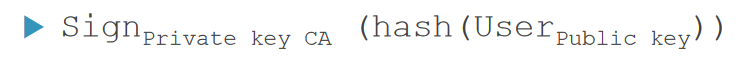
Teórica – Prova 2

# Certificados digitais

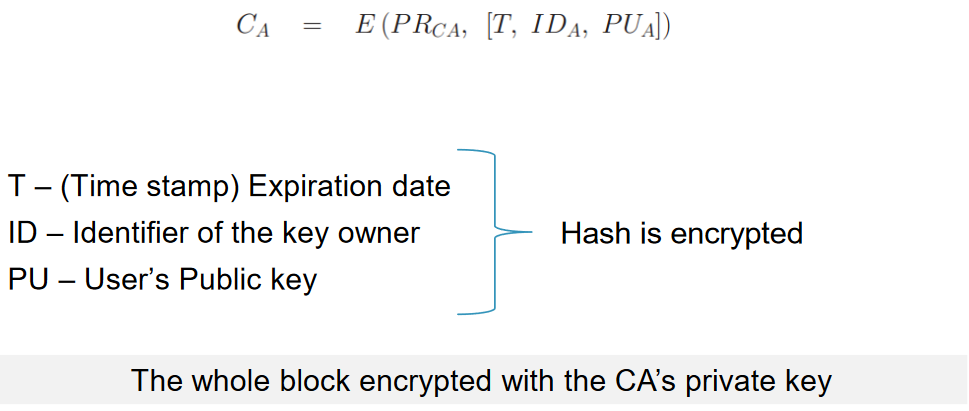
Um certificado enviado por uma **Autoridade de Certificados** (CA), autêntica a tua **chave pública**. Simplificando, um certificado é a tua chave pública assinada por uma chave privada de uma CA

**Mecanismo de atestado:**



🡪 Para verificar utilizamos a chave pública da CA certificada.

**Dados mínimos assinados pela CA**

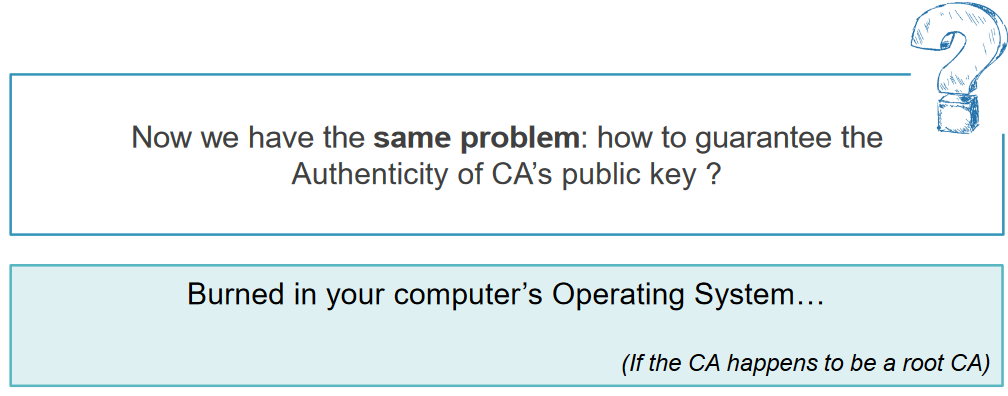


**Outros dados que são assinados por uma CA**

* Chave pública do dono
* Números de série
* Organização que enviou o certificado e a sua assinatura

