Protocoale de Securitate

Rezumate de mesaje, semnaturi digitale si protocoale de securitate

Rezumatele mesajelor

Proprietati MD – Message Digest:

- Cunoscand P, este usor sa se calculeze MD(P)
- Cunoscand MD(P), este practic imposibil sa se afle P
- Cunoscand P nimeni nu poate gasi P' astfel ca MD(P') = MD(P)
- O schimbare a intrarii de 1 bit produce o iesire diferita

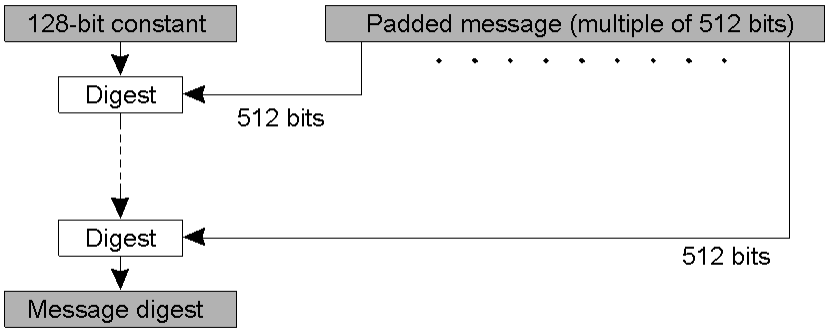
Functii hash

- MD5 (Message Digest)
- SHA-1 (Secure Hash Algorithm)

Functii Hash: MD5

MD5 – Message Digest 5
Calculeaza un rezumat de mesaj de 128 biti

Structura algoritmului MD5 - faze



Functii Hash: MD5 (2)

O **faza** corespunde unui **bloc** de mesaj de 512 biti. Are 4 runde.
O **runda** are 16 **iteratii**. Fiecare runda foloseste o functie diferita:

F(x,y,z) = (x AND y) OR ((NOT x) AND z)
G(x,y,z) = (x AND z) OR (y AND (NOT z))
H(x,y,z) = x XOR y XOR z
I(x,y,z) = y XOR (x OR (NOT z))

$b_0,\ldots,b_{15}$ – **sub-blocuri** 32-biti (total 512)

p, q, r, s – variabile *digest*

$C_1, \ldots, C_{16}$ – constante (in total 64)

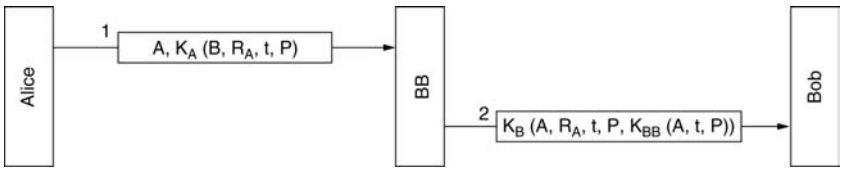
<<< denota rotatie stanga

Iterations 1-8	Iterations 9-16
$p \leftarrow (p + F(q,r,s) + b_0 + C_1) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_8 + C_9) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_1 + C_2) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_9 + C_{10}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_2 + C_3) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{10} + C_{11}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_3 + C_4) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{11} + C_{12}) \lll 22$
$p \leftarrow (p + F(q,r,s) + b_4 + C_5) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_{12} + C_{13}) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_5 + C_6) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_{13} + C_{14}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_6 + C_7) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{14} + C_{15}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_7 + C_8) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{15} + C_{16}) \lll 22$

Semnaturi Digitale

- Bazate pe
  - Chei simetrice
  - Chei publice
- Rezumate de mesaje

Semnaturi cu chei simetrice



Semnaturi digitale cu Big Brother.

