária para o trabalho actual), mas que não é apagada
      - Face à mobilidade e número de dispositivos que cada utilizador dispõe, é necessário controlar um conjunto variado de dispositivos:
        - SmartPhones,
        - PDAs,
        - PENs USB,
        - cartões de memória, ...

12 NOÇÕES DE CRIPTOGRAFIA

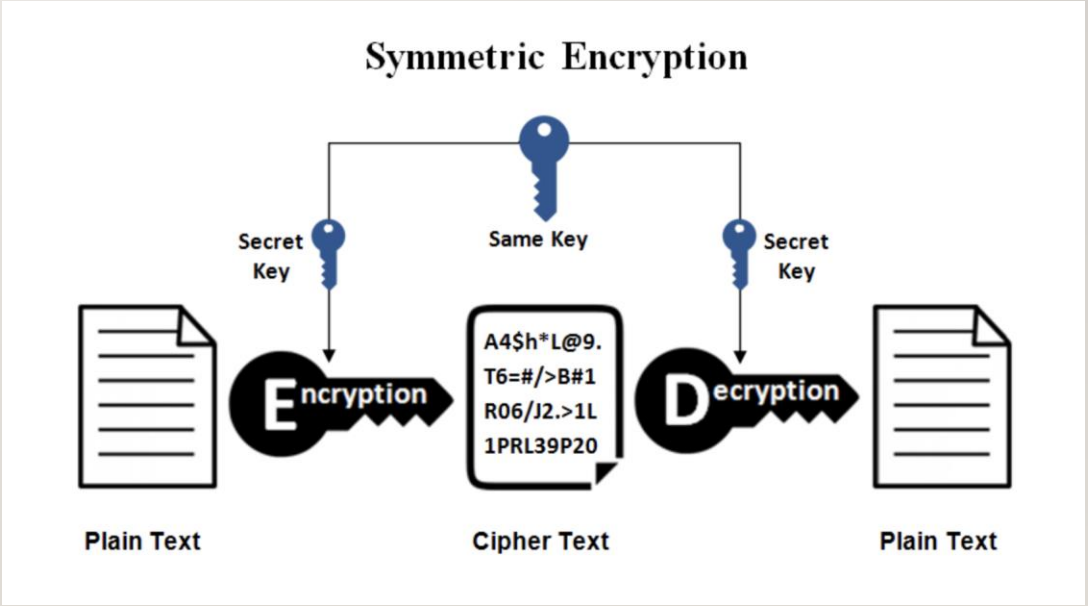
- A resposta pode ser proteger a diversos níveis, de acordo com o tipo de informação ou dispositivo:
  - discos, Tapes, PENs
  - File System
  - ou um nível acima DRM

DriveLock



13 NOÇÕES DE CRIPTOGRAFIA

- **Sistemas criptográficos simétricos**
  - Usam a mesma chave para encriptar e desencriptar mensagens; ou pelo menos, chaves que possam ser determinadas de forma simples e directa uma a partir da outra.



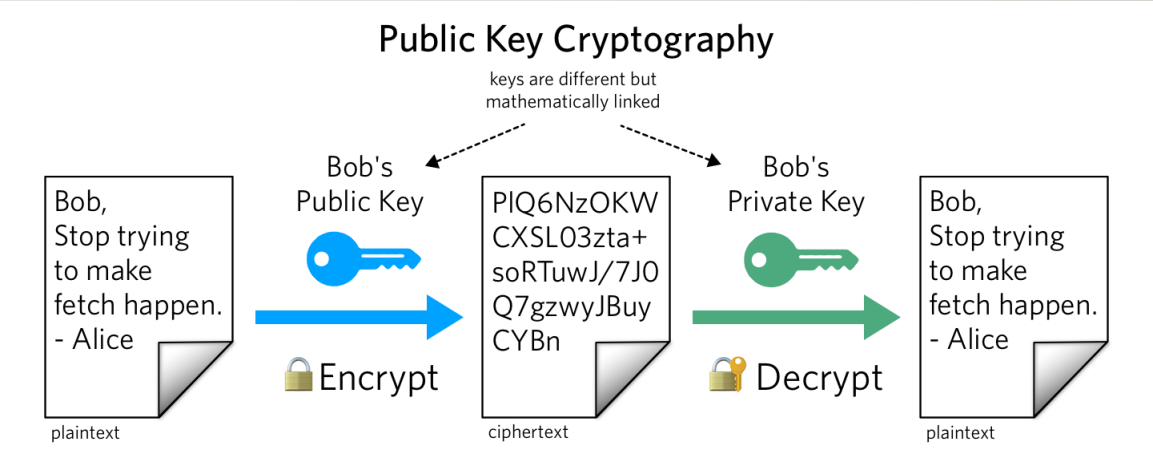
14 NOÇÕES DE CRIPTOGRAFIA

- Sistemas criptográficos simétricos
  - Necessitam de um canal seguro para a divulgação das chaves.
  - Só os utilizadores do grupo podem ter acesso às chaves.
  - Com a saída de um utilizador do grupo, o sistema fica comprometido