**Verificação de certificados**

Fazemo-lo ao decifrar o certificado com a chave pública da CA



Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

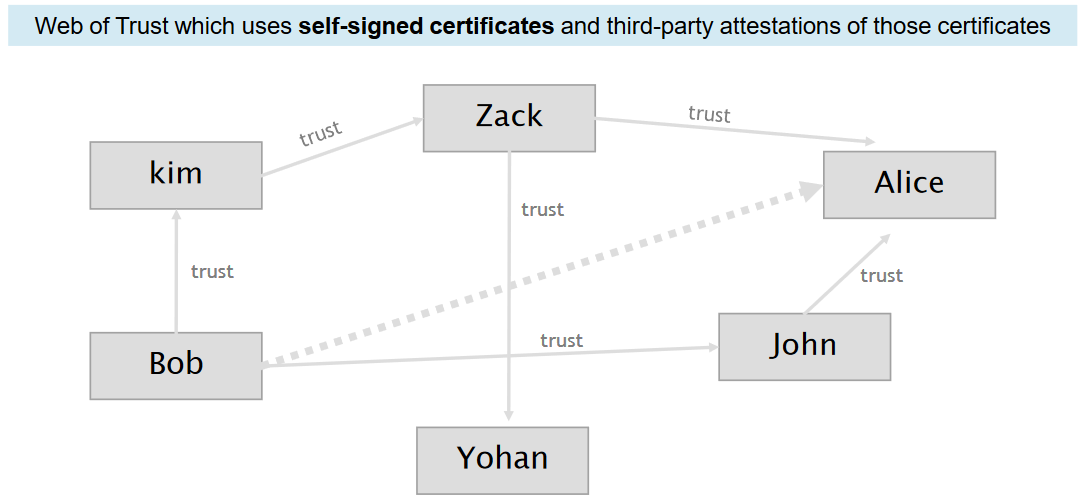
**Outras maneiras de confiar**

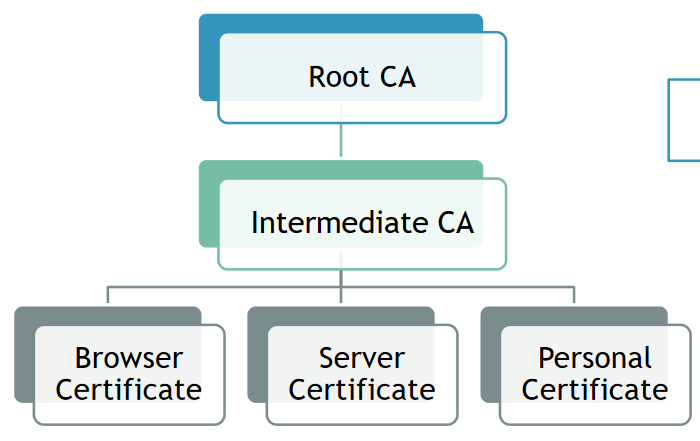
Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto, interior, captura de ecrã

Descrição gerada automaticamente





Outro acrónimo que está relacionado com a CA é **RA (Registration Autority)**

* Funcionam como revendedores de um certificado pelas CA
* Não devem ser confundidos como CA de nível intermédio

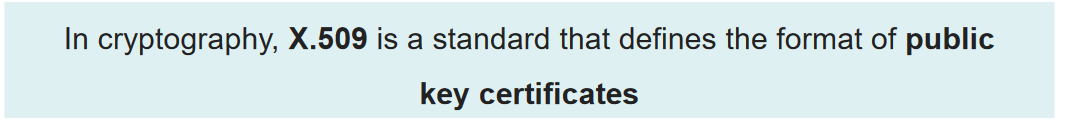
Uma **CA de nível intermédio** é apenas a CA que não é a root, apenas assina por baixo o seu certificado

# Certificados X.509

O padrão de formato de **certificado X.509** para a **chave pública de infraestruturas (PKI)**

Uma imagem com texto

Descrição gerada automaticamente



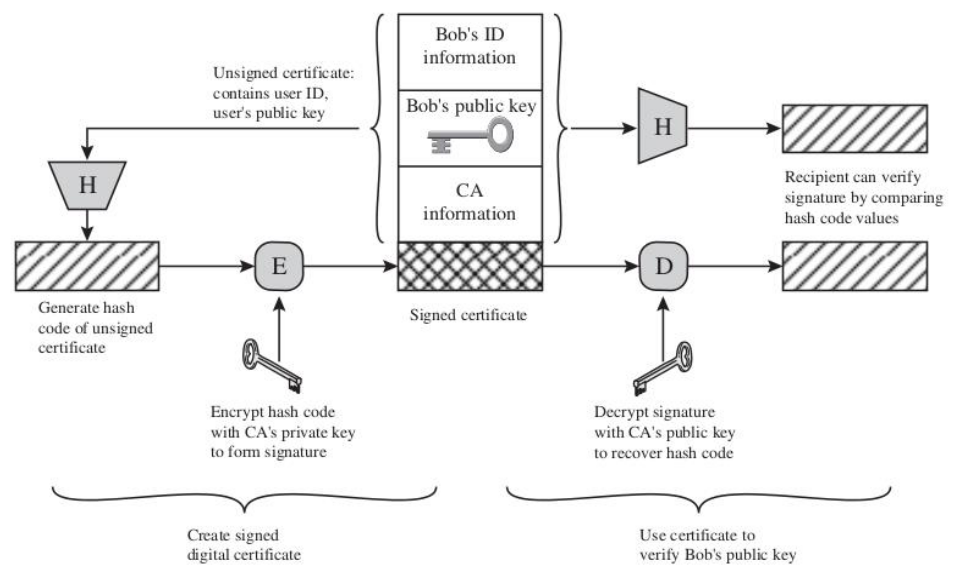
Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

* O X.509 define uma framework para a prestação de serviços de autenticação pela diretoria X.500 para os seus users
* A diretoria pode servir como **repositório de certificados de chaves públicas**
* O certificado **contém** a **chave pública do user e também é assinado pela CA confiada**.



Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto, interior, captura de ecrã

Descrição gerada automaticamente

Uma imagem com texto, interior, captura de ecrã

Descrição gerada automaticamente

Quantas mais CA o nosso browser confia, mais comprometemos em segurança. Devido a essas razões muita gente critica o modelo das CA

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

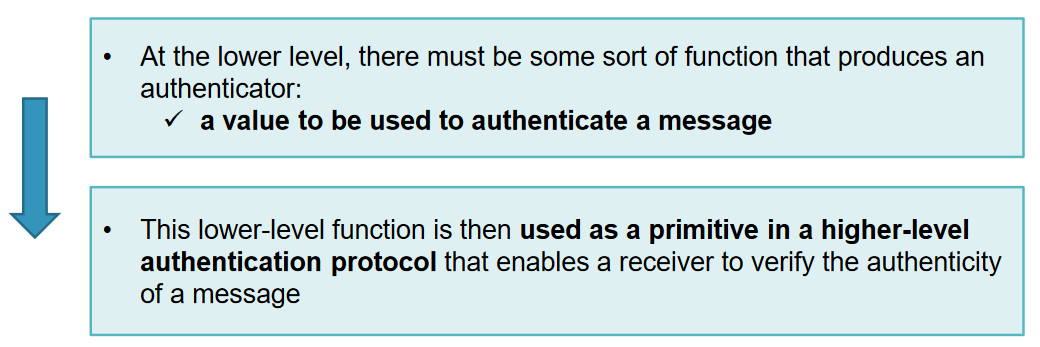
# Assinaturas digitais

Uma imagem com texto

Descrição gerada automaticamente

# Autenticação de Mensagens

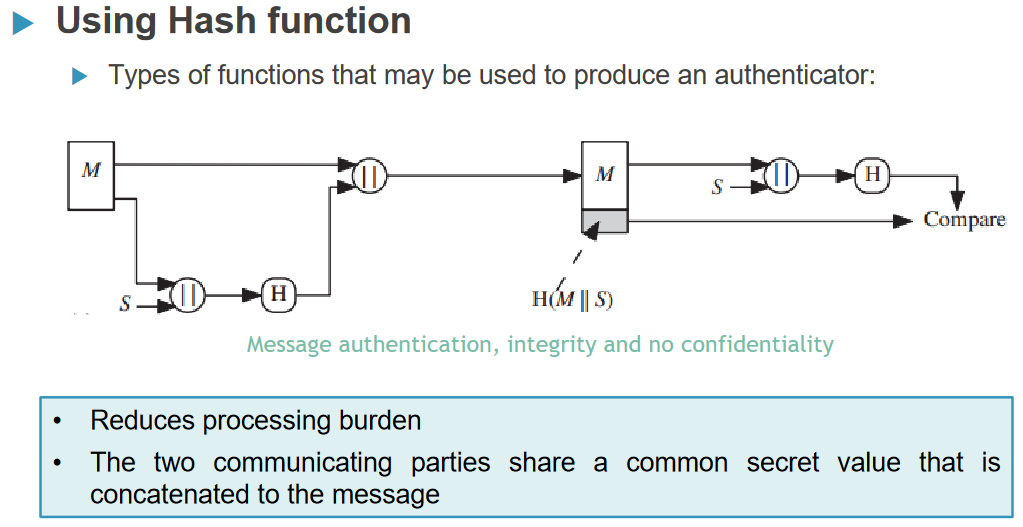
Autenticação de mensagem ou assinatura digital tem dois níveis de funcionalidade

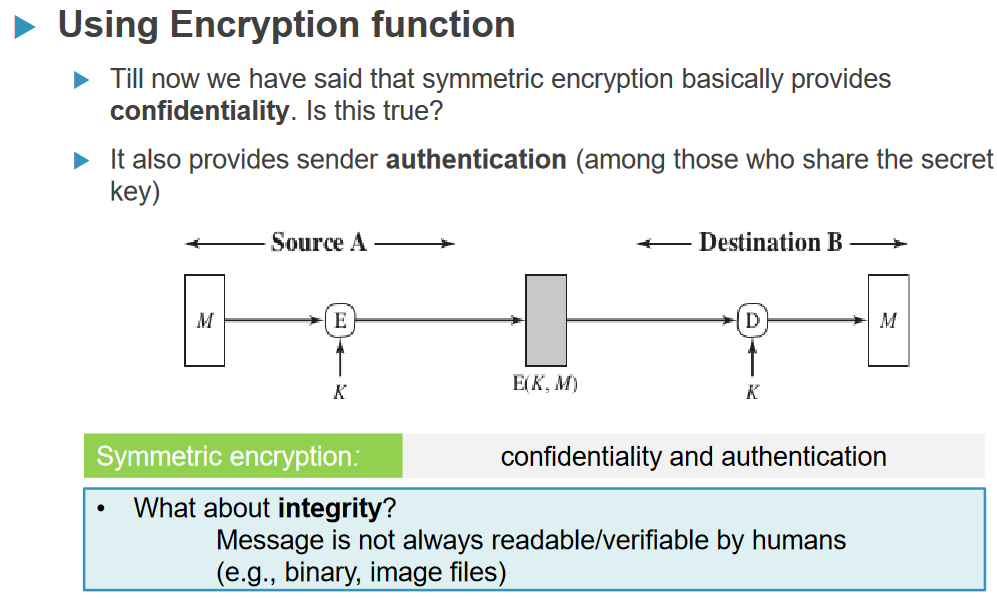


Tipos de funções que podem ser utilizadas para produzir autenticadores

Uma imagem com texto

Descrição gerada automaticamente





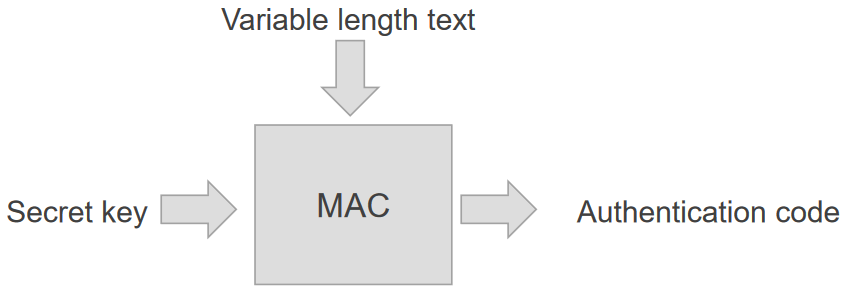
**Códigos de autenticação de mensagens (MAC)**