- R_A – numar aleator (control replici)
- t – timestamp (mesaj recent)
- K_A – cheie secreta a lui A
- K_B – cheie secreta a lui B
- K_{BB} – cheie secreta Big Brother

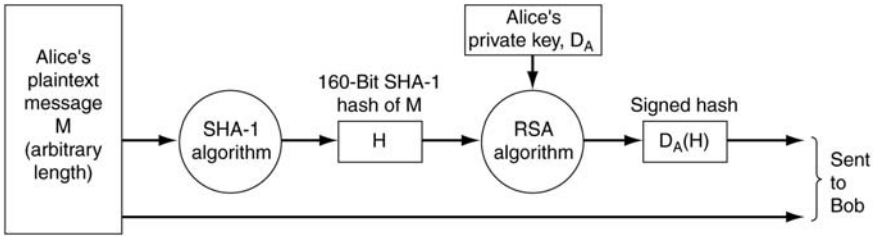
Comentarii

t utilizat pentru a detecta atacuri prin replica pentru mesaje vechi

K_{BB} (A, t, P)) folosit pentru non-repudiere

Semnaturi cu chei publice

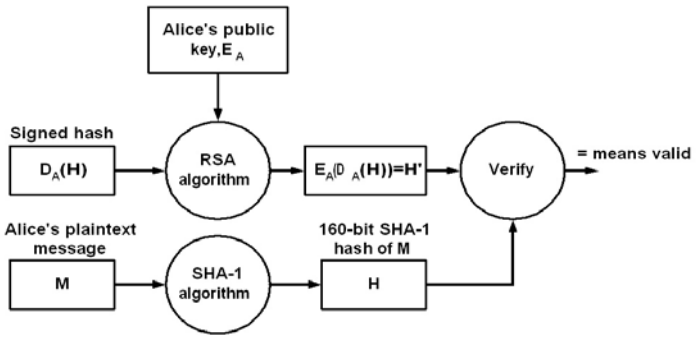
Utilizarea SHA-1 si RSA pentru semnarea mesajelor nesecrete.



Caracteristici

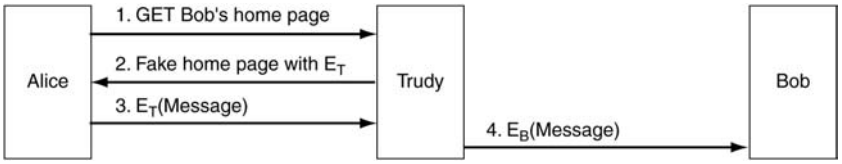
- Rezumatul SHA-1 este semnat cu cheia secreta a transmitatorului D_A
- Mesajul M este transmis in clar

Verificare semnatura digitala



Orice modificare a textului clar M este detectata prin H<>H'
Un intrus nu poate modifica si M si rezumatul criptat $D_A(H)$

Probleme cu difuzarea cheilor publice



Problema: difuzarea cheii publice prin pagina de referinta a proprietarului

- Trudy raspunde in locul lui Bob cu cheia sa publica
- Trudy poate modifica mesajele trimise de Alice lui Bob

Universitatea Politehnica Bucureşti - Facultatea de Automatică şi Calculatoare

Managementul cheilor publice

- Certificate
  - Asociaza identitatea cu cheia publica
- X.509
  - Standard de certificate
- PKI - Public Key Infrastructures
  - Programele, echipamentele, tehnologiile de criptare si serviciile de gestiune a infrastructurii criptografice si a cheilor publice ale utilizatorilor.

Certificate

Rol: leaga cheia publica de un proprietar (principal) sau de un atribut

I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

Un certificat nu este secret

este semnat de o autoritate de certificare - CA (Certificate Authority)

Verificarea certificatului de catre Alice

A calculeaza rezumatul SHA-1 al certificatului (fara semnatura)
A aplica cheia publica a CA asupra semnaturii
A compara cele doua rezultate

