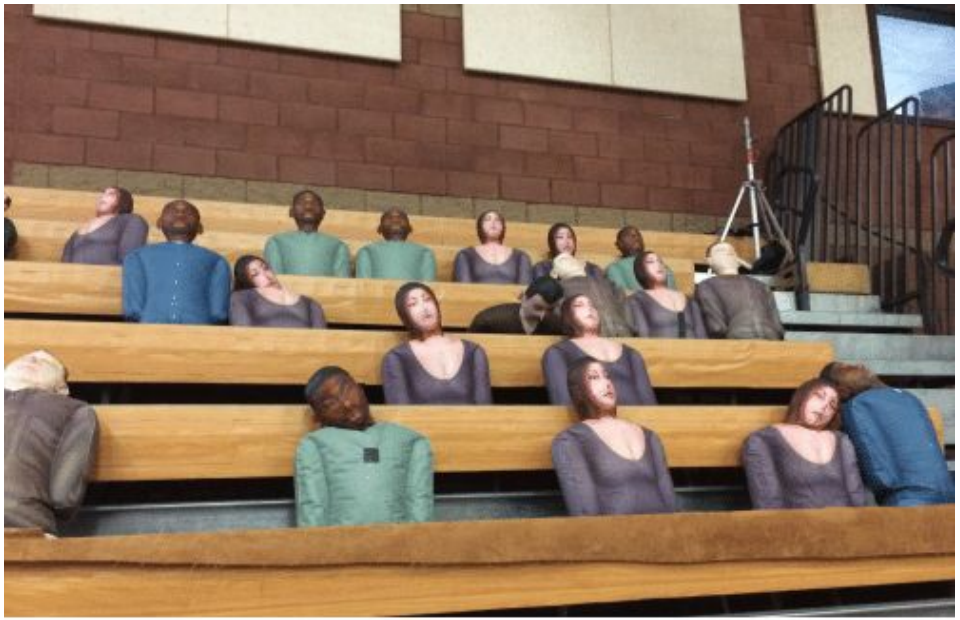
INE5429-07208 Segurança em Computação Criptografia Assimétrica e Integridade

Prof. Jean Everson Martina

O que vimos na aula passada:

- Modos de Operação
- Números Primos
- Teoremas de Fermat e Euler
- Testes de Primalidade
- Geradores de Números Aleatórios
- Logaritmo Discreto
- Propriedades de Criptosistemas de Chave Publica