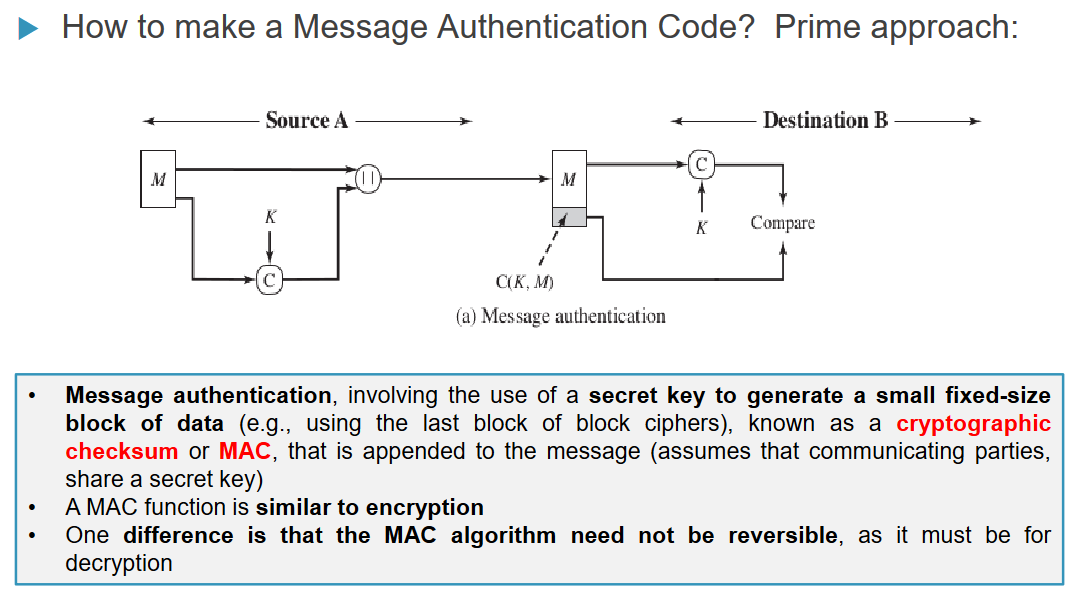
Algoritmo MAC é um algoritmo simétrico de criptografia que providencia autenticação de mensagem

Para utilizar o MAC, o remetente e destinatário partilham a mesma chave simétrica.

Uma imagem com texto

Descrição gerada automaticamente



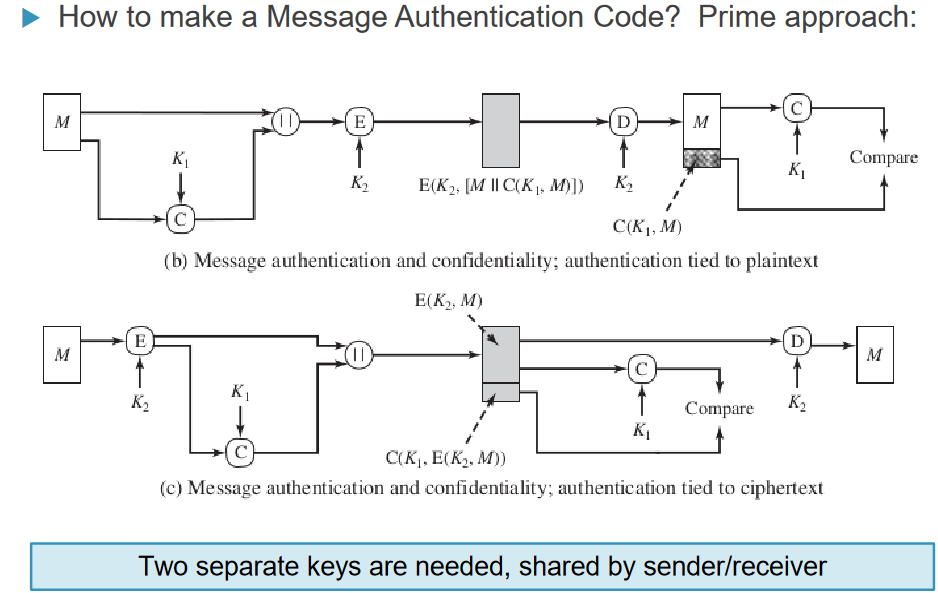


A principal diferença entre uma hash e o algoritmo MAC é que o MAC usa a chave secreta durante a compressão

Se quisermos usar confidencialidade, temos de encriptar a mensagem.