Universitatea Politehnica Bucureşti - Facultatea de Automatică şi Calculatoare

Campurile de baza dintr-un certificat X.509

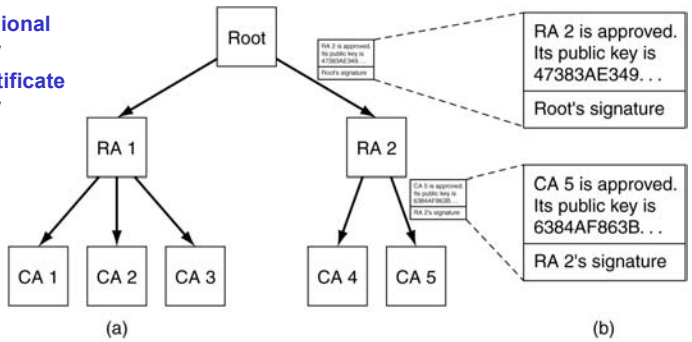
Câmp	Seminificatie
Versiune	Ce versiune de X.509 este utilizată
Număr Serial	Acest număr împreună numele CA-ului identifică în mod unic certificatul
Algoritm de semnare	Algoritmul folosit la semnarea certificatului
Emitent	Numele X.500 al CA-ului
Perioada de validitate	Momentele de început si sfârşit ale perioadei de validitate
Numele subiectului	Entitatea care este certificată
Cheia publică	**Cheia publică a subiectului şi ID-ul algoritmului folosit**
ID emitent	Un ID opțional identificând în mod unic emitentul certificatului (nume X.500 sau DNS)
ID subiect	Un ID opțional identificând în mod unic subiectul certificatului
Extensii	ptr identificarea cheii publice a emitentului, a certificatului care contine o anumita cheie publica, scopul utilizarii cheii (criptare, semnare,…) si altele
Semnătura	**Semnătura certificatului (semnat cu cheia privată a CA-ului)**

PKI - Public Key Infrastructure

- **PKI- Set de componente (hard & soft)** care lucreaza impreuna pentru utilizarea sigura a tehnologiei de chei publice
- **CA**- autoritate de incredere care certifica faptul ca cheia publica inclusa apartine persoanei cu numele atasat
- **CA**- administratie centrala care elibereaza certificate:
  - organizatie sau companie - pentru angajati
  - universitate - pentru studenti
  - CA publice (VeriSign) - pentru clienti

PKI - Public-Key Infrastructures

RA – Regional Authority
CA – Certificate Authority



(a) PKI ierarhic. (b) Un lant de incredere (certification path).

A cunoaste si are in credere in Root
- gaseste certificatul lui B semnat de CA 5
- certificatul lui CA 5 semnat de RA 2
- certificatul lui RA 2 semnat de Root

Simplificare
- A primeste de la B tot lantul de certificate

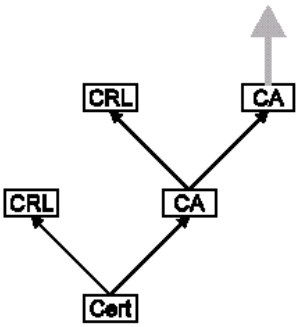
Revocarea Certificatelor

- Un certificat trebuie **revocat** cand:
  - cheia primara este **compromisa**;
  - cheia primara este **pierduta**;
  - o persoana pleaca din companie
  - altele.

- Revocarea trebuie cunoscuta de toti utilizatorii;
- Alternativa - se folosesc liste de revocare
  - **CRL – Certificate Revocation List**;
- **Greu** de implementat si folosit.
  - se verifica listele de revocare inainte de utilizarea certificatelor
  - locul de pastrare a listelor de revocare – duplicare, cache
  - difuzarea listelor de revocare

Universitatea Politehnica Bucureşti - Facultatea de Automatică şi Calculatoare

Verificarea revocarii Certificatelor



Verificare certificate

verifica certificat
verifica CRL
repeat
    verifica certificatul pentru CA
    verifica CRL al CA
until radacina