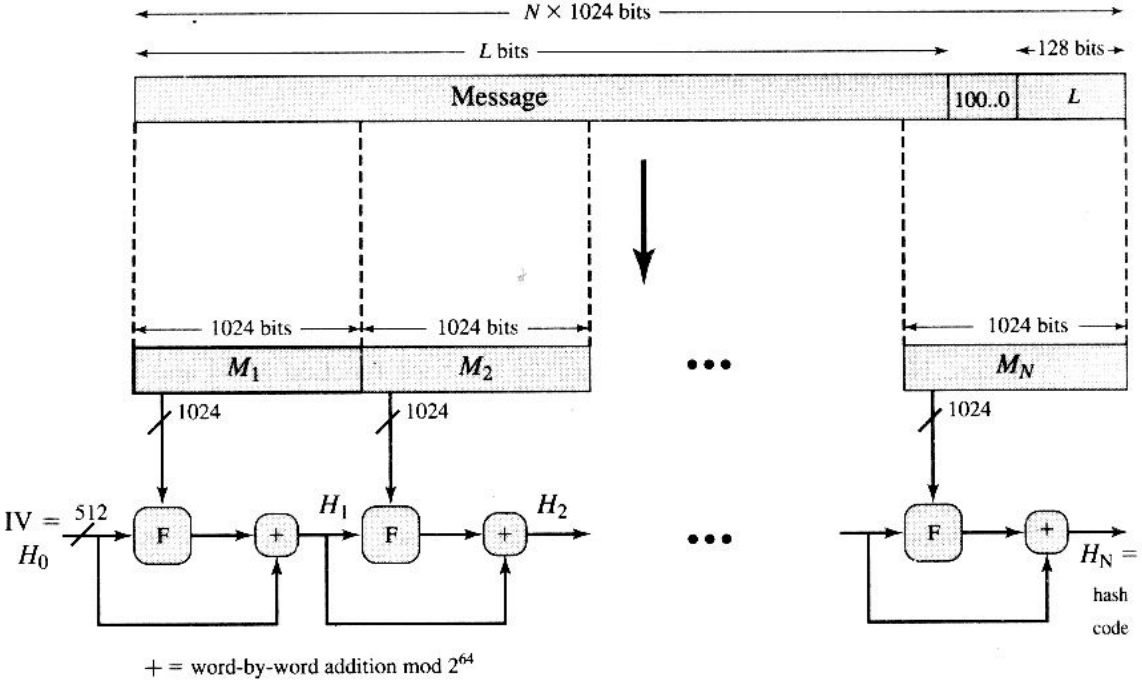


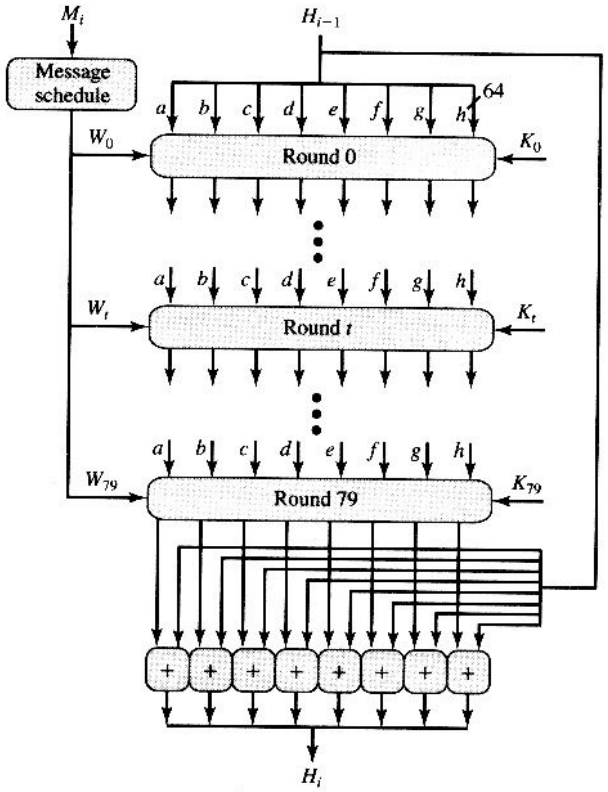
Secure Hash Algorithm

	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

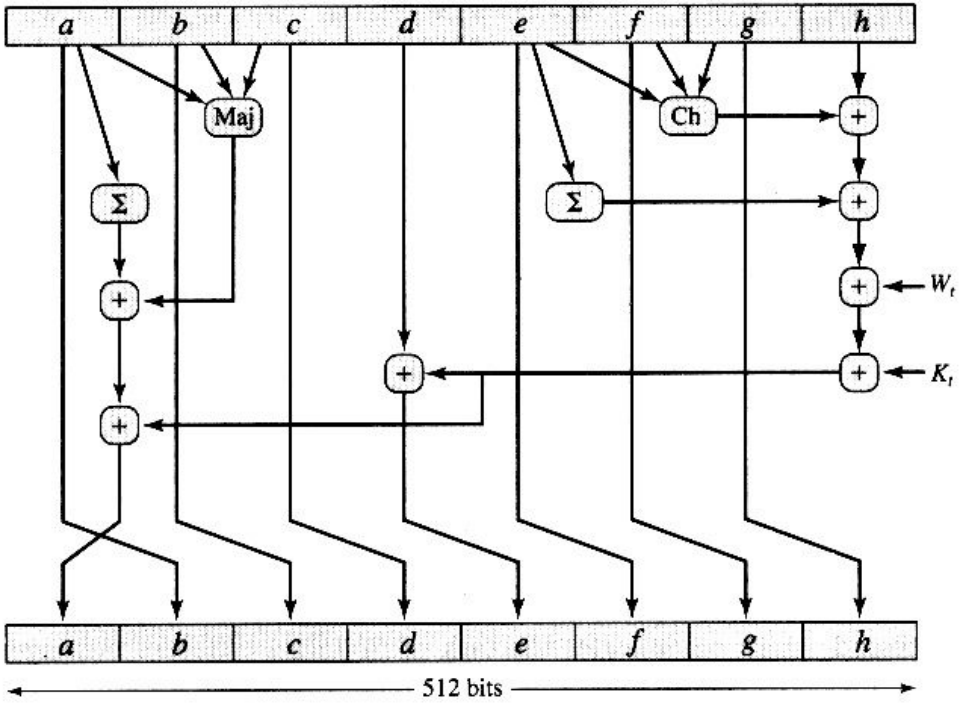
- NIST – FIPS 180/1993 – FIPS 180-1/1995 – FIPS 180-2/2002
- Baseado no MD4
- RFC 3174 – FIPS + Código C de referência
- SHA-1, SHA-256, SHA-384, SHA-512
- SHA-1 não recomendada pois tem colisões em 2^{69}