Uma imagem com texto

Descrição gerada automaticamente



**As limitações do MAC**

Estão apenas associadas a natureza da parte simétrica

Uma imagem com texto

Descrição gerada automaticamenteUma imagem com texto

Descrição gerada automaticamente

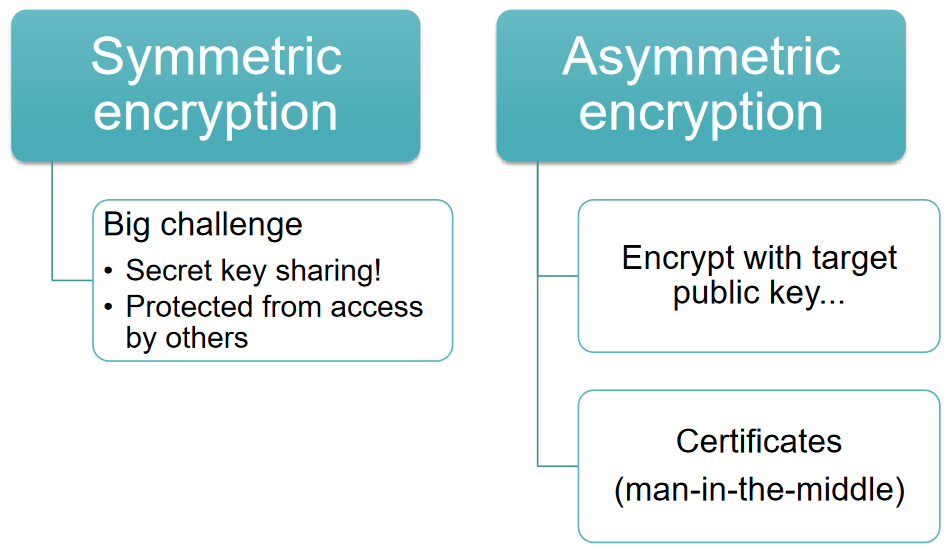
Ambas estas limitações, podem ser ultrapassadas utilizando uma **assinatura digital**

# (Confiança Mútua) - Gerenciamento e Distribuição de Chaves

Uma imagem com texto

Descrição gerada automaticamente

O ponto forte que qualquer sistema de criptografia, está na técnica de distribuição das chaves.



Uma imagem com texto

Descrição gerada automaticamente

Modos de distribuição de chaves:

Uma imagem com texto

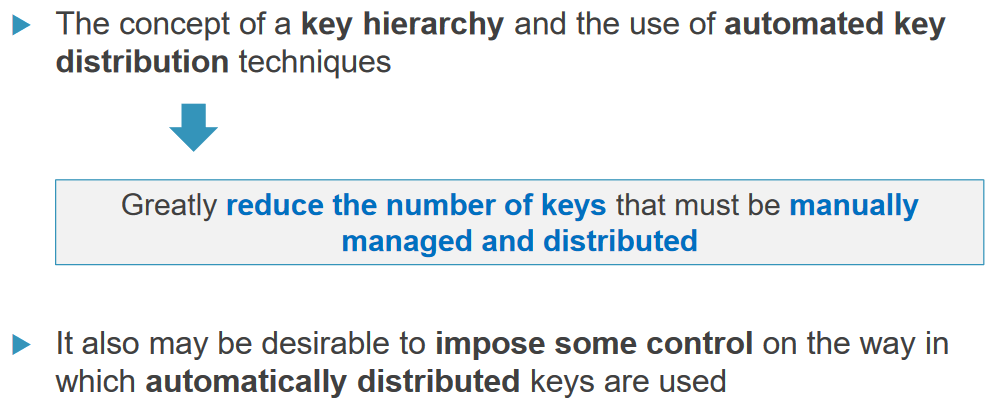
Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

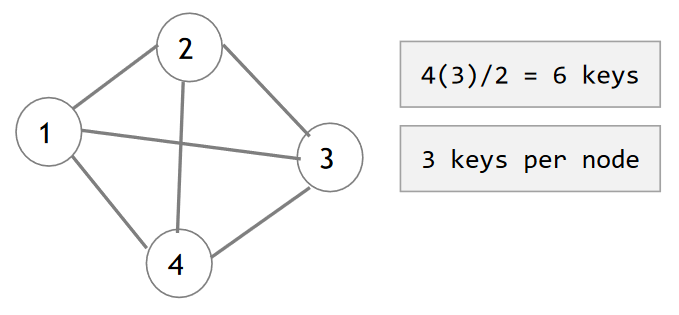


Uma imagem com texto, captura de ecrã, interior

Descrição gerada automaticamente

Uma imagem com texto

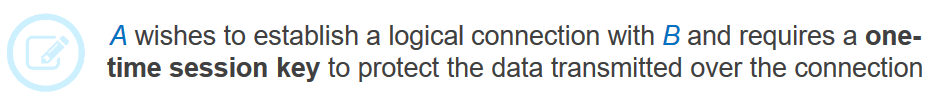
Descrição gerada automaticamente



Uma imagem com texto

Descrição gerada automaticamente

# KDC (Centros de Distribuição de Chaves)



Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto, captura de ecrã, símbolo

