UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança da Informação I
# Quinta Aula

Prof. Frederico Sauer, D.Sc.

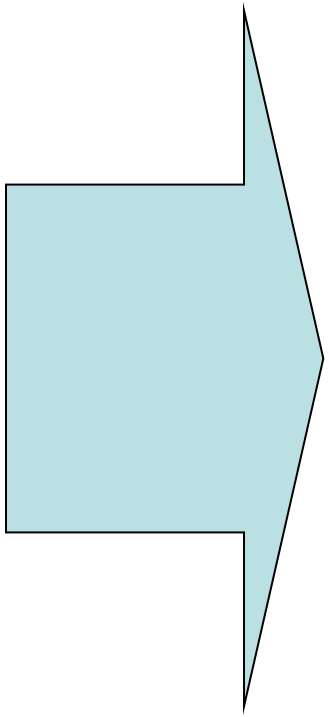
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Autenticação de Mensagens e Algoritmos de Hash

- Mecanismos de Autenticação
  - Integridade da Mensagem
  - Identificação da Autoria da Mensagem
  - Não-repudiação
- Mecanismos
  - Encriptação da Mensagem
  - Message Authentication Code (MAC)
  - Funções de Hash

# Ataques Possíveis

- *Disclosure*
- *Traffic analysis*
- *Masquerade*
- *Content modification*
- *Sequence modification*
- *Timing modification*
- *Source repudiation*
- *Destination repudiation*



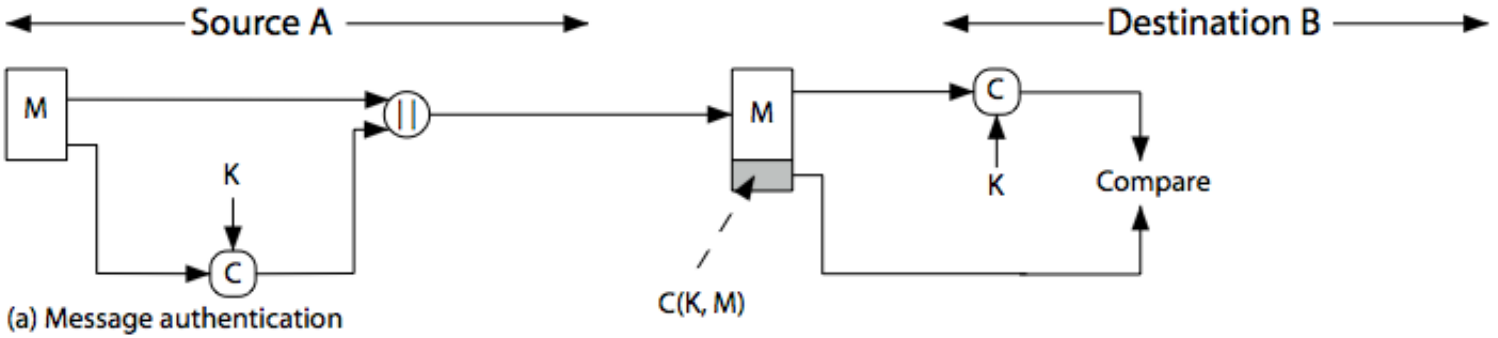
**Combatidos pela Autenticação**

# Encriptação da Mensagem

- Simétrica
  - Requisito de segredo da chave garante autoria e anonimicidade
  - Alterações em trânsito comprometem o criptograma
- Assimétrica
  - Não protege a identidade do autor
    - Pode-se combinar chaves pública e privada para anonimicidade
  - Maior custo computacional