SHA-512


N × 1024 bits
L bits
128 bits
Message
100..0
L
1024 bits
1024 bits
1024 bits
M1
M2
MN
1024
1024
1024
IV =
H0
512
F
+
H1
F
+
H2
F
+
HN =
hash
code
+ = word-by-word addition mod 2^64


Mi
Hi−1
Message
schedule
64
a b c d e f g h
W0
Round 0
K0
Wt
Round t
Kt
W79
Round 79
K79
+
Hi

SHA-512



$Ch = (\wedge)\otimes(\neg\wedge)$

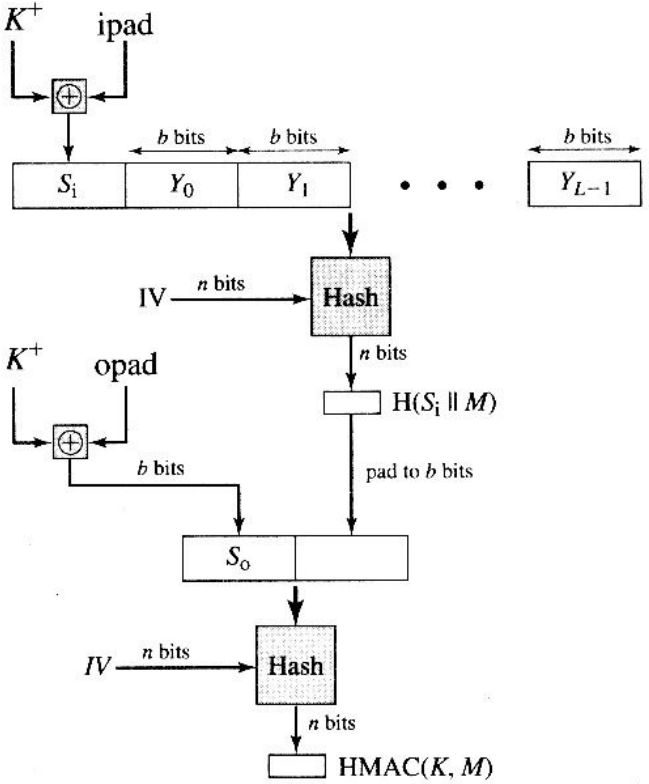
$Maj = (\wedge)\otimes(\wedge)\otimes(\wedge)$

$\sum a = R^{28}\otimes R^{34}\otimes R^{39}$

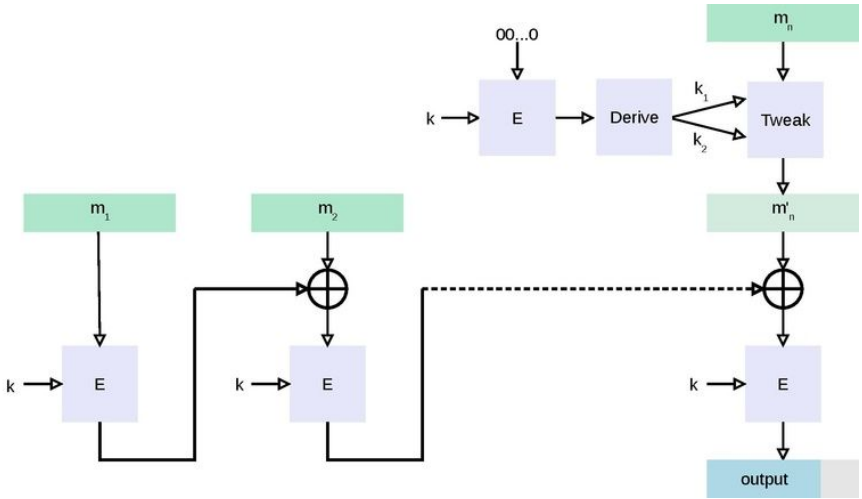
$\sum e = R^{14}\otimes R^{18}\otimes R^{41}$

HMAC

- MAC baseado em função HASH
- Objetivos:
  - Mais rápido que cifragem
  - Funções HASH amplamente disponíveis
- RFC 2104 /FIPS 198 → como adicionar um chave a um HASH
- Usado em SSL e IPSEC
- Objetivos:
  - Usar funções HASH sem modificação
  - Permitir trocar a função HASH
  - Preservar a performance do HASH
  - Usar chave de maneira simples
  - Ter toda análise criptográfica baseada no função HASH



CMAC



- FISP PUB 113 – Baseado em CBC-MAC
- CBC-MAC só funciona para tamanho de mensagens fixos
- Usa-se o ultimo bloco do CBC e se adiciona uma chave derivada no ultimo XOR
- A chave derivada é uma multiplicação $GF(2^n)$
- O polinômio base é padronizado

Assinatura Digital

- É um mecanismo de autenticação que possibilita o criador da mensagem ser identificado
- A autenticação provida poder ser de um caminho ou mútua
- Prove não-repúdio
- Pode ser direta ou arbitrada
- Requisitos:
  - A assinatura deve depender de cada bit da mensagem
  - Deve usar algo único do criador
  - Deve ser fácil de produzir, reconhecer e verificar
  - Dever ser computacionalmente não forjável
  - Dever ser possível reter uma cópia

Digital Signature Standard

- NIST FIPS PUB 186-2/2000
- Usa SHA-1
- Foi revisado duas vezes por problemas de segurança
- A ultima versão, além do algoritmo baseado em Elgamal permite RSA e Curvas Elipticas.
- O DSS original provê somente assinatura
- O HASH de entrada é sempre entregue com um número aleatório → duas assinatura da mesma origem não necessariamente produzem o mesmo resultado
- O resultado (r,s) depende da chave privada e de um conjunto de parâmetros das partes
-

DSS - Construção

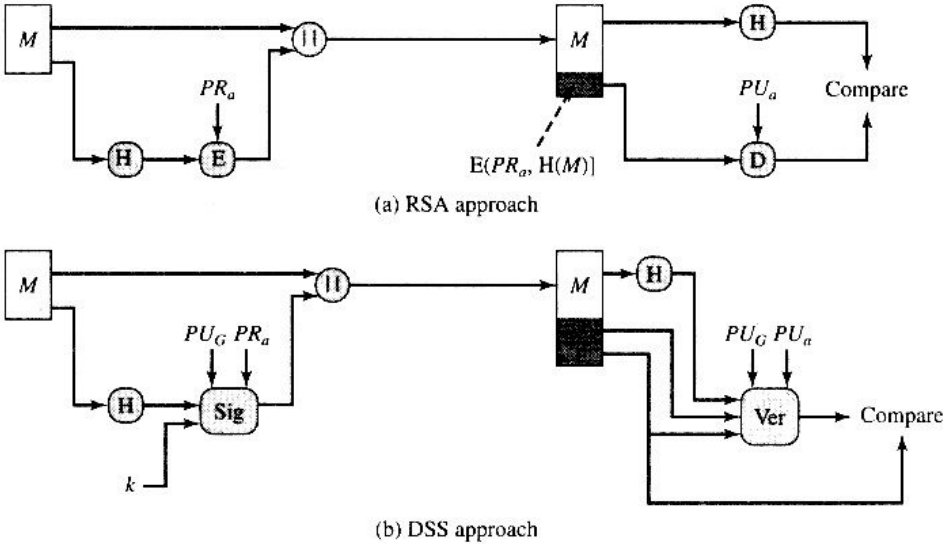
- Globais:
  - p: primo entre 512 e 1024 bits múltiplo de 64bits
  - q: primo de 160bits divisor de (p-1)
  - $g=h^{(p-1)/q} \bmod p \wedge 1 < h < (p-1)$
- Usuário:
  - x: chave privada aleatória | $0 < x < q$
  - $y = g^x \bmod p \rightarrow$ chave pública
- Mensagem:
  - k: aleatório | $0 < k < q$

- Assinatura
  - $r = (g^k \bmod p) \bmod q$
  - $s = \{k^{-1}(H(M) + xr)] \bmod q$
- Verificação
  - $w = (s')^{-1} \bmod q$
  - $u1 = [H(M')w] \bmod q$
  - $u2 = (r')w \bmod q$
  - $v = [(g^{u1}\ y^{u2}) \bmod p] \bmod q$
  - V = r é a validação

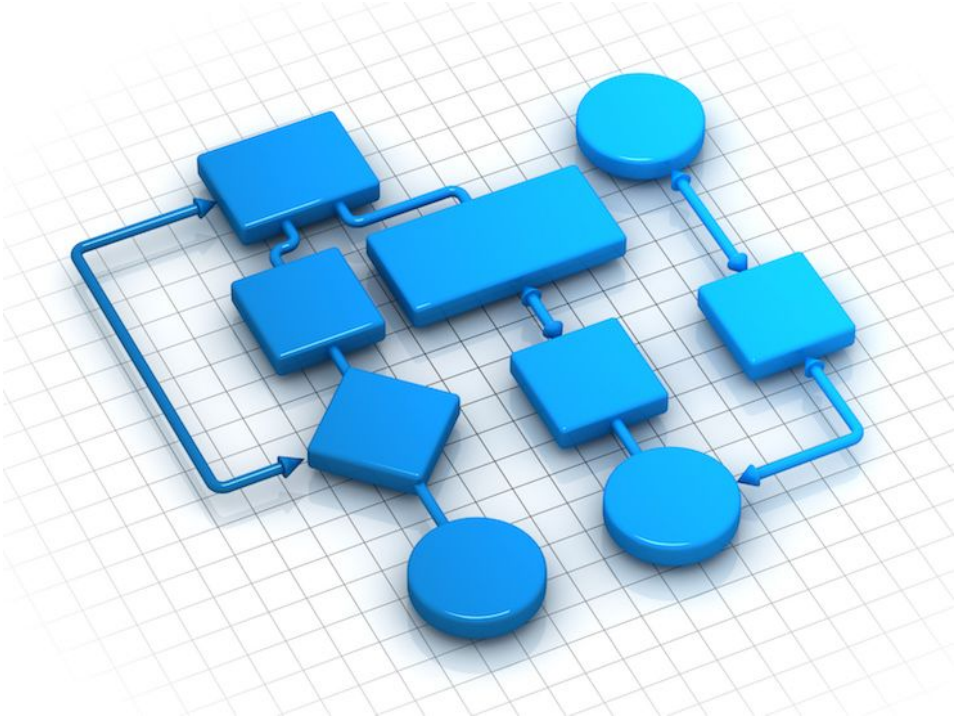
DSS - Características

- g^k mod p é única parte intensiva
- Vários r's podem ser pré-calculados pois não dependem da mensagem
- É impossível recuperar k a partir de r e x a partir de s
- Uma assinatura é de fato composta por (p, q, g, y, r, s) concatenados a mensagem

RSA x DSS



Protocolos Criptográficos



- Como algoritmos devem ser usados para atingir objetivos com menor custo.
- É uma computação distribuída baseada numa séries de passos
- Criptografia por si só não é eficiente
  - Uma porta de ferro sozinha não torna um ambiente seguro
- Combinam as propriedades das várias técnicas para alcançar novos objetivos
- Aspectos
  - Acordo ou estabelecimento de chaves
  - Autenticação de Entidades
  - Criptografia simétrica com autenticação de mensagens
  - Segurança em camada de transporte
  - Métodos de não repúdio