Descrição gerada automaticamente

Uma imagem com texto

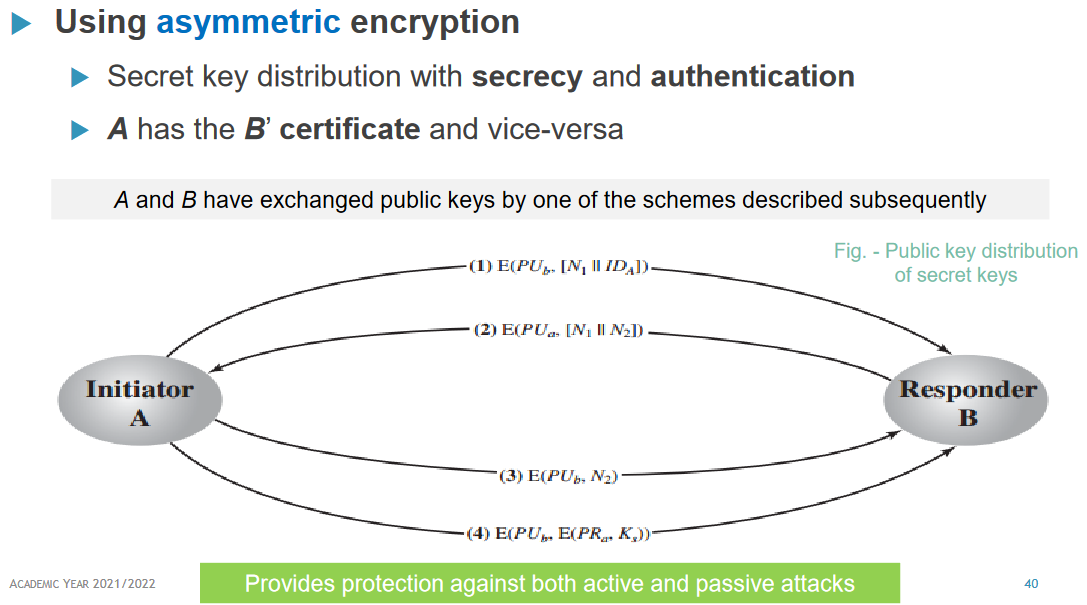
Descrição gerada automaticamente

Uma imagem com texto

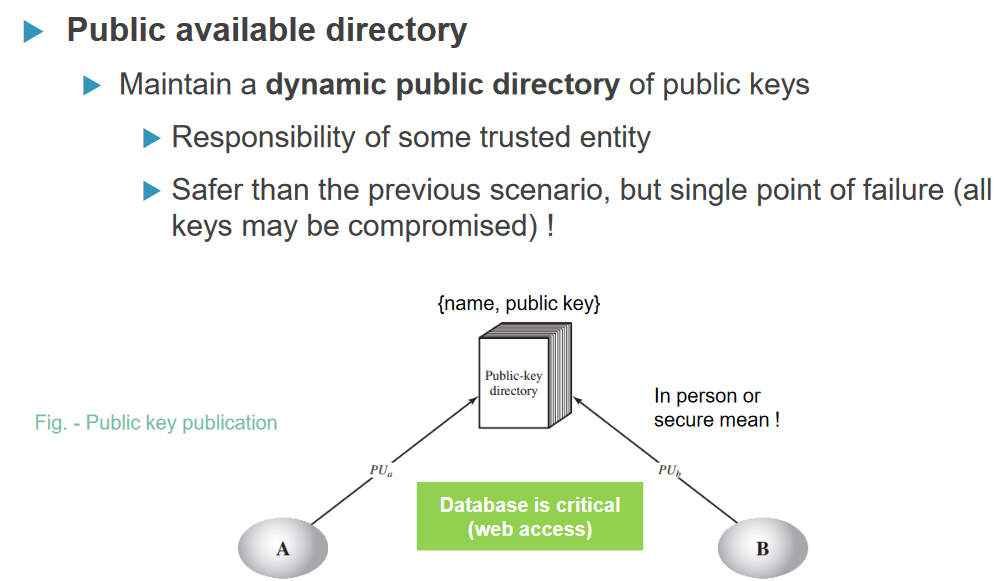
Descrição gerada automaticamente

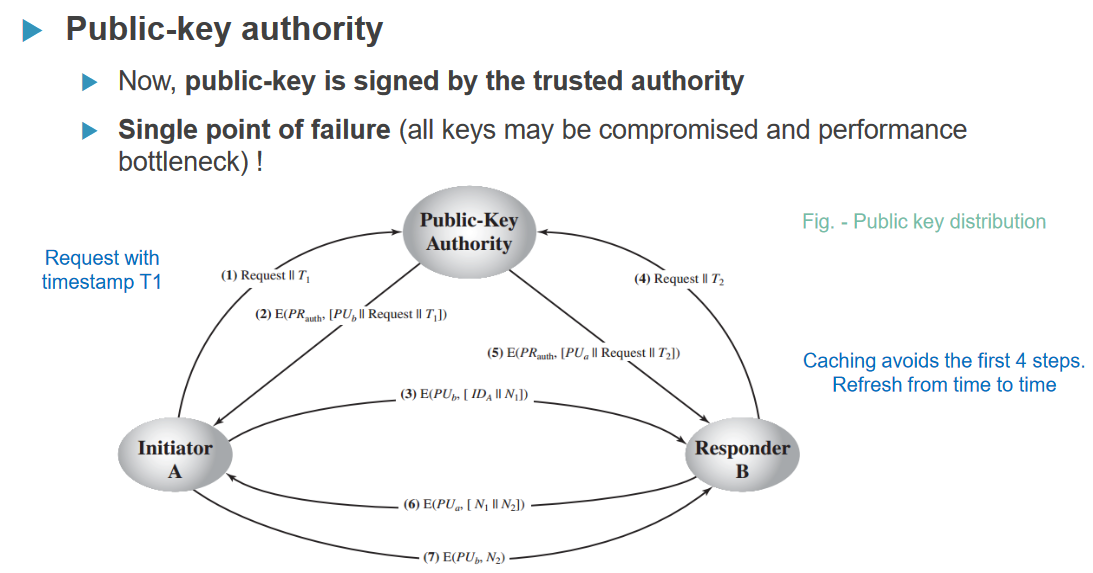
Uma imagem com texto

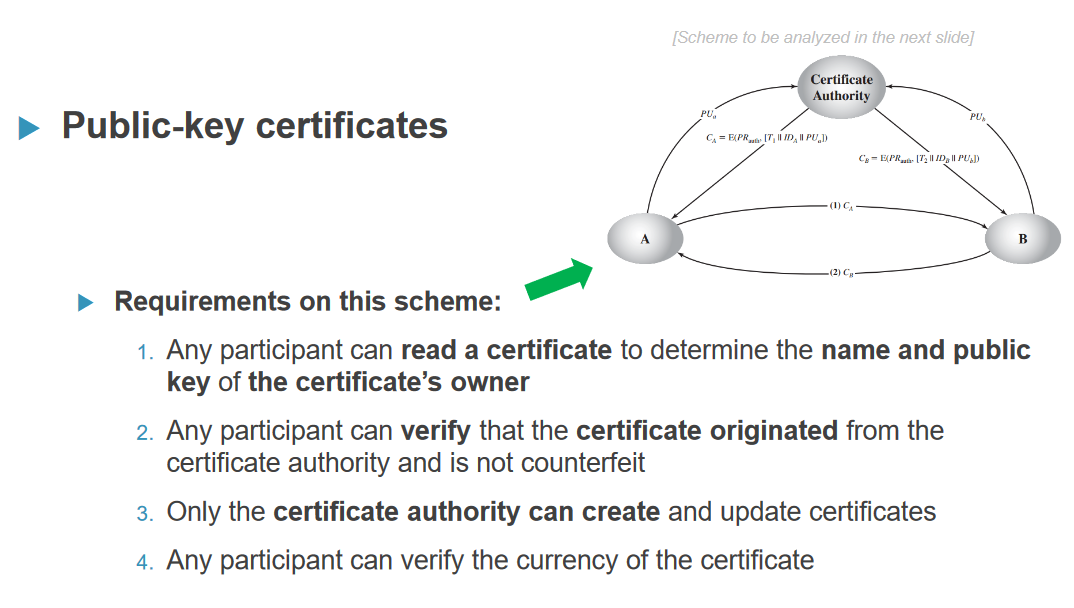
Descrição gerada automaticamente



# Distribuição de chaves públicas







Uma imagem com texto

Descrição gerada automaticamente

# Cyber segurança

Uma imagem com texto

Descrição gerada automaticamente

**Prevenir**

* Medidas de segurança devem ser tomadas para proteger a informação
* Durante a fase de prevenção
  + Políticas de segurança
  + Controlos (físicos, técnicos, legais, etc.)
  + Processos devem de ser desenhados e implementados
* Proteger de:
  + Desastres naturais, fogos, terramotos…
  + Acidentes
  + Erros
  + Mau funcionamento
  + Ataques

**Deteção**

* A deteção de um sistema que está comprometido é extremamente crítico
* Uma defesa em layers deve de ser implementada
  + Para sempre que um layer seja comprometido, avisa logo o a seguir e faz suar um alarme de aviso
* O elemento mais importante desta estratégia é deteção a tempo e notificação do compromisso

Uma imagem com texto

Descrição gerada automaticamente

Hacker 🡪 Geek que explora a vulnerabilidades do sistema, White Hacker

Cracker 🡪 Usa as vulnerabilidades do sistema como sua vantagem para fazer dinheiro, Black Hacker