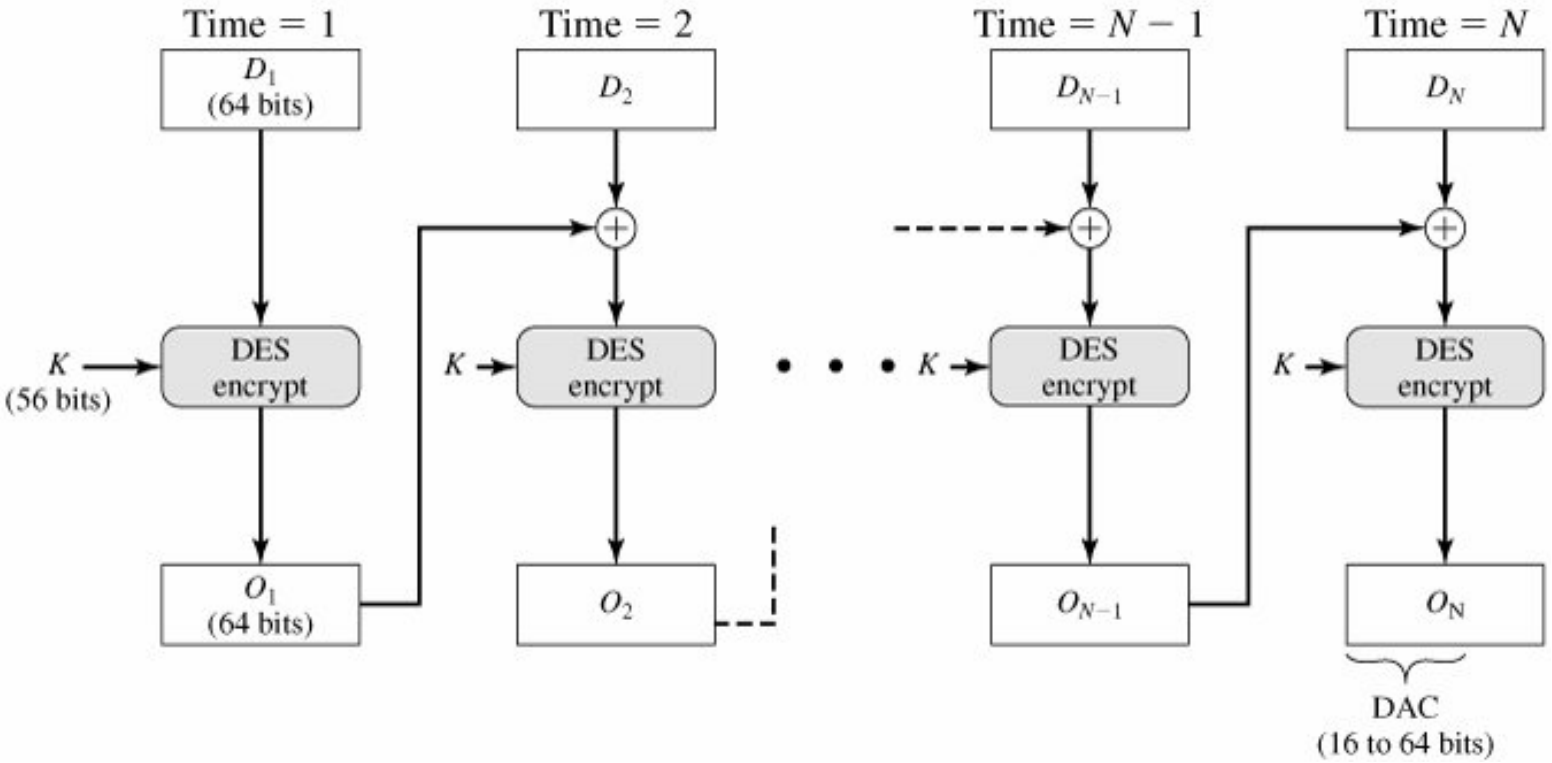
# MAC

- Bloco de tamanho fixo é criado em função do arquivo de entrada e uma chave
- É impossível obter o texto original apenas do MAC
- É concatenado à mensagem
- No destino o receptor calcula o MAC e compara com o recebido



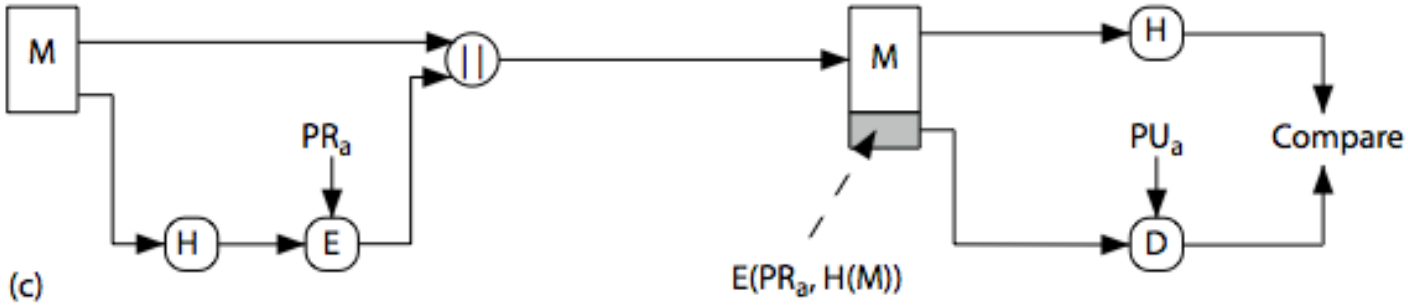
# Cômputo do MAC

- Pode-se usar o CBC → o bloco final é o MAC
- DAA (*Data Authentication Algorithm*) → DES-CBC



# Funções de Hash

- Mesmo princípio que o MAC, sem chaves
- Pode ser usado para criar assinaturas digitais com criptografia assimétrica
- Tipicamente implementado com XOR para maior rapidez



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Robustez

- Há vários ataques conhecidos
- Evidencia a necessidade de aumentar os blocos e uso de chaves
- MD5 é exemplo de fragilidade

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# SHA – Secure Hash Algorithm

- Projetado pelo NIST/NSA em 93 e revisado em 95
- Padrão para o DSA

**Table 12.1. Comparison of SHA Parameters**

| | SHA-1 | SHA-256 | SHA-384 | SHA-512 |
|---|---|---|---|---|
| Message digest size | 160 | 256 | 384 | 512 |
| Message size | $<2^{64}$ | $<2^{64}$ | $<2^{128}$ | $<2^{128}$ |
| Block size | 512 | 512 | 1024 | 1024 |
| Word size | 32 | 32 | 64 | 64 |
| Number of steps | 80 | 64 | 80 | 80 |
| Security | 80 | 128 | 192 | 256 |

*Notes:* 1. All sizes are measured in bits.

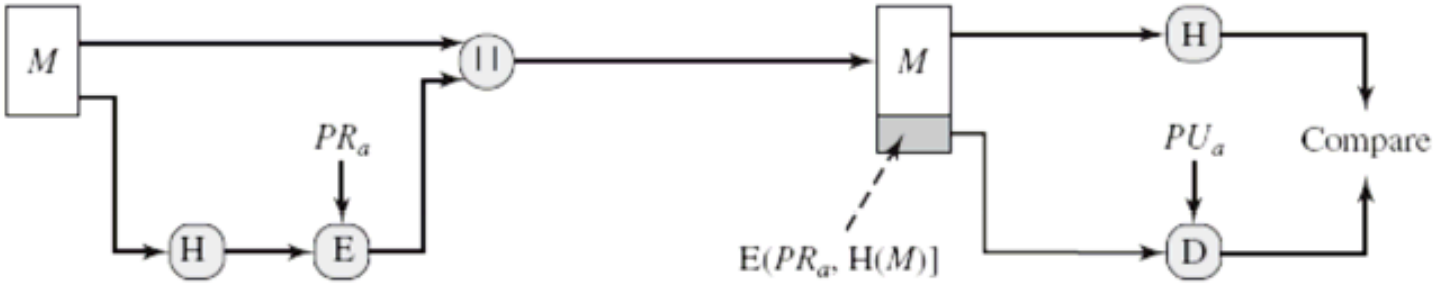
2. Security refers to the fact that a birthday attack on a message digest of size *n* produces a collision with a workfactor of approximately $2^{n/2}$

# Assinaturas Digitais

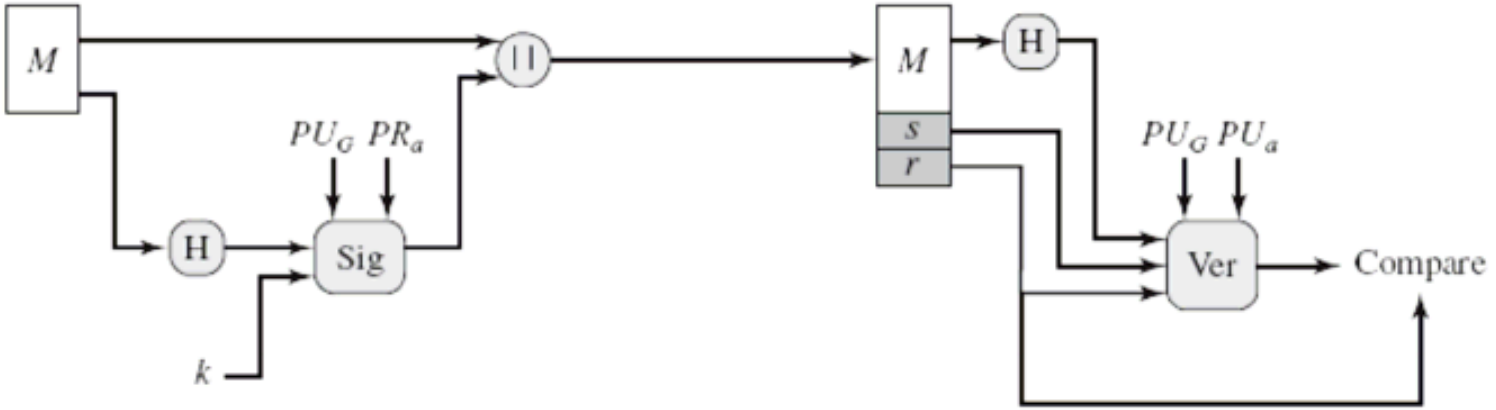
- Requisitos de Confiança transcendem os mecanismos MAC e HASH
  - Verificação de autoria, data e hora da assinatura da mensagem
  - Autenticar o conteúdo da Mensagem
  - Poder ser verificado por terceiros para conflitos de autoria
  - Ser robusto aos ataques por replay

# DSS – Digital Signature Standard

- Usa o algoritmo DSA




(a) Técnica do RSA




(b) Técnica do DSS

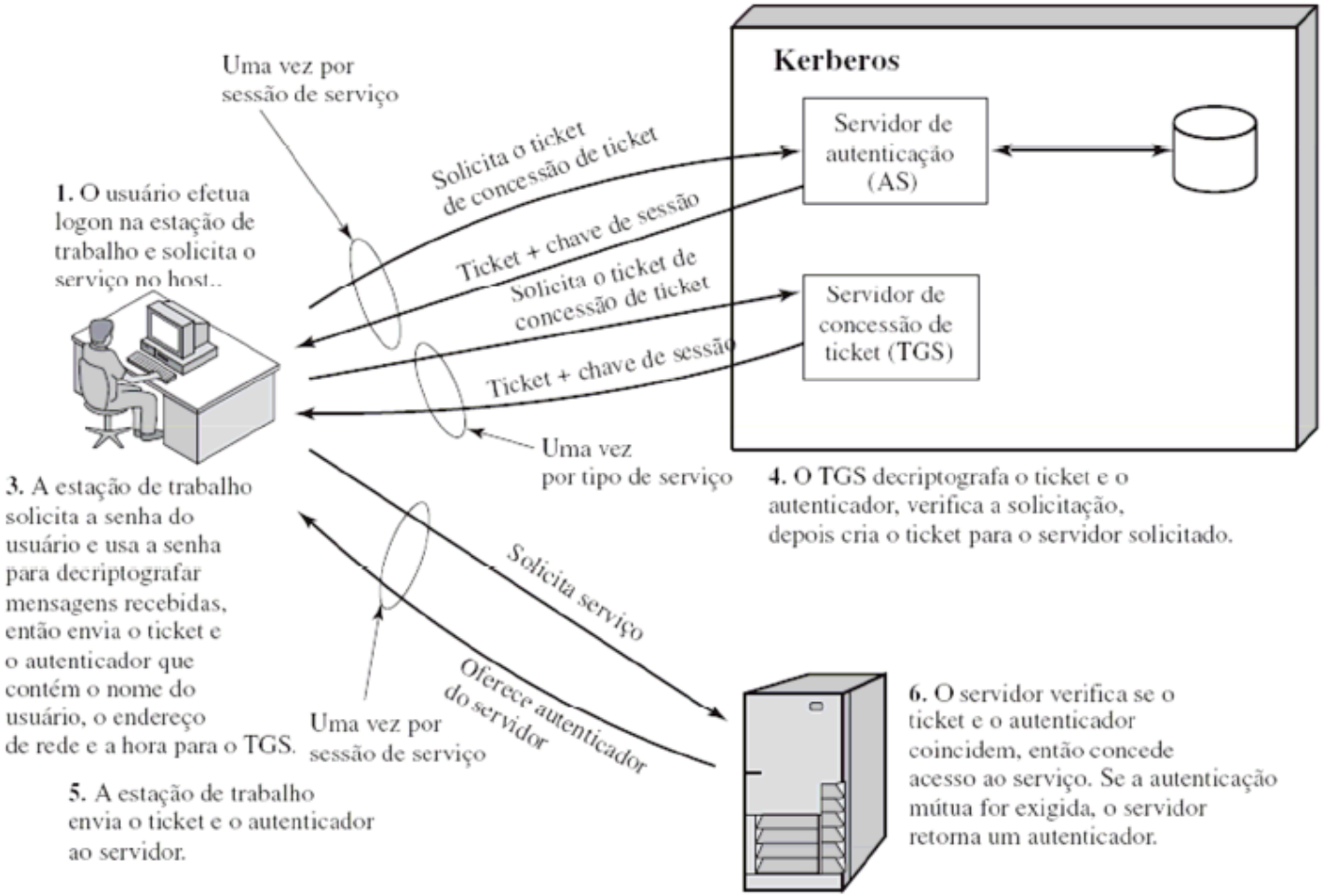
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Kerberos e PKI

- Aplicações para autenticação
- Kerberos → Autorização para uso de recursos
  - Estabelecer uma relação de confiança entre clientes e servidores
  - Sistemas clientes são autenticados através das identidades de seus usuários
  - Usuários provam sua identidade para acesso a cada serviço e servidores provam suas identidades para os clientes
- PKI →Infraestrutura global de acordo com a ITU-T X.509