Protocolos Criptográficos - Propriedades

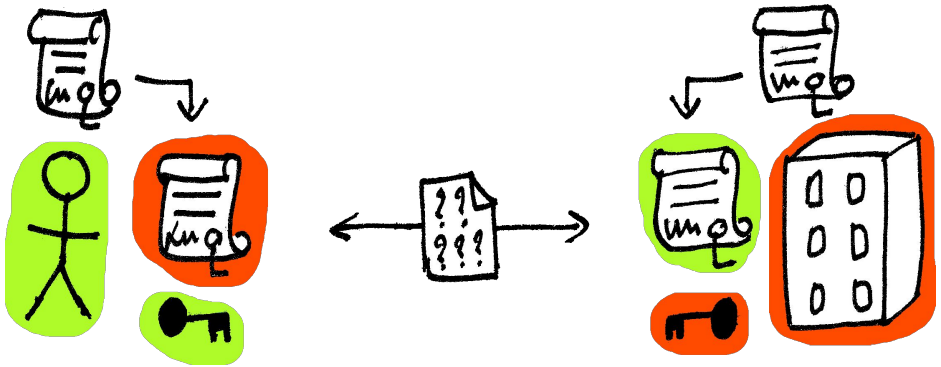
- Confidencialidade
- Integridade
- Autenticação
- Anonimato (Assinaturas Cégas)
- Temporalidade
- Não-repúdio
- Composições variadas

Modelos de Ameaças

- Dolev-Yao → modelo formal de ameaça
  - Atacante onipotente
  - Ouve, intercepta e sintetiza
  - Só é limitado pelos métodos criptográficos e pela incapacidade de adivinhar
- Repetição
- Oráculo
- Colusão

Protocolos Criptográficos de Autenticação Mútua

- Permite ambas as partes do protocolo se satisfazerem da identidade da outra parte
- Se focam na troca de chaves, confidencialidade e temporalidade
- Normalmente se defendem da ameaça de repetição mas não de colusão
- Podem ser baseado em chave assimétrica, simétrica ou ambos
- Simétrico
    - As partes compartilham uma chave simétrica com uma terceira parte confiável e concordam numa chave simétrica
    - Distribuem uma chave simétrica depois provam a posse para o outro lado
    - Exemplos:
        - Needham-Schroeder Shared Key
        - Denning-Sacco



Needham-Schroeder Shared Key

- A → KDC: A,B,Na
- KDC → A: E(Ka,[Kab,B,Na,E(Kb,[Kab,A])])
- A → B: E(Kb,[Kab,A])
- B → A: E(Kab,Nb)
- A → B: E(Kab,Nb+1)
- Seguro por 15 anos
- Execução por tempo indeterminado
- Não revogação de chaves de sessão

Denning-Sacco (avô-Kerberos)

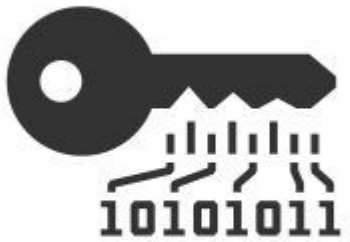
- A → KDC: A,B
- KDC → A: E(Ka,[Kab,B,T,E(Kb,[Kab,A,T])])
- A → B: E(Kb,[Kab,A,T])
- B → A: E(Kab,Nb)
- A → B: E(Kab,Nb+1)
- Também inseguro por Oráculo
- Deu origem ao Neumann em 1990

Autenticação Mútua - Assimétrico

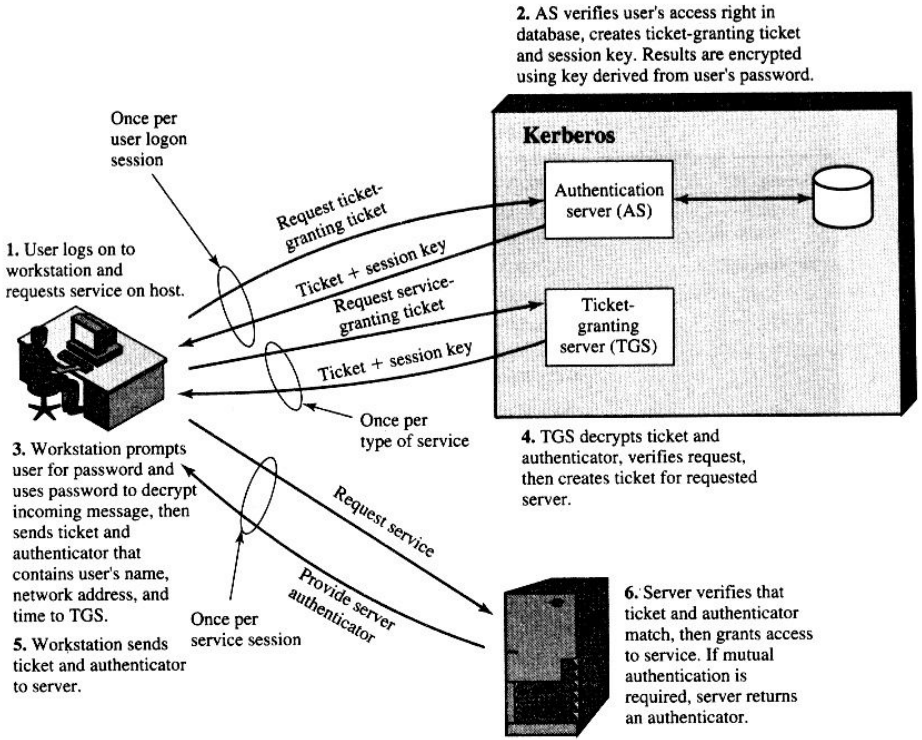
- Ambas as partes possuem um par de chaves assimétricas, das quais uma é privada e a outra é amplamente pública
- Trocam nonces que podem ser usados para troca de chaves simétricas depois
- Exemplos
  - NS Public Key
  - Woo-Lam
  - SSL/TLS

Needham-Schroeder Public Key

- A → B: E(KuB,[Na,A])
- B → A: E(KuA,[Na,Nb])
- A → B: E(KuB,Nb)
- Execução por tempo indeterminado
- Vulnerável a Oráculo



Kerberos

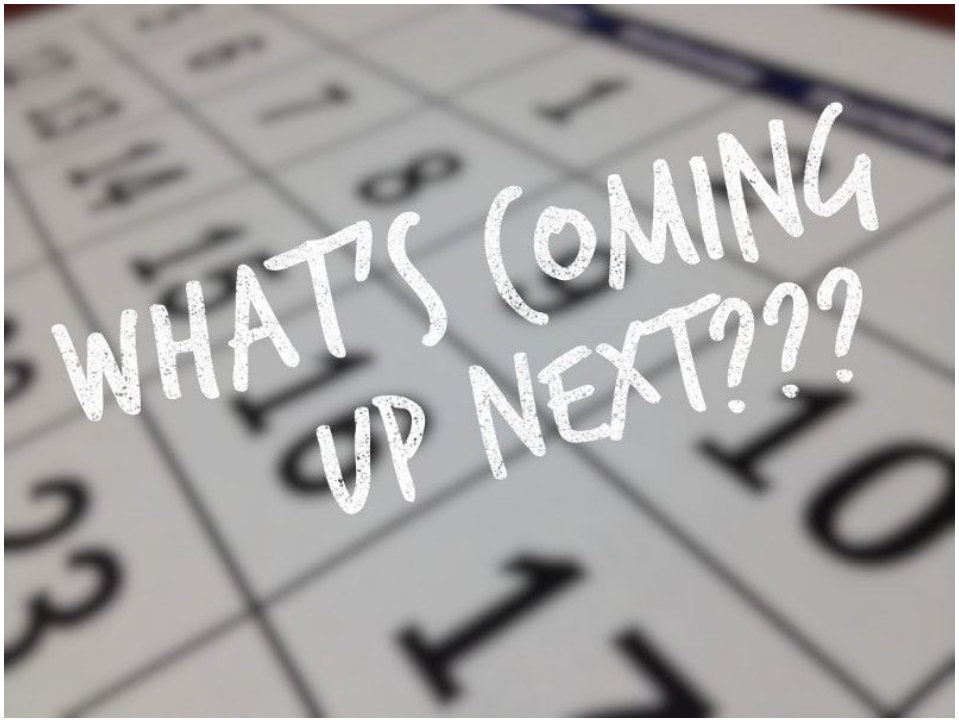


- Desenvolvido pelo MIT na década de 1980 é o protocolo mais usado do planeta
- Baseado na idéia de tickets
- Usa um modelo cliente-servidor
- Prove autenticação mútua
- Se protege de vazamentos e ataques de repetição
- 100% criptografia simétrica

Próximas Aulas

- Prática:
  - Trabalho Individual III

- Teórica:
  - Protocolos Avançados e Documento Eletrônico



Perguntas?

jean.martina@ufsc.br