  - Exemplos
    - Cifra de Vigenère
    - Sistema de Gronsfeld
    - Código Playfair
    - Substituição de Hill
    - Data Encryption Standard (DES)
    - International Data Encryption Algorithm (IDEA)
    - One Time Pad (One time key, ou Chave Única)
    - Advanced Encryption Standard (AES)

15 NOÇÕES DE CRIPTOGRAFIA

- **Sistemas criptográficos assimétricos (chave pública)**
  - Tipo de encriptação que usa duas chaves distintas, uma para a encriptação e outra para a desencriptação de mensagens (chave pública e chave privada, respectivamente).



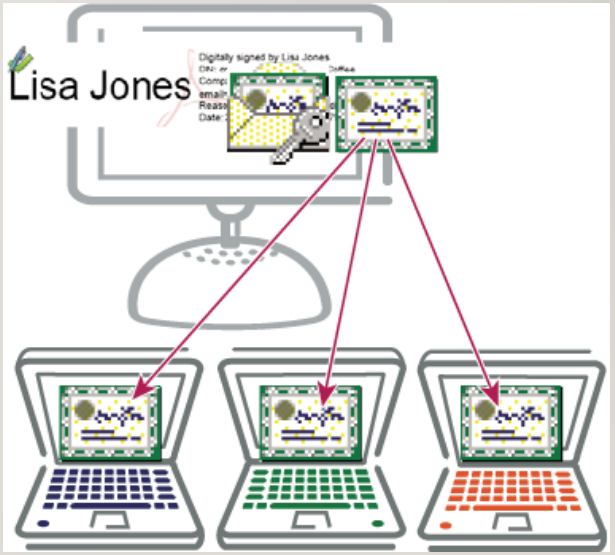
16 NOÇÕES DE CRIPTOGRAFIA

- Sistemas criptográficos assimétricos (chave pública)
  - Evita o problema da divulgação das chaves, dos sistemas simétricos.
  - Cerca de 1000 vezes mais lento que os algoritmos simétricos
  - Utilizações mais comuns ...
    - Distribuição de chaves sem "segredos" pré-acordados
    - Assinaturas digitais e não repúdio
    - Identificação utilizando protocolos de "desafio-resposta" com chaves públicas
    - Encriptação (mas muito mais lento)

  - Exemplos
    - Diffie - Hellman (# 1° sistema de chave pública inventado)
    - HM (Merkle e Hellman)
    - RSA (Ron Rivest, Adi Shamir e Leonard Adleman)
    - PGP (Pretty Good Privacy)

17 NOÇÕES DE CRIPTOGRAFIA

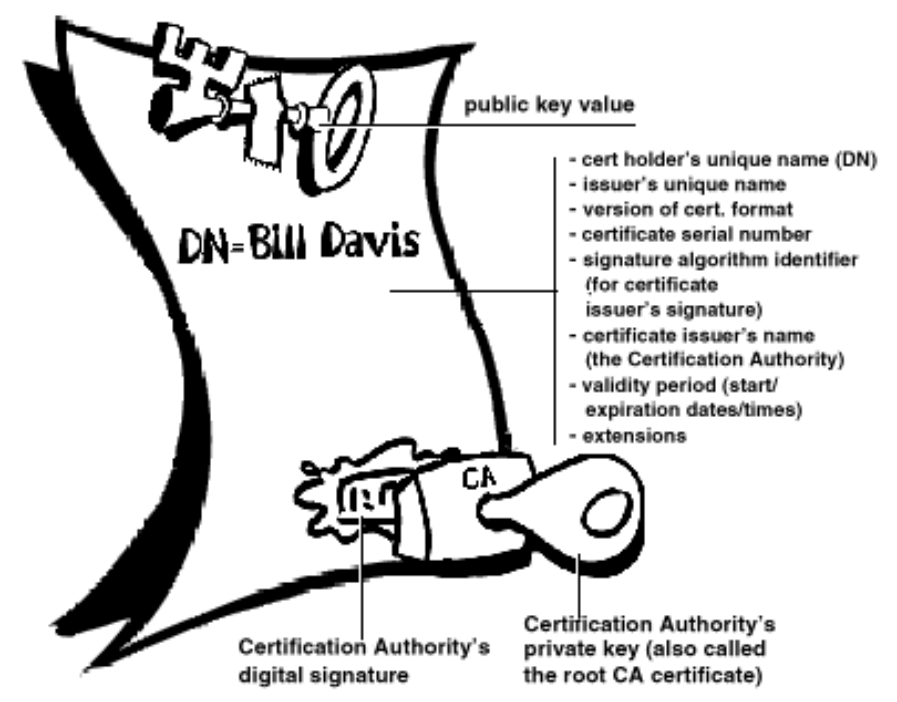
- Sistemas criptográficos assimétricos
  - **PKI – Public Key Infrastructure**
    - Infraestrutura necessária para a gestão do "ciclo de vida" das chaves criptográficas de sistemas assimétricos
      - Geração
      - Distribuição
      - Renovação
      - Revogação
      - etc.
    - Chave Privada = Chave Privada
    - Certificado Digital = Chave Pública
      + Metainformação (Subject, Issuer, Validity, Usage, etc.)