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Kerberos

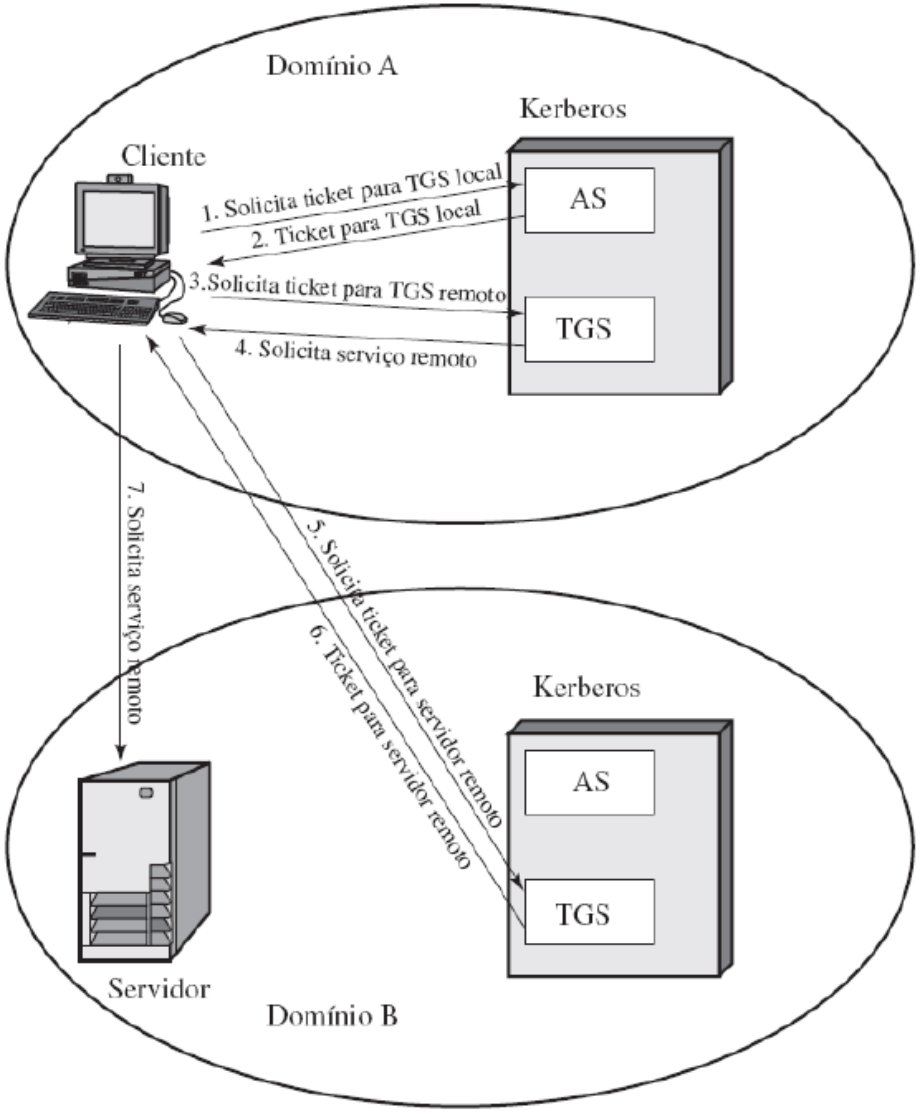


UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Kerberos

- Domínios Kerberos
  - Um servidor Kerberos
  - Clientes registrados com o servidor, que possuem os hashes das suas senhas
  - Servidores de Aplicações com chaves compartilhadas com o servidor
- Para escalar, os servidores Kerberos devem compartilhar chaves

# Kerberos – Múltiplos Domínios



# Kerberos v4 e v5

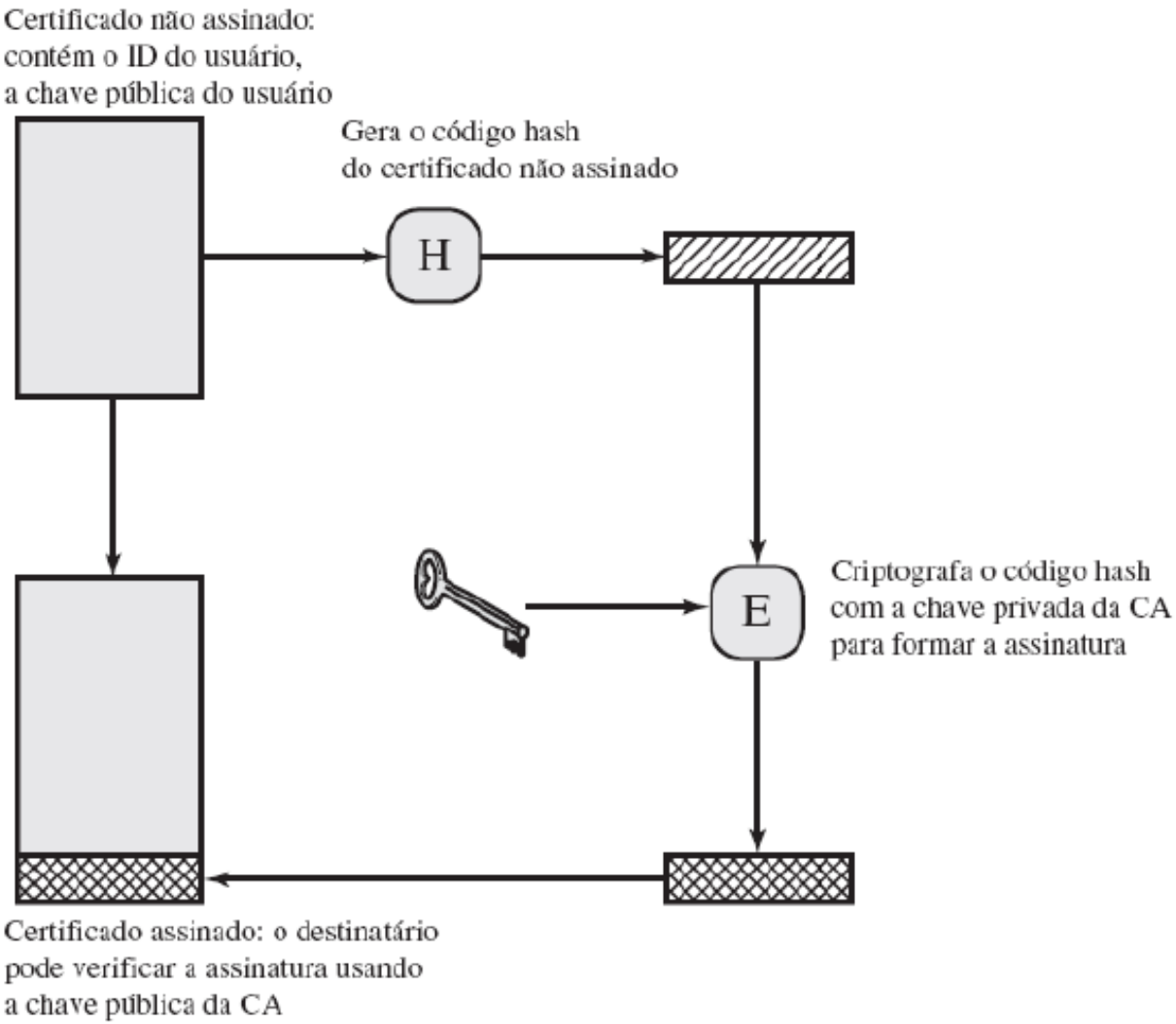
- Versão 4 → ainda em uso, algumas limitações ambientais e deficiências técnicas. Exemplos:
  - Apenas o DES pode ser usado
  - Tempo de vida do ticket limitado (21 horas)
- Versão 5 → RFC 1510 (uso global)
  - Endereça as deficiências da versão 4
    - Qualquer algoritmo de criptografia
    - Validade do ticket ilimitada

# Autenticação X.509

- A recomendação prevê a existência de servidores públicos de diretório, onde os certificados podem ficar disponíveis
- As Autoridades de Certificação (CA) dão confiabilidade às chaves públicas
- Não padroniza algoritmos mas recomenda o RSA
- Formato padrão de certificado X.509

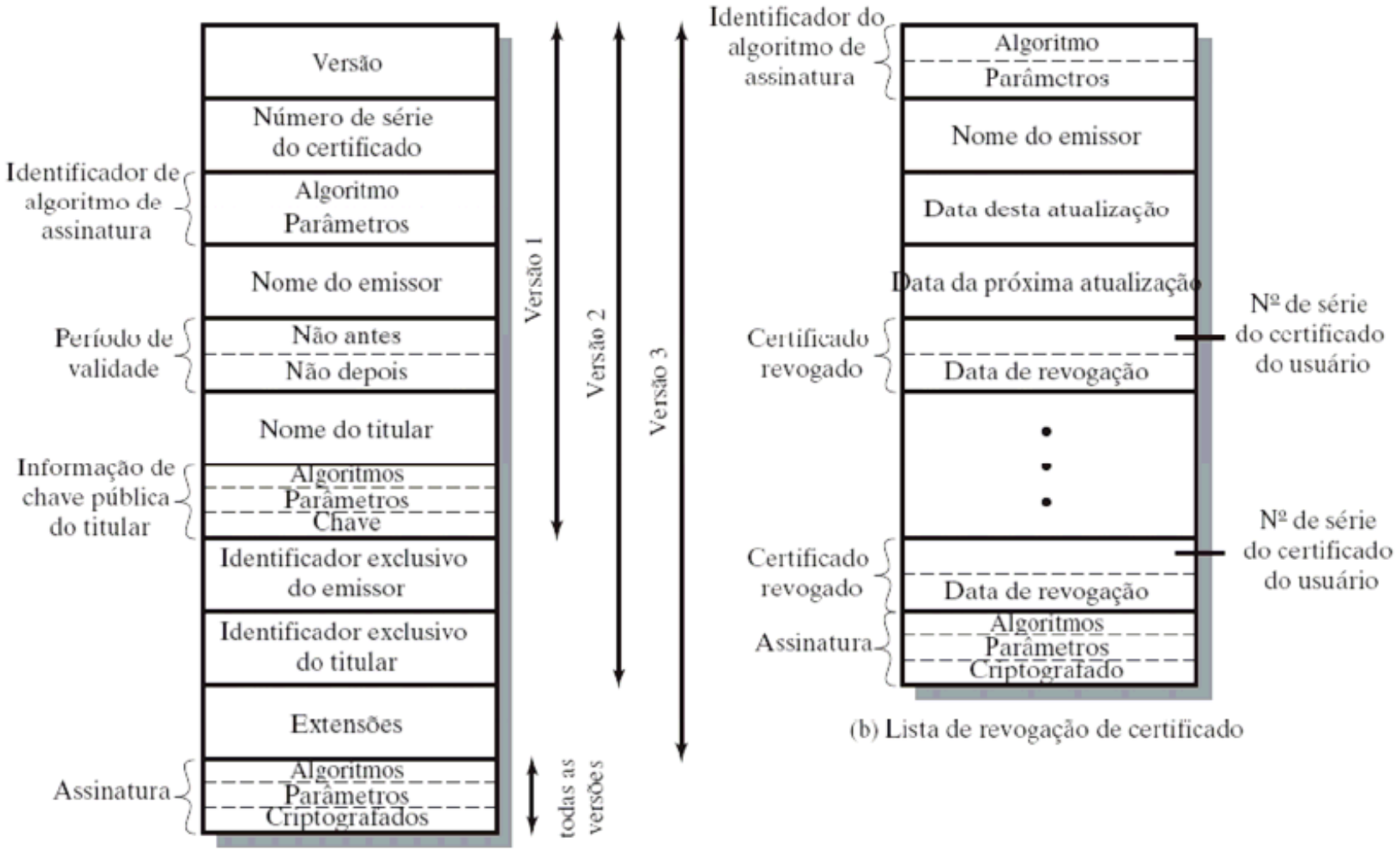
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Criação de um Certificado



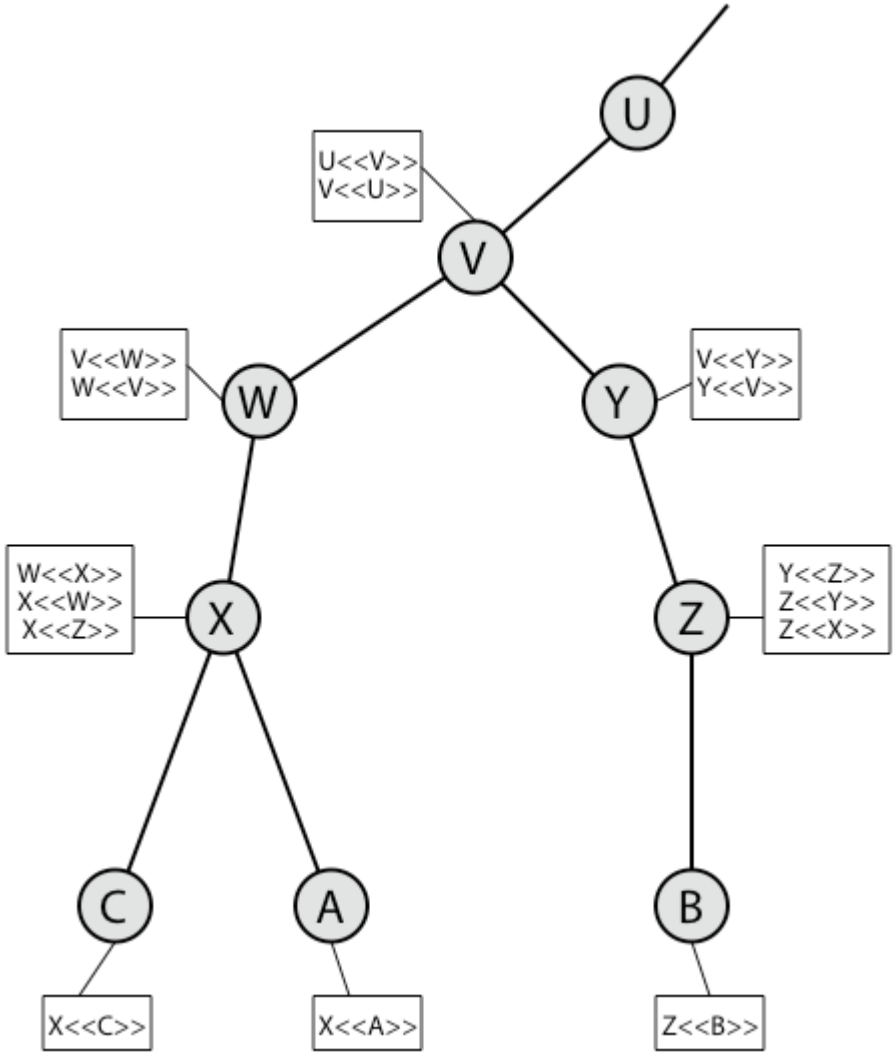
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Formato do Certificado

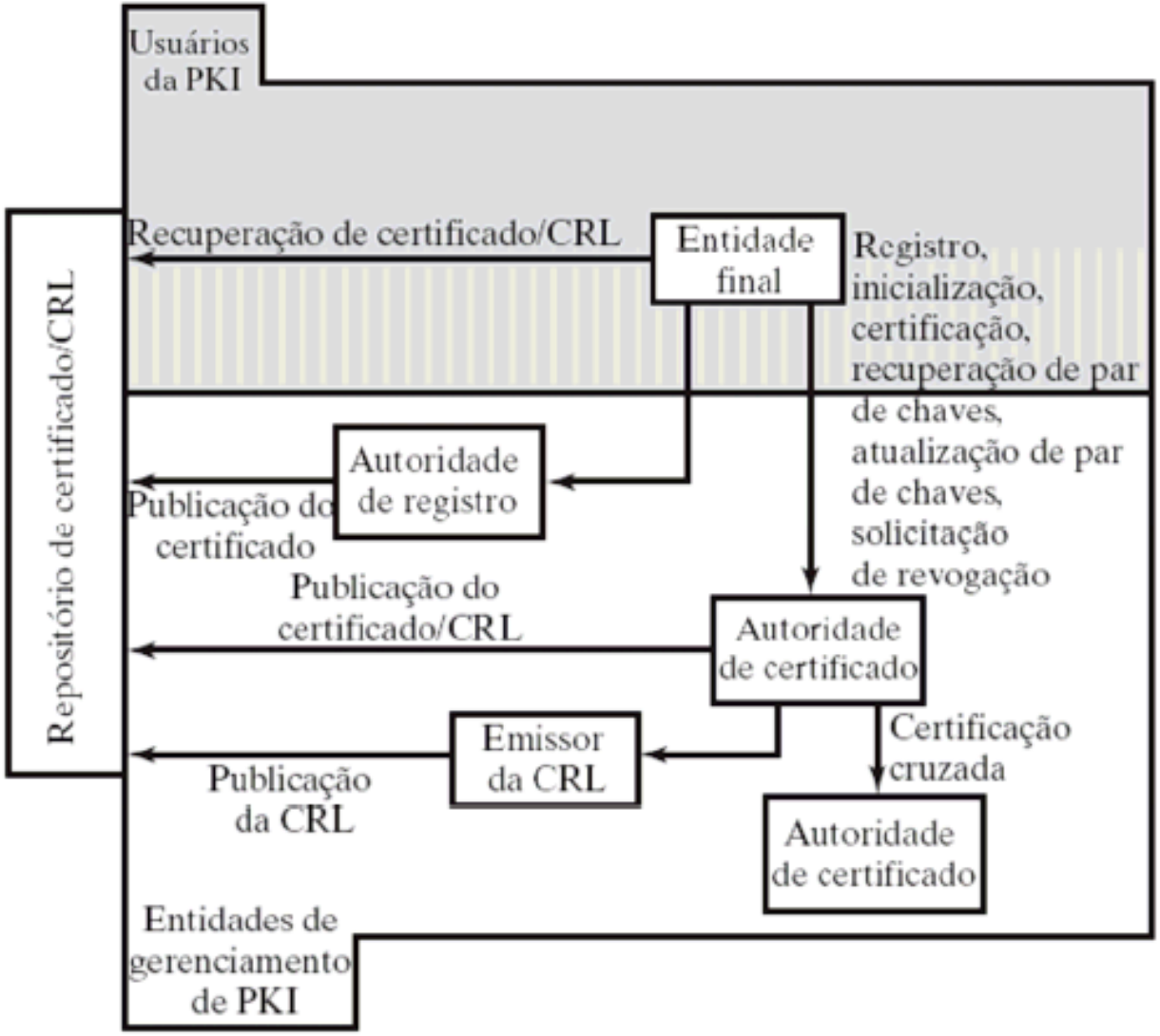



(b) Lista de revogação de certificado

# Hierarquia de CA




- A validação de certificados pode ser feita recursivamente
- As CA mantém uma CRL com certificados que perderam a validade e os que foram comprometidos

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# PKI