A maioria dos hackers são, Gray Hackers

**Motivos dos ataques**

* De dentro da empresa
* Intencional
* Acidental
* Erros

Uma imagem com mesa

Descrição gerada automaticamente

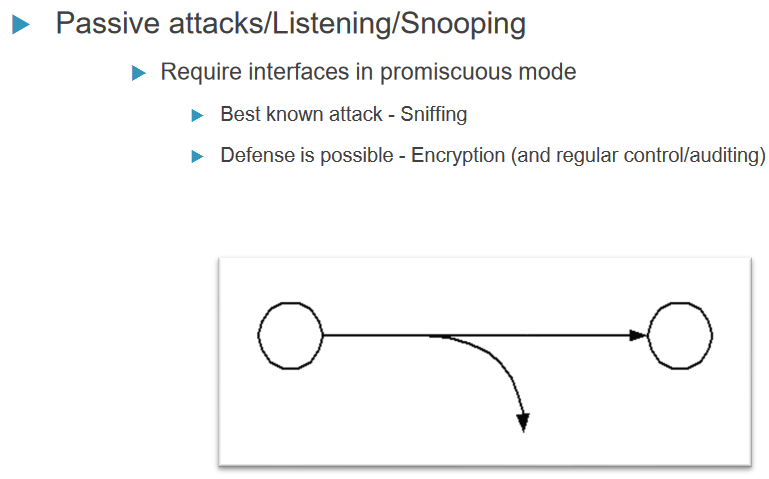
Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

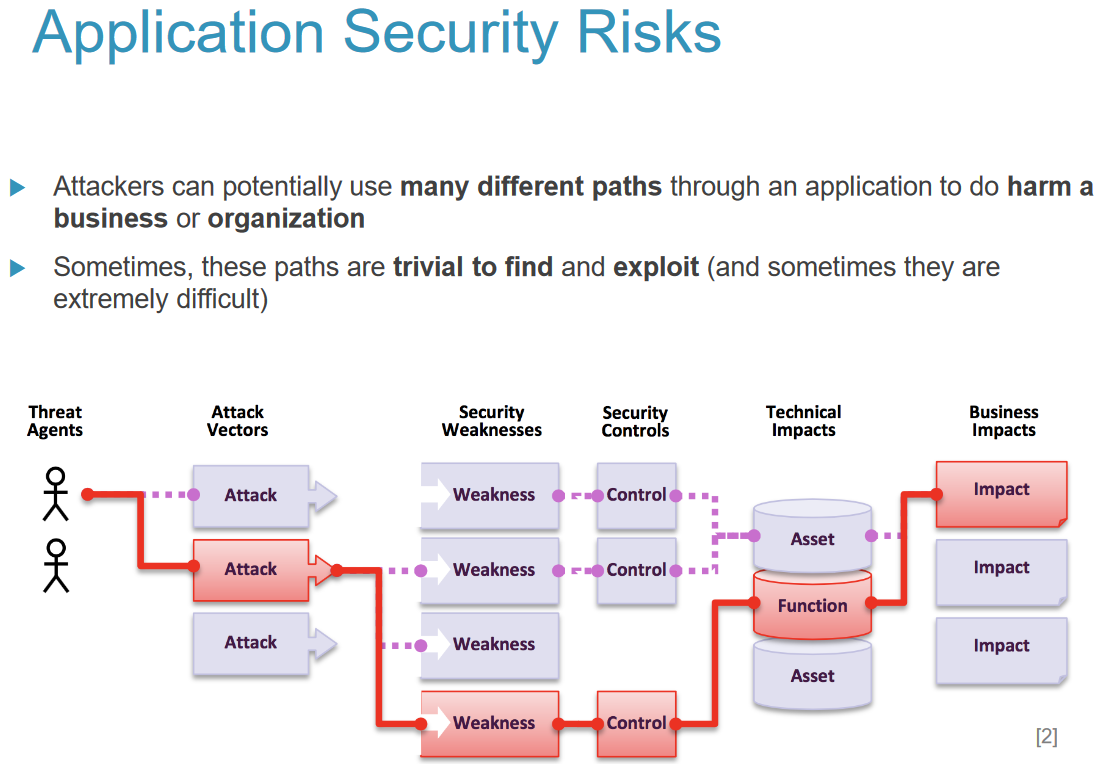
Uma imagem com texto

Descrição gerada automaticamente

**Ataques ativos**

* Ataques na HW/SW (cortar os cabos de rede ou energia, tudo o que for ativo e no momento)
* Bombardear o email
* SYN Flood, para fazer o request denial
* Spoofing, do endereço IP
* Vírus
* Software malicioso
* DoS

# Vulnerabilidade



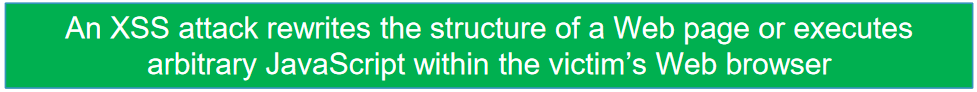
* Ataques de vetores, dão a oportunidade de hackers encontrarem vulnerabilidades no sistema

# SQL Injection

* Cracker pode apagar todos os dados dos utilizadores ou mesmo, ter acesso a todos os dados dos utilizadores

# Cross-site scripting (XSS) ataque

* Conteúdo que um website pode correr HTML ou JS sem o utilizador saber



Uma imagem com texto, interior, captura de ecrã

Descrição gerada automaticamente

* O cracker consegue inserir JS dentro de uma textbox, que depois vai afetar o cliente

# Cross-Site Request Forgery (CRSF) attack

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente