Criptografia com chaves públicas (Criptografia assimétrica)

SEGA4 – Segurança da Informação

Objetivos

- Apresentar histórico e motivação para a criptografia com chaves públicas.
- Conhecer o protocolo de Diffie e Hellman.
- Conhecer o protocolo RSA.
- Conhecer o conceito de infra-estrutura de chaves públicas.
- Conhecer o protocolo SSL.

Motivação

- Logística para a distribuição de chaves simétricas.
  - Distribuir chaves é um problema complexo:
    - Dentro de uma força armada: Cada unidade (cada vaso de guerra, cada aeronave, tanque, etc), requer o reabastecimento periódico de livros de chaves, diskettes, fitas, etc.
- Assinatura digital
  - Como criar um mecanismo digital que possa demonstrar a autoria de uma mensagem ou documento?

Analogia com cadeados

- Alice precisa enviar uma mensagem para Bob. Mas o correio é não confiável e os carteiros frequentemente tem acesso ao conteúdo das cartas.
- Alice envia a mensagem para Bob dentro de uma caixa com fechos para dois cadeados. Alice utiliza um dos fechos com o seu cadeado.

Cont.

- Bob ao receber a caixa, coloca o seu cadeado no outro fecho e envia a caixa de volta para Alice.
- Alice retira o seu cadeado e devolve a caixa para Bob.
- Bob retira o seu cadeado e abre a caixa.

Problemas

- A criptografia simétrica não funciona como os cadeados. A ordem de encriptação e decriptação é importante.
- Este problema inspirou Diffie e Hellman na busca por uma solução para o problema das chaves simétricas.
- Problema era considerado insolúvel.

Função unidirecional

- Fácil de calcular em um sentido, mas muito difícil desfazer.
- Analogia: quebrar um ovo é fácil, mas é muito difícil reconstituir o ovo original.

Aritmética Modular

- Exemplo: Relógio trabalha com módulo 12.
  - Para 17h o relógio marca 5h=(17 mod 12).
- Exemplo de função unidirecional.
  - $7^x \bmod 11$

Algoritmo de Diffie e Hellman para troca de chaves

- O algoritmo baseia-se na função $G^x \pmod N$.
- Bob e Alice concordam em valores para G e N. Por exemplo G=7 e N=11 (com G<N e G e N primos).

Passos

- 1: Alice escolhe um número A (ex. 3) e guarda esse número como segredo. Bob escolhe um número B (ex. 6) e também guarda como segredo.
- 2: Alice calcula $7^3 \pmod{11} = 2$ e envia esse resultado para Bob. Bob calcula $7^6 \pmod{11}=4$ e envia esse resultado para Alice.

Cont.

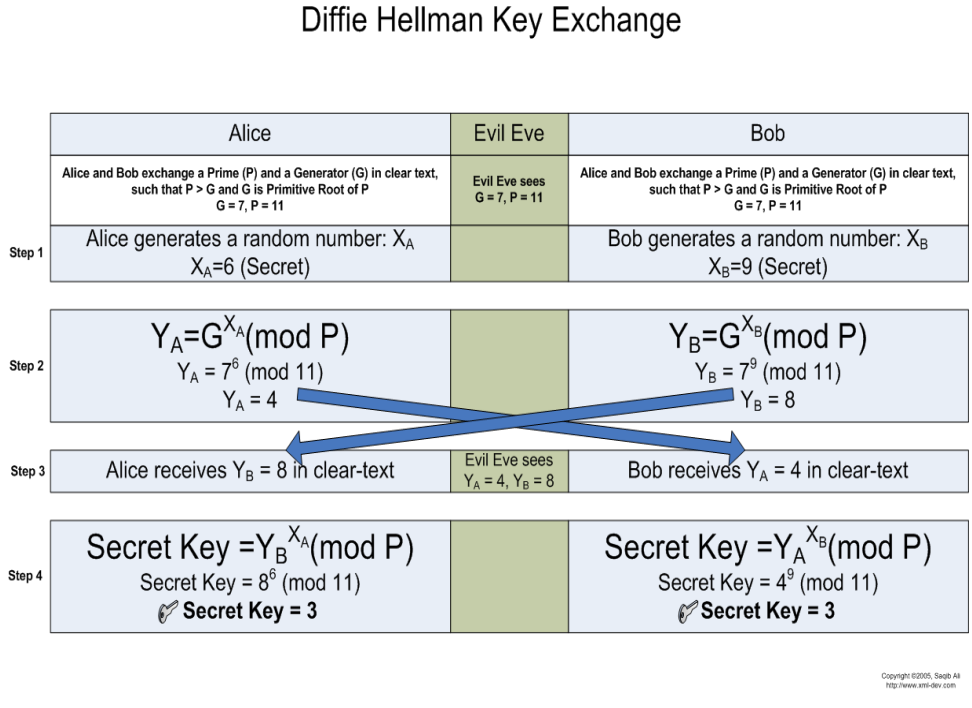
- 3: Alice pega o valor de Bob e calcula $4^3 (\text{mod } 11) = 9$. Bob pega o valor de Alice e calcula $2^6 (\text{mod } 11) = 9$.
- 9 é a chave comum entre Alice e Bob. A chave não precisa passar pelo canal inseguro.