18 NOÇÕES DE CRIPTOGRAFIA

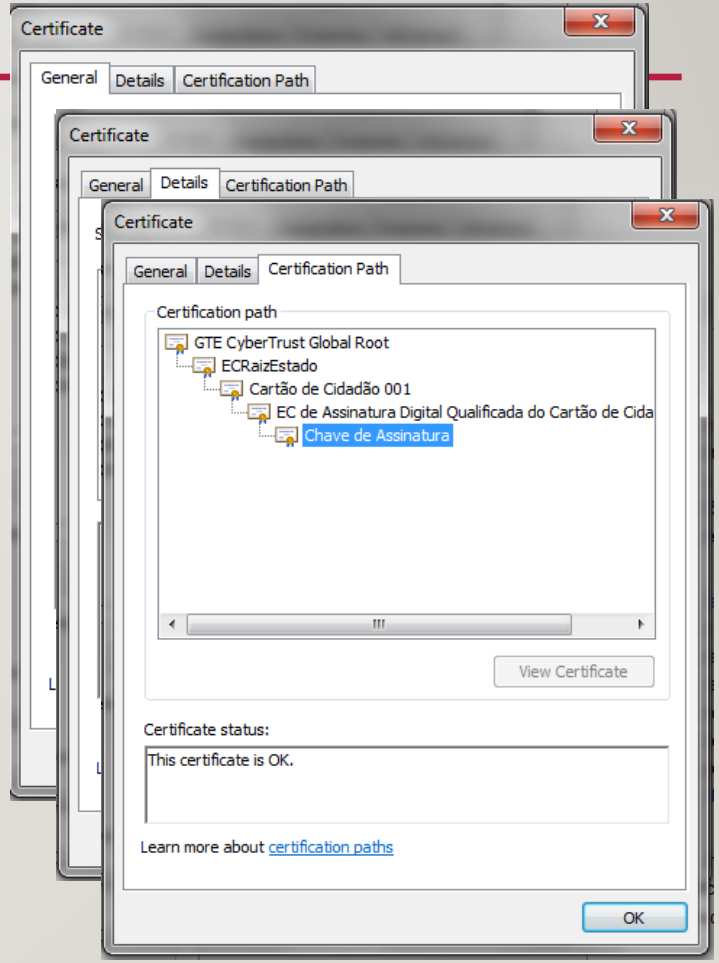
- Digital Certificate:
  - É um documento eletrónico que liga a identidade física de um entidade (pessoa, organização ou computador)

    à sua chave pública
  - Em sistemas seguros (particularmente em PKIs) um certificado digital é emitido para
    - autenticar a(s) parte(s) envolvidas numa transação,
    - assinar eletronicamente documentos assegurando a integridade do seu conteúdo e/ou não repúdio de transações eletrónicas
  - ITU-T X.509 define o formato dos certificados digitais



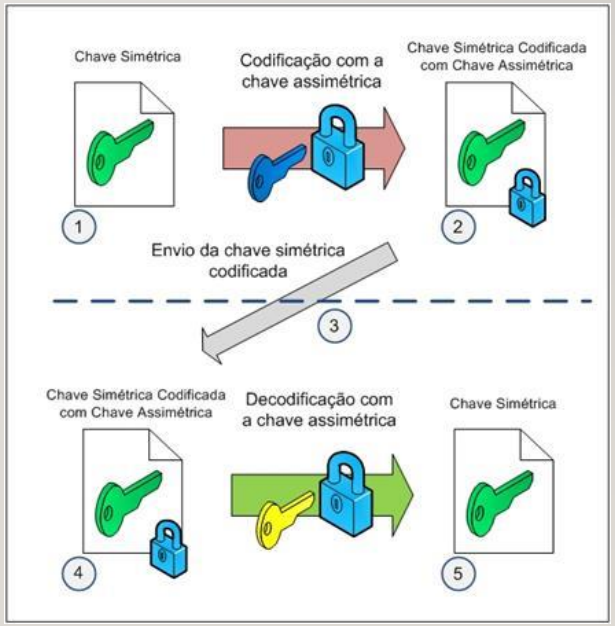
19 NOÇÕES DE CRIPTOGRAFIA

- Sistemas criptográficos assimétricos
  - Standards
    - Certificados Digitais: X509v3
    - Certificate Revocation Lists (CRLs)
    - Certificate Trust Lists (CTLs)
    - Sistemas de Directório: X500 (importante para a definição dos campos 'Subject' e 'Issuer')
  - Outros
    - EMV Certificate: utilizado na área da banca
      - 'more compact than x.509 certificates and are created using the ISO/IEC 9796-2 digital signature algorithm that provides "message recovery" '
    - PGP – Pretty Good Privacy (Philip Zimmermann em 1991)



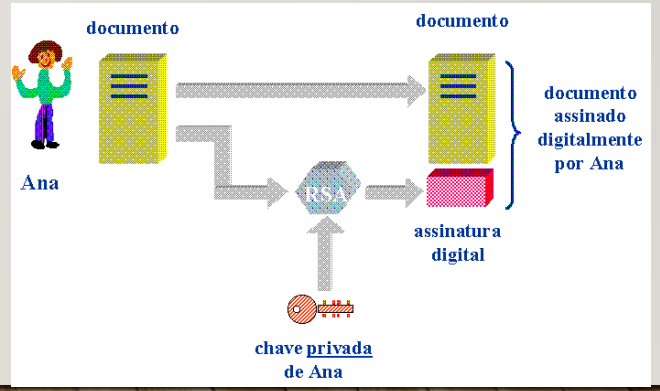
20 NOÇÕES DE CRIPTOGRAFIA

- **A combinação dos dois métodos…**
  - **Codificando-se a mensagem com o método da chave simétrica e trocando a chave simétrica com o método de chave pública.**
    - **Chave de sessão simétrica**
      - **processamento mais rápido**
    - **Partilhada recorrendo a criptografia assimétrica**
      - **mais lenta**
      - **mas mais segura**



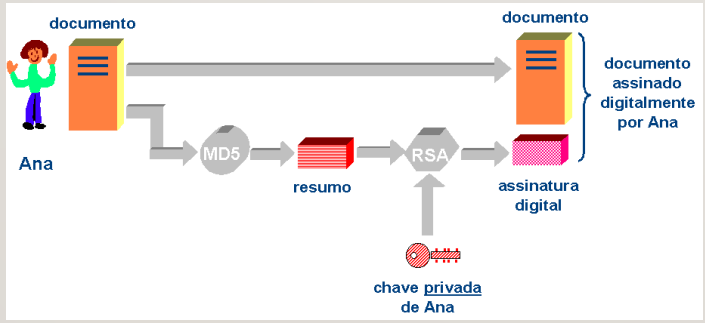
21 NOÇÕES DE CRIPTOGRAFIA

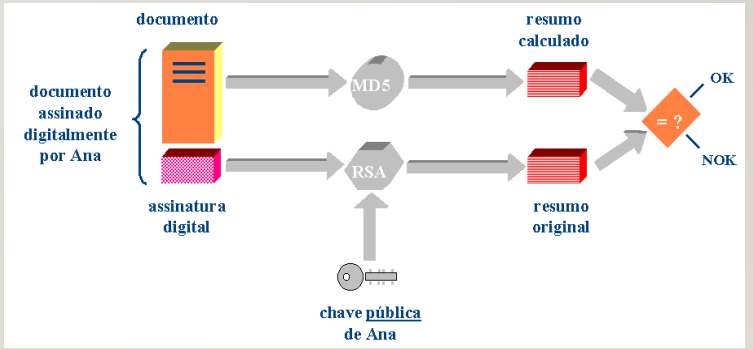
- **A Assinatura Digital**
  - Proporcionado pela criptografia assimétrica
  - que permite garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo
  - No caso de se pretender enviar uma mensagem garantindo a integridade:
    - Mensagem é cifrada na origem com a chave privada
    - Destinatário utiliza a chave pública do emissor, para decifrar a mensagem
    - Fica garantida assim a
      - autenticidade,
      - integridade e
      - não-repudiação da mensagem recebida