Repetição

- Utilizando um canal inseguro Alice e Bob concordam em dois números primos G e N. N deve ser um número grande (1024 bits).
- Alice escolhe um número inteiro A e usando A ela calcula $B = (G^A) \text{ mod } N$. Ela transmite B para Bob.
- Bob seleciona um inteiro C , e calcula $D = (G^C) \text{ mod } N$. Ele transmite D para Alice.

Cont.

- Alice calcula K = (D^A) mod N e Bob calcula K = (B^C) mod N.
- K é igual a (G^{AC})mod N em ambos os casos.
- Eva, não pode calcular K pois não conhece A ou C. Assim K pode ser utilizada como uma chave entre Alice e Bob.
- O algoritmo é seguro pois é difícil obter o valor de um logaritmo em módulo (problema do logaritmo discreto). Para um N (primo) com mais de 300 digitos, A e C com pelo menos 100 digitos o cálculo do logaritmo levaria o tempo de existência do Universo.



Restrição

- Necessidade de troca mútua de parâmetros para o cálculo da chave compartilhada.
  - Alice e Bob precisam estar simultâneamente ativos para que se possa estabelecer uma chave comum.
- É necessário o uso de duas chaves públicas para estabelecer a comunicação.

Vulnerabilidades

- Ataque man in the middle
  - Eva pode se mascarar como Alice para Bob. Bob e Eva passam a compartilhar uma chave comum.
- Geração de números aleatórios.
  - Se a saída do gerador não for “muito” aleatória e for possível adivinhar valores, o atacante terá a sua tarefa simplificada.

RSA

- Criado por Ron Rivest, Adi Shamir e Len Adleman no MIT em 1977.
- Clifford Cocks descreve um algoritmo semelhante em 1973. (novamente, um segredo guardado por interesses governamentais)
- Patenteado nos EUA em 1983 (A patente expirou em 21 de setembro de 2000).

Idéia central

$y = f(x) = x^e \bmod n$ É fácil para computar.

$x = f^{-1}(y)$ É extremamente difícil para computar.

Operação

- Selecione **p** e **q** (2 primos grandes) e calcule **n=pq** (n é conhecido como módulo).
- Selecione um número **e** < **n** e primos relativos a **(p-1)(q-1**). Isto é, **e** e **(p-1)(q-1)** não possuem fatores comuns exceto 1.
- Encontre outro número **d** tal que **(ed-1**) é divísivel por **(p-1)(q-1).**

Cont.

- Os valores **e** e **d** são chamados respectivamente de expoentes públicos e privados.
- A chave pública é o par **(n,e)** e a chave privada é o par **(n,d**). Os fatores **p** e **q** podem ser descartados ou mantidos com a chave privada.

Encriptação e decriptação

- O texto cifrado c é obtido de:
  - $c = m^e \bmod n$. (usando a chave pública).
- O texto original é obtido de:
  - $m = c^d \bmod n$ (uso da chave privada).

Exemplo simples

- *Seja*
- $p = 61$ número primo (mantido secreto)
- $q = 53$ segundo primo (secreto)
- $N = pq = 3233$ (público)
- $e = 17$ (expoente público)
- $d = 2753$ (expoente privado)

Cont.

- A função de encriptação é:
  - encrypt(n) = n^e mod N = n^{17} mod 3233
- A função de decriptação é:
  - decrypt(c) = c^d mod N = c^{2753} mod 3233
- Para encriptar 123, calcula-se
  - encrypt(123) = 12317 mod 3233 = 855
- Para decriptar o texto cifrado, calcula-se
  - decrypt(855) = 855^{2753} mod 3233 = 123

Assinatura digital

- O RSA pode ser utilizado como assinatura digital de uma pessoa.
- Suponha que Alice deseja mandar uma mensagem **m** para Bob e garantir a autenticidade.
- Alice cria uma assinatura digital **s**. Onde:
  - $\mathbf{s = m^d \bmod n}$.
- Ela envia m e s para Bob. (poderia utilizar um hash de m).
- Bob verifica a autenticidade se $\mathbf{m = s^e \bmod n}$.

Geração de chaves

1. Selecione um número n aleatório.
2. Selecione um número a<n aleatório.
3. Execute um teste de primalidade, tal como o Miller e Rabin, com a como parâmetro. Se n falhar, volte para o passo 1.
4. Se n passou por um número suficiente de testes, aceite n; caso contrário volte para o passo 2.

- Quantas tentativas serão realizadas?
  - Pelo teorema dos números primos, os primos estão espaçados de um número N em média ln(N).
  - Retirando os pares temos: ln(N)/2. Assim para $N=2^{200}$ teremos $\ln(2^{200})/2 = 70$ tentativas.

Segurança do RSA

- A segurança do RSA depende do problema de fatoração de números grandes (N) em dois números primos (p,q).
- Não existem algoritmos polinomiais (até o momento) para resolver este problema.
- Até 2004 era possível fatorar números com 174 digitos (576 bits). As chaves do RSA são de 1024-2048 bits.
- Alguns especialistas estimam a quebra de chaves de 1024 bits num médio prazo.

Ataques

- Temporização
  - Foi reportado que é possível deduzir a chave ***d*** a partir de medidas de tempo para decifração de diferentes textos cifrados.
  - Contra-medida: garantir que o tempo de término seja constante para qualquer texto cifrado.

Cont.

- Man in the middle
  - Eva pode enviar uma chave pública para Bob fingindo ser de Alice.
  - Eva pode interceptar mensagens de Bob para Alice, ler ou copiar estas mensagens e enviar uma cópia para Alice com a chave pública de Alice.
- Solução:
  - Certificados digitais e outros componentes de uma ICP – Infra-estrutura de chaves públicas (PKI).

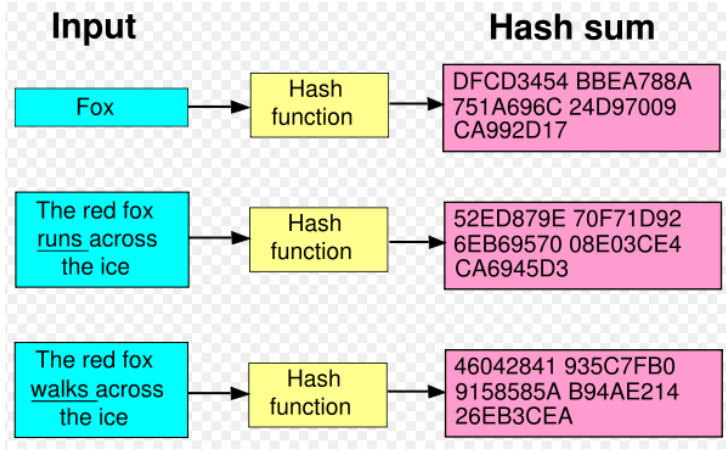
Criptografia Híbrida

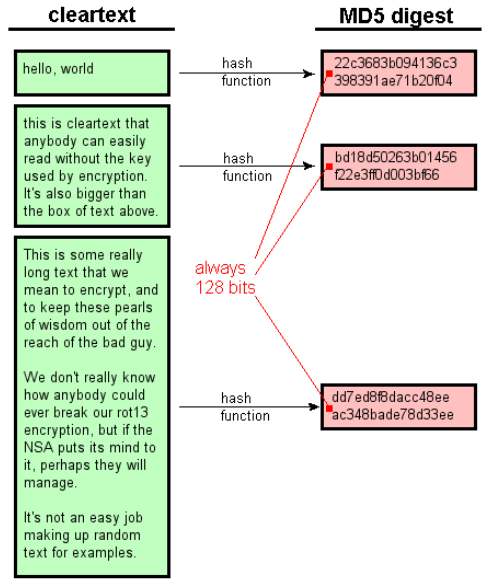
- A criptografia assimétrica tem uma limitação:
  - Desempenho.
- Solução:
  - Utilizar a criptografia assimétrica para trocar uma chave simétrica.
  - Uma vez estabelecida a chave simétrica, a comunicação é efetuada com essa chave.

Integridade de mensagens

- A criptografia prove confidencialidade dos dados.
- Mas a integridade dos dados não é necessariamente garantida.
  - É possível alterar blocos da mensagem e essa alteração não ser detectada.
- É necessário o uso de uma função para a garantia de integridade da informação.
  - Ao final da mensagem é anexado um valor para verificação da integridade da mensagem.

Função de Hash





Propriedades do Hash

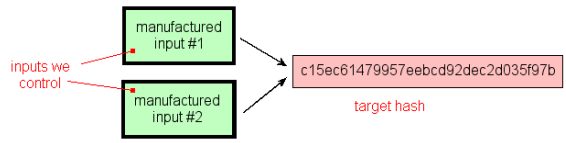
- Um hash é uma espécie de assinatura para um conjunto de dados que representa um documento.
- Algumas propriedades:
  - Avalanche: uma pequena mudança no conteúdo causa uma grande mudança no Hash.
  - Hash é uma função uni-direcional.
  - É pouco provável obter uma colisão:
    - Um hash de 128 bits é um número entre 3,4 $X10^{38}$ possibilidades.

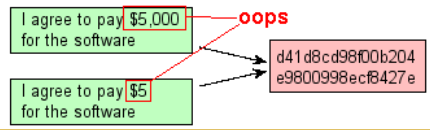
Requisitos de uma função de Hash

1. Aplicável para um bloco de dados de qualquer tamanho.
2. Produz sempre uma saída com o mesmo comprimento.
3. Fácil de ser calculada para qualquer valor x.

4. Resistência a colisão

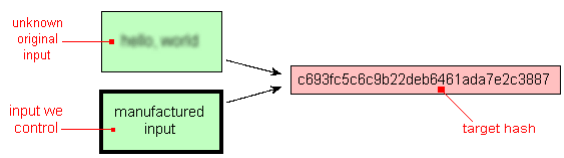
- Deve ser computacionalmente inviável obter duas entradas que produzem o mesmo valor de hash.





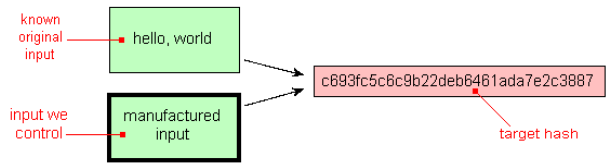
5. Resistência a uma pré-imagem

- Deve ser computacionalmente inviável encontrar uma entrada x que produza uma determinada saída h.



6. Resistência a segunda pré-imagem

- Dado um x conhecido, deve ser computacionalmente inviável obter uma entrada y, diferente que x, que produza o mesmo valor de hash que x.



Usos do Hash

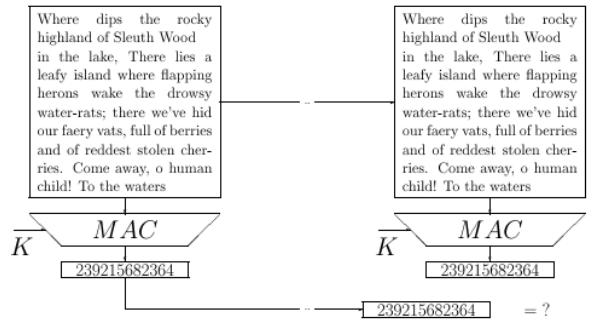
- Verificação de integridade de arquivos.
- Armazenamento de senhas.
- Assinatura de documentos. (Ao invés de criptografar um documento todo, criptografar apenas o hash).

MDC (Manipulation Detection Code)

- MDC é uma função de hash sem o uso de uma chave secreta.
  - Algoritmos utilizados:
    - SHA-1
    - RIPEMD 160.

MAC (Message Authentication Code)

MAC = hash function with secret key.

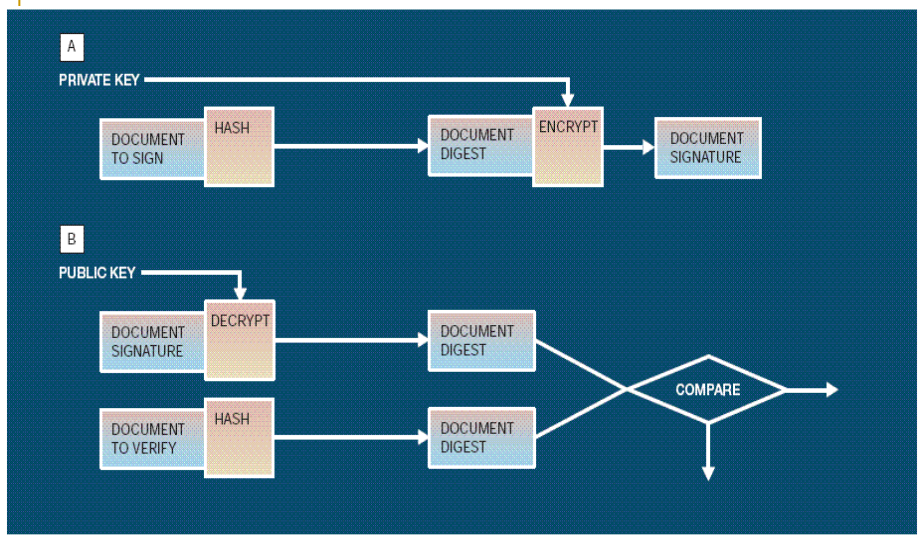


Uso do MAC

- MAC é utilizado principalmente no modo CBC sendo necessário duas chaves. Uma chave para a cifragem e outra para o MAC.
- O último bloco transmitido é o MAC.
- Exemplos de algoritmos
  - HMAC e OMAC.

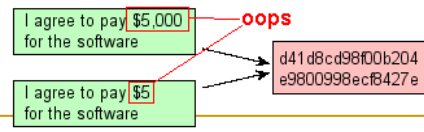
Assinatura Digital

- A combinação de uma função de Hash e a criptografia com chaves públicas possibilita a construção de mecanismos que impedem a não repudiação de autoria de documentos.



Ataques contra funções de hash

- São relatados ataques contra a propriedade de resistência a colisão dos algoritmos MD5 e SHA1 (alguns casos particulares).
- Implicações:
  - Um atacante é capaz de encontrar (x ,y) que produzem um mesmo valor de hash em um tempo viável (ataque da data de aniversário).



Certificado digital

- Um certificado digital é uma assinatura que liga uma chave pública a uma identidade.
- A assinatura é feita por um terceiro de confiança (Autoridade Certificadora)
- O certificado digital serve para comprovar que uma chave pública pertence a uma determinada identidade.

ICP – Infra-estrutura de chaves públicas (PKI)

- Para o gerenciamento de chaves públicas é estabelecido uma infraestrutura onde um terceiro de confiança (autoridade certificadora) estabelece a ligação entre uma chave pública e uma identidade.
- Um usuário pode assinar uma mensagem com a sua chave privada, e o usuário receptor pode verificar a assinatura consultando o diretório de uma autoridade certificadora.
- Isto permite que dois ou mais participantes, possam trocar mensagens confidenciais sem a necessidade de troca de dados secretos.

Estrutura de uma ICP

- Uma organização utiliza os serviços de um ICP. Para tal consulta uma AC (Autoridade certificadora).
- Atualmente um dos padrões mais utilizados para a implementação de ICPs é o X.509.
- Existem ICPs públicas e privadas (Ex. Verisign).

Usos

- Autenticação de usuários
  - Usuário apresenta um certificado para uma aplicação.
  - A aplicação valida o certificado e senha (opcional) em uma AC.
  - A AC verifica se o certificado está associado a uma identidade e uma senha.

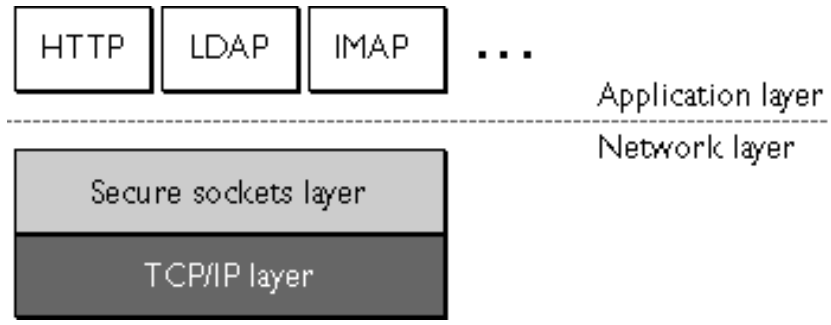
Cont.

- Assinatura digital e não repudiação
  - Em um documento de viagem, um usuário assina, usando sua chave privada, um campo onde ele declara gastos efetuados.
  - O receptor verifica, através de uma AC, a identidade do assinante.
- SSL
  - Um cliente deseja efetuar uma conexão segura com um site de banco.
  - O site estabelece uma conexão segura oferecendo um certificado associado a um certo endereço DNS.
  - O browser do cliente verifica em uma autoridade certificadora a validade do certificado.

Alguns riscos de uma PKI

- Quem é a autoridade de confiança?
  - Uma AC é apenas um gerenciador de chaves.
  - Não dá garantias quanto a corretude das identidades, confiabilidade, autenticidade e integridade.
- Riscos da chave privada.
  - A chave privada está no computador do usuário. Eventualmente em um smartcard. Qualquer uso dessa chave é responsabilidade do usuário.
- Segurança do computador que faz a gerência dos certificados.
- Qual é a identidade associada a um certificado?
  - A identidade identifica o indivíduo correto?
  - Pode ocorrer conflito de nomes.
- Conscientização do usuário.
  - Usuário verifica se a identidade apresentada é o do site desejado?

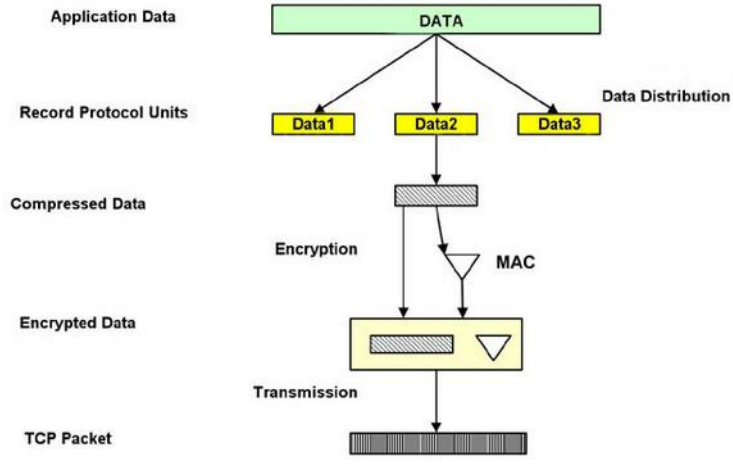
SSL



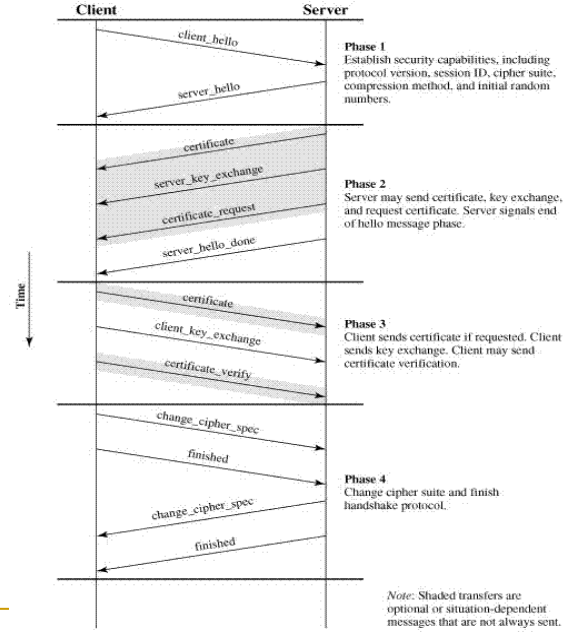
SSL Protocol Stack

SSL handshake protocol	SSL cipher change protocol	SSL alert protocol	Application Protocol (eg. HTTP)
SSL Record Protocol			
TCP			
IP			

Record Protocol



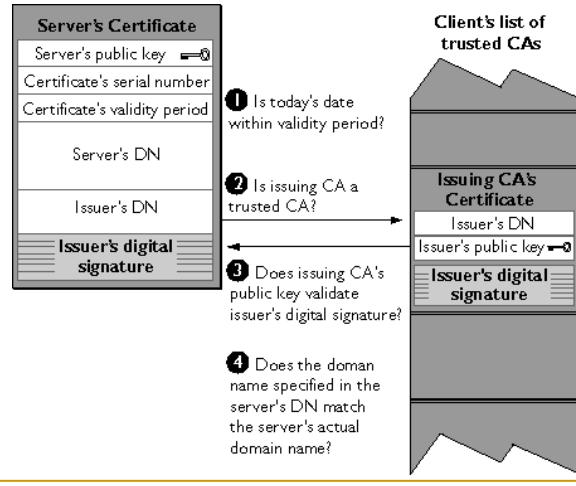
Handshake



Resumo das fases do SSL

- Autenticação do servidor.
- Autenticação do cliente.
- Conexão criptografada.
  - Após autenticação do servidor, o cliente divulga cifradores disponíveis.
  - Utilizando-se da chave pública o cliente recebe uma chave simétrica para um determinado cifrador.
  - A comunicação é feita através de chaves simétricas.

Como um cliente Netscape autentica um certificado recebido



Cifradores comumente utilizados

- RSA
- RC4 (128 bits)
- MD5(para autenticação de mensagens).
- DES (56 bits).

Conclusões

- A criptografia com chaves públicas é um dos grandes avanços tecnológicos das últimas décadas.
- Baseia-se em propriedades matemáticas de funções unidirecionais, fatoração de números primos, etc.
- A privacidade de usuários e a viabilidade de transações comerciais na Internet depende dos algoritmos de criptografia assimétrica.
- Funções de hash são fundamentais para verificação de integridade e criação de assinaturas digitais.