22 NOÇÕES DE CRIPTOGRAFIA

- **A Assinatura Digital**
  - Para assegurar o não-repúdio de forma eficiente deverá ser utilizado um Digest (informação resumida do documento)
    - Função Hashing
  - É pouco prático ou inviável em documentos grandes, estar a utilizar a assinatura sobre todo o documento



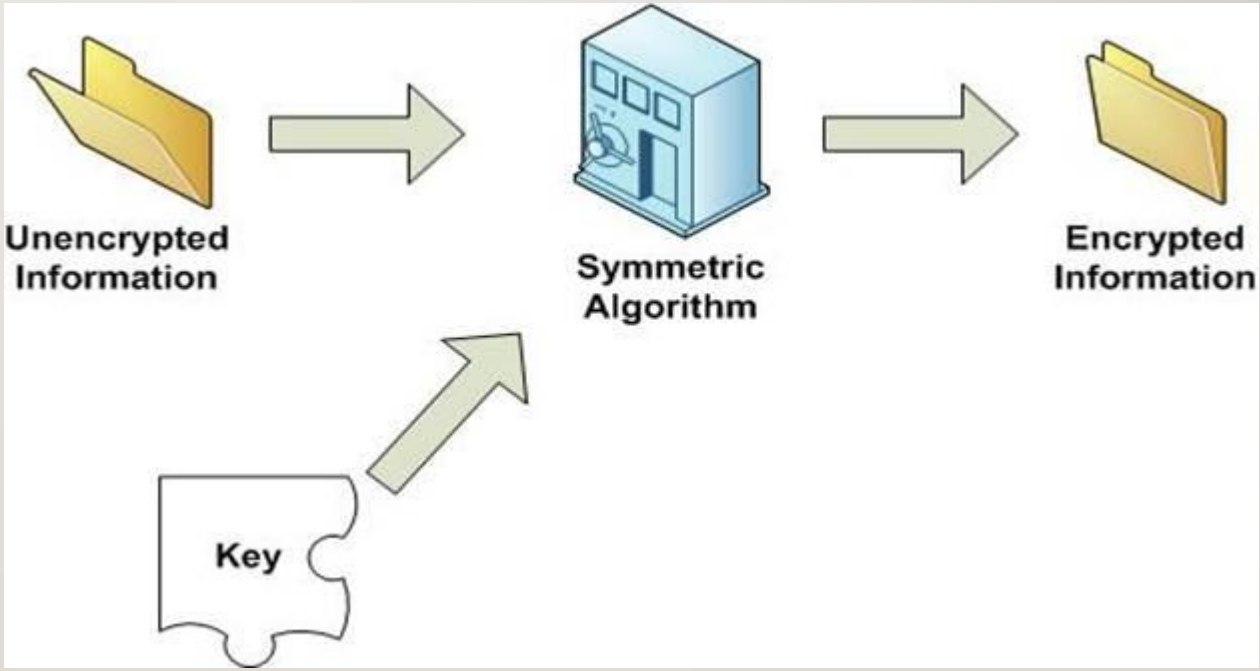


23 AGENDA

- Noções de criptografia
- Gestão de chaves

24 GESTÃO DE CHAVES

- A Cifra requer:
  - os dados a proteger
  - algoritmos de cifra
  - chaves de cifra



25 GESTÃO DE CHAVES

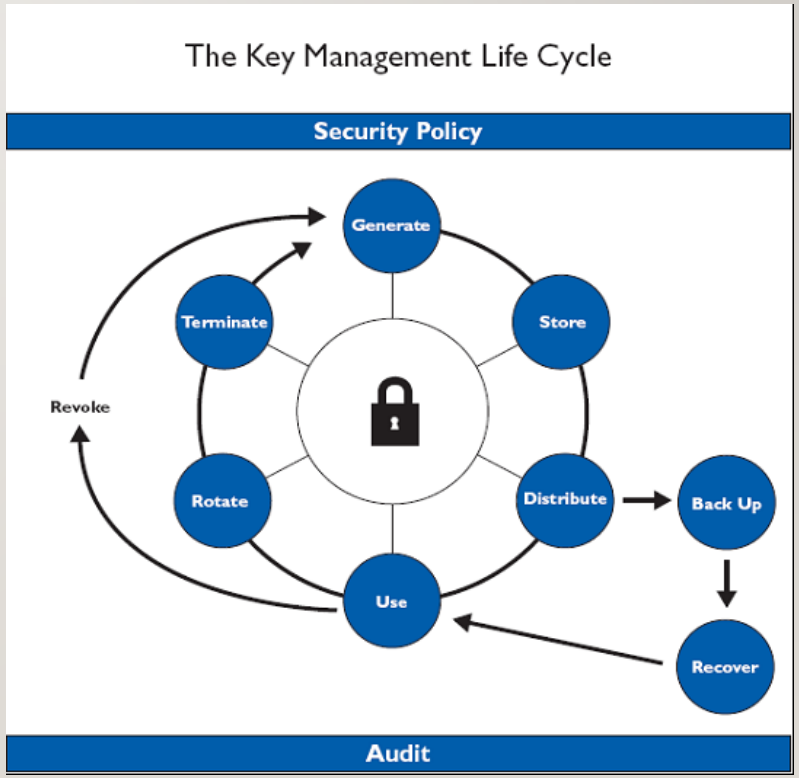
- O processo de cifrar é uma comodidade disponibilizada por um conjunto variado de ferramentas

- Ter em atenção que nenhum algoritmo é inquebrável
  - A questão é quanto tempo leva a quebrar

- **O foco deve ser dado também ao nível da Gestão de chaves**
  - **Uma gestão de chaves fraca pode comprometer processos e algoritmos de cifra robustos**
  - **Dar acesso, apenas, a pessoas autorizadas e de acordo com políticas de aprovação e atribuição**

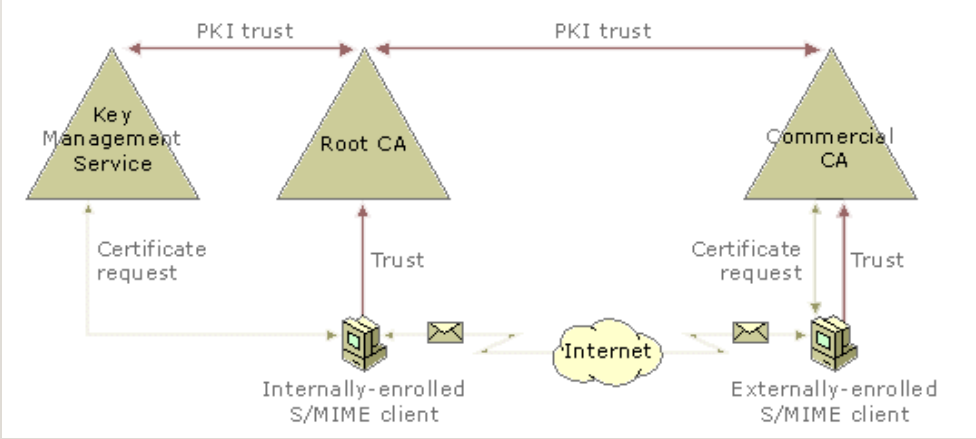
26 GESTÃO DE CHAVES

- Para uma gestão eficaz, é necessário perceber que as **chaves têm um ciclo de vida**:
  - Geração de chaves
  - Armazenamento de chave
  - Distribuição de chave
  - Utilização da chave
  - Rotação da chave
  - Backup da chave
  - Recuperação de chave
  - Revogação da chave
  - Desactivação da chave
  - Aplicação de políticas
  - Auditorias



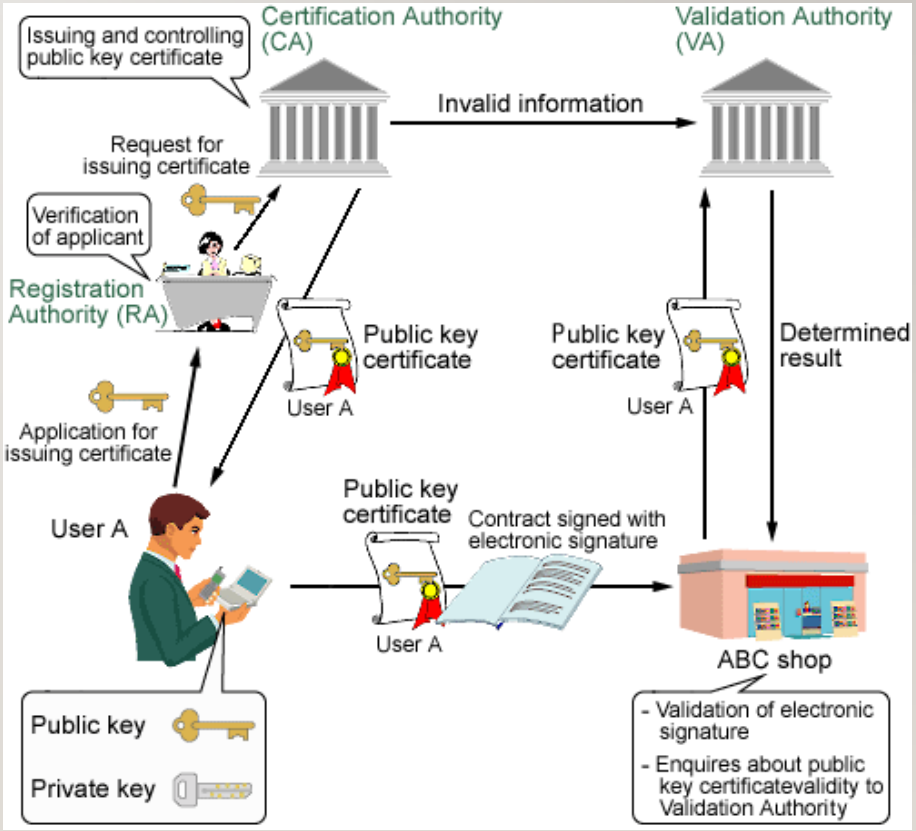
27 GESTÃO DE CHAVES

- O que é a Gestão de chaves
  - É o conjunto de técnicas e procedimentos relacionados com o ciclo de vida das chaves criptográficas
  - Mas também das relações entre as entidades emissoras
  - Mantendo as chaves e essas relações em segurança



28 GESTÃO DE CHAVES - PKI

- **Public Key Infrastructure (PKI)**
  - Certificate Authority (CA)
    - CA é uma organização que emite certificados utilizando uma assinatura digital, que vincula um certificado digital à identidade de uma entidade
  - Registration Authority (RA):
    - RA autentica a identidade das entidades e requer à CA a emissão do certificado para cada uma desssa entidades
    - Hierarquicamente, a RA opera na dependência da CA e atua como interface da CA para com o utilizador ou entidade requerente
  - Validation Authority (VA):
    - VA pode fazer parte do serviço fornecido pela CA ou por um terceiro.
    - Valida os certificados digitais, emite comprovativos digitais e serviços confiáveis de reconhecimento como prova de que uma transação eletrónica ocorreu



29 GESTÃO DE CHAVES - PKI

- Registration service: (RA)
  - Verifica Identidade e atributos especícicos da entidade (pessoa ou empresa). Resultados passados para "certificate generation service"
- Certificate generation service: (CA)
  - Cria e assinacertificados baseados na identidade e atributos verificados pelo "registration service".
- Dissemination service: (CA)
  - Dissemina os certificados aos requerente, e, se consentido por este, divulga para terceiras partes
  - Também é responsável por disseminar os termos e condições da CA, e as políticas e práticas de certificação
- Revocation management service: (CA)
  - Processa os pedidos e relatórios referentes à revogação, para determinar as medidas a serem tomadas.
  - Resultados distribuídos através do revocation status service.
- Revocation status service: (CA)
  - Providencia a informação do estado de revogação de certificados
  - Pode ser um serviço em tempo-real, ou ser baseado em informação que é publicada periodicamente
- Subject device provision service: (opcional - RA)
  - Disponibiliza um dispositivo de criação de assinatura
  - Exemplos de utilização:
  - Um serviço que gera o par de chaves e entrega a chave privada à entidade requerente;
  - Um serviço que prepara o subject's secure-signature-creation device (SSCD) e o entrega à entidade

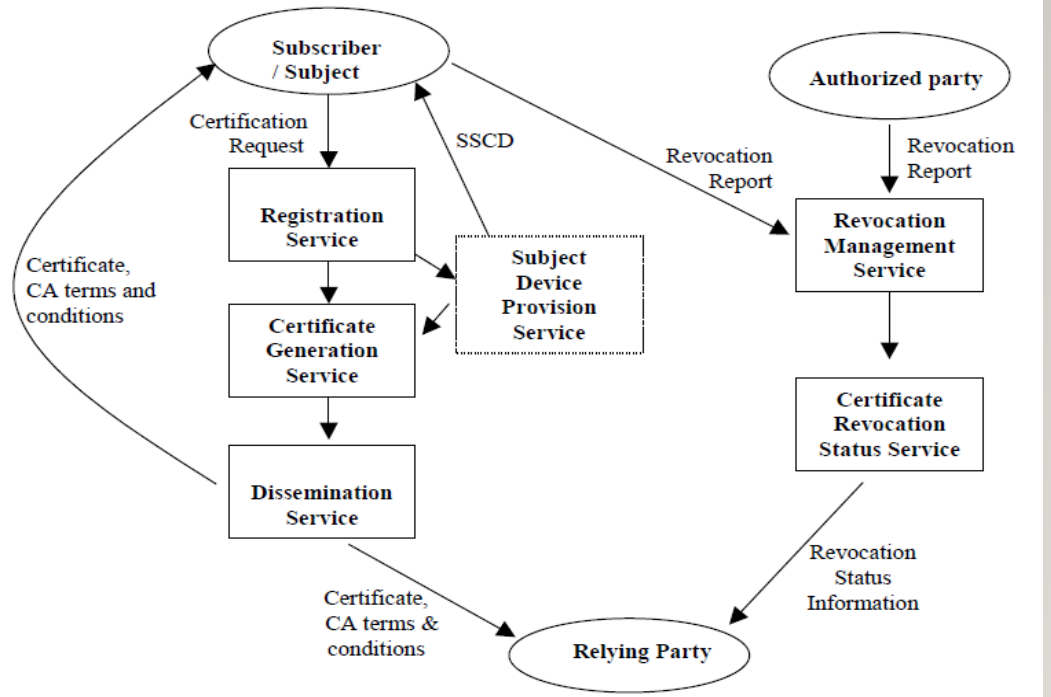
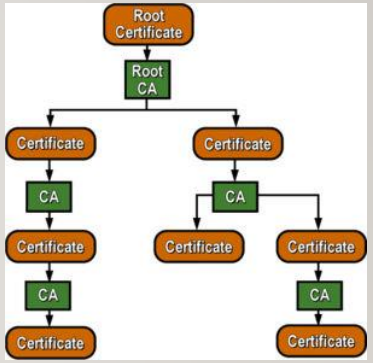


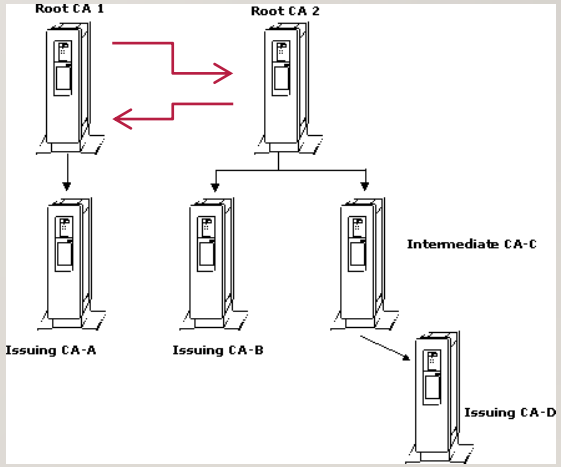
Figure 1: Illustration of subdivision of certification services used in the present document

30 GESTÃO DE CHAVES - PKI

- Relações de confiança entre CAs
  - Existe um modelo hierárquico que estabelece as relações de confiança entre CAs diferentes, dentro da hierarquia de confiança mesmo.



  - No entanto, se os seus CAs não compartilham de uma raiz comum CA, deve ser realizada uma certificação cruzada
  - As CAs raiz devem desenvolver relações de confiança bilateral.
    - Constituindo um modelo híbrido de relações de confiança



31 GESTÃO DE CHAVES - PKI

- Alguns referenciais
  - CEN - CWA 14167
    - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
      - Part 1: System Security Requirements
      - Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
  - European Telecommunications Standards Institute (ETSI)
    - ETSI TS 101456 - Electronic Signatures and Infrastructures (ESI);.
      - Policy requirements for certification authorities issuing qualified certificates
      - Baseado no IETF RFC 3647 - Internet X.509 Public Key Infrastructure
        - Para maior detalhe consultar o RFC 3647
    - ETSI TS 102 176 - Algorithms and Parameters for Secure Electronic Signatures
      - Part 1: Hash functions and asymmetric algorithms
      - Part 2: Secure channel protocols and algorithms for signature creation devices
    - ETSI TS 101 861 - Time stamping profile
  - Federal Information Processing Standard (FIPS), do NIST
    - FIPS 140-2 - Security Requirements for Cryptographic Modules

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2020/21

CRIPTPGRAFIA E GESTÃO DE CHAVES

LUIS AMORIM

17 Abr 2021