Securitatea Comunicatiei

- IPsec
- Ziduri de protectie (Firewalls)
- Virtual Private Networks

IP Security Protocol - IPSec

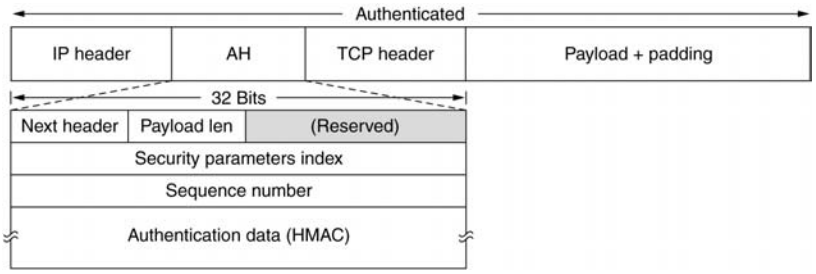
- Implementat la nivel IP
- Suporta autentificarea si confidentialitatea
- Bazat pe Security Association
  - **SA** = relatie **one-way** intre transmitator si receptor, cu servicii de securizarea traficului
  - set de parametri de securitate pentru comunicare
    - algoritmul de criptare si modul (ex. DES in mod block-chaining)
    - cheia de criptare
    - parmetrii de criptare (ex. Initialization Vector)
    - protocolul de autentificare si cheia
    - durata de viata a unei asociatii (permite sesiuni lungi cu schimbarea cheii daca este necesar)
    - adresa capatului opus al asociatiei
    - nivelul de senzitivitate al datelor protejate.
  - pentru relatie bilaterala – 2 SA

SA Database

- Doua protocoale de securitate:
  - protocol de autentificare - AH (Authentication Header)
  - protocol combinat criptare/autentificare - ESP (Encapsulating Security Payload)
- Un sistem pastreaza o baza de date cu asociatiile de securitate
  - include parametrii de securitate (slide precedent) si
  - **contor** numere de secventa: pentru antete AH si ESP
  - Indicator **overflow** pentru contor numere de secventa: ce-i de facut la depasire limita contor
  - fereastra **anti-replay**: determina daca un pachet este o copie
  - **Path MTU**: path Maximum Transmission Unit (pentru evitare fragmentare)
- Fiecare intrare unic identificata de:
  - **Security Parameters Index (SPI)**: identificare SA la receptor
  - **IP Destination Address**
  - **Security Protocol Identifier**: AH sau ESP

Universitatea Politehnica Bucureşti - Facultatea de Automatică şi Calculatoare

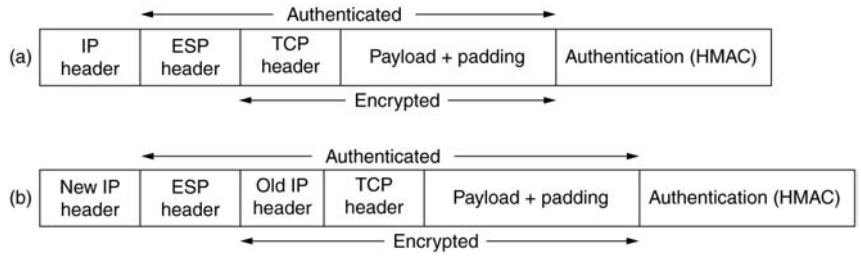
Protocol AH – in mod transport pentru IPv4



Authentication Header – inserat in datagrama IP

- Next header – val camp protocol din IP header inlocuita cu 51
- Payload len – lungime AH (nr cuvinte 32 biti) minus 2
- Security Parameter Index – indica inregistrarea din BD a receptorului
- Sequence number - evitare atacuri prin replica
- HMAC – Hashed Message Authentication Code
  - Utilizeaza cheia simetrica
  - Calculeaza rezumat peste intreaga datagrama (campurile variabile neincluse) + cheia simetrica

ESP in modurile transport si tunel



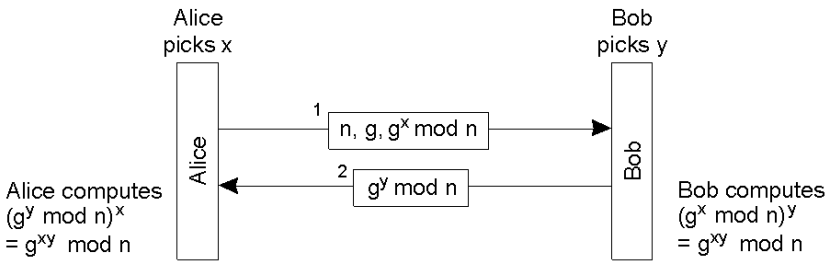
ESP – Encapsulating Security Payload
(a) ESP in mod transport. (b) ESP in mod tunel.

ESP header include
- Security Parameters Index
- Numar de Secventa
- **Vector de initalizare** (pentru criptare date)

La sfarsit: HMAC – Hashed Message Authentication Code

Gestiunea cheilor

- ISAKMP – Internet Security Association Key Management Protocol
- Genereaza o cheie distincta pentru fiecare asociatie
- Implementat cu IKE (ISAKMP Key Excnange)
  - Foloseste Diffie – Hellman
- Pentru Alice:
  - x este cheia privata
  - $g^x \bmod n$ este cheia publica
  - $K_{A,B} = g^{xy} \bmod n$ este cheia secreta partajata cu Bob



Algoritmi IPSEC

- IPSec permite unui sistem sa
  - selecteze protocoalele de securitate,
  - determine algoritmii folositi
  - aleaga cheile criptografice
- Algoritmi folositi
  - DES in mod CBC pentru criptare
  - HMAC/MD5 si HMAC/SHA (trunchiat la 96 biti) pentru autentificare
- Alti algoritmi adaugati in versiuni mai noi
  - 3DES
  - Blowfish
  - CAST-128
  - IDEA
  - RC5

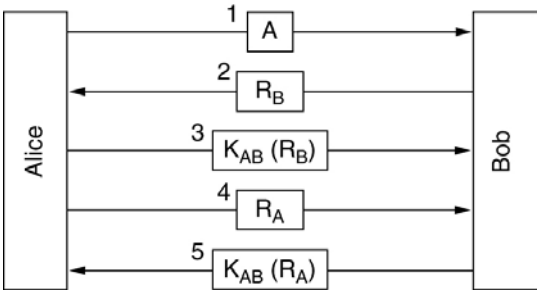
Universitatea Politehnica Bucureşti - Facultatea de Automatică şi Calculatoare

Protocoale de Autentificare

Folosesc

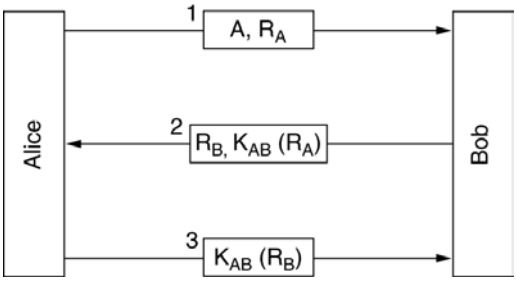
- Cheie secreta partajata
- Stabilirea unei chei partajate: Diffie-Hellman
- KDC - Key Distribution Center
- Kerberos
- Public-Key Cryptography

Autentificare cu cheie secreta partajata



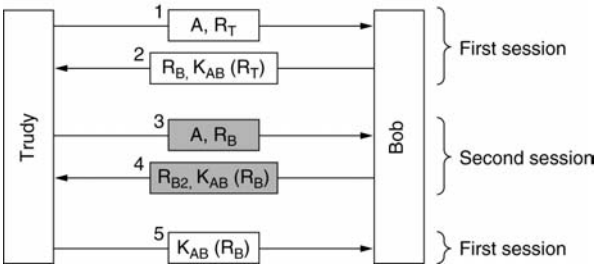
Autentificare reciproca cu un protocol challenge-response

Autentificare cu cheie secreta partajata (2)



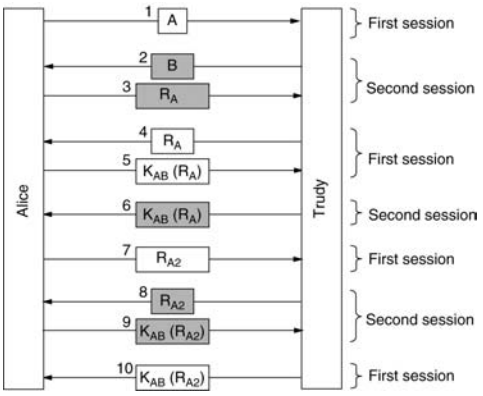
Reducere numar de pasi

Autentificare cu cheie secreta partajata (3)



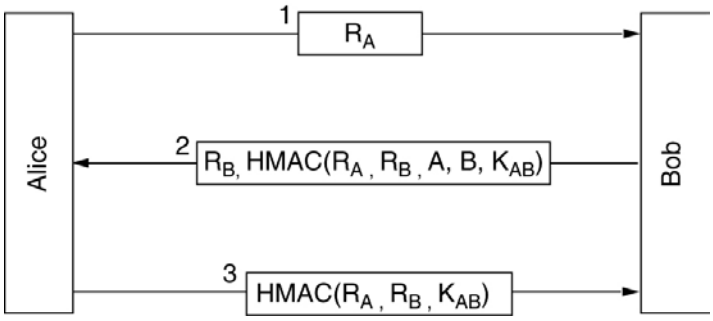
Atacul prin reflexie

Autentificare cu cheie secreta partajata (4)

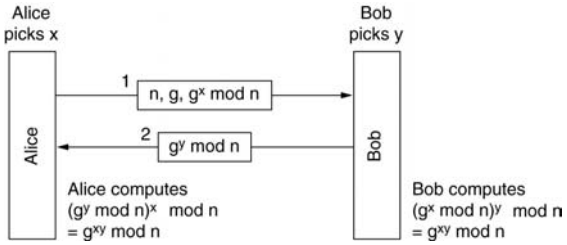


Atacul prin reflexie pe protocolul initial

Autentificarea cu HMACs



Stabilire cheie partajata: Diffie-Hellman

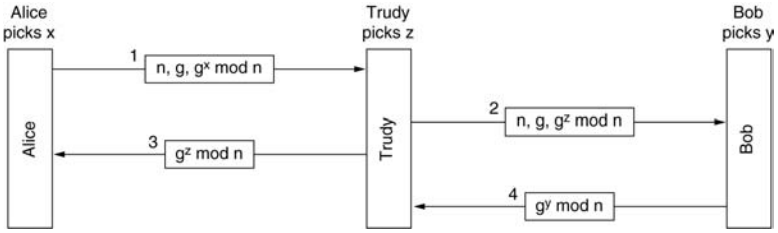


n, g – numere mari
n prim
(n-1)/2 prim

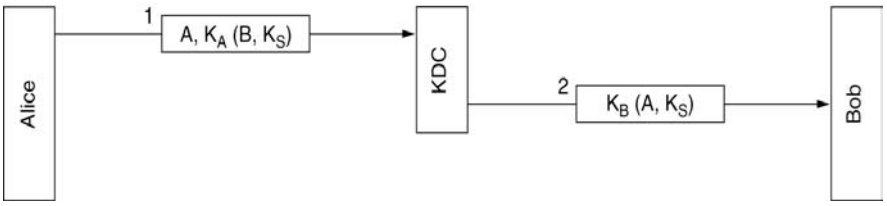
x nu poate fi calculat din $g^x \bmod n$
$g^{xy} \bmod n$ nu poate fi calculat din $g^x \bmod n$ si $g^y \bmod n$ cand n este mare

g < n (generator) are proprietatea:
pentru fiecare *p* intre 1 si *n*-1 inclusiv, exista o putere *k* a lui *g* astfel ca $p = g^k \bmod n$.

Atacul man-in-the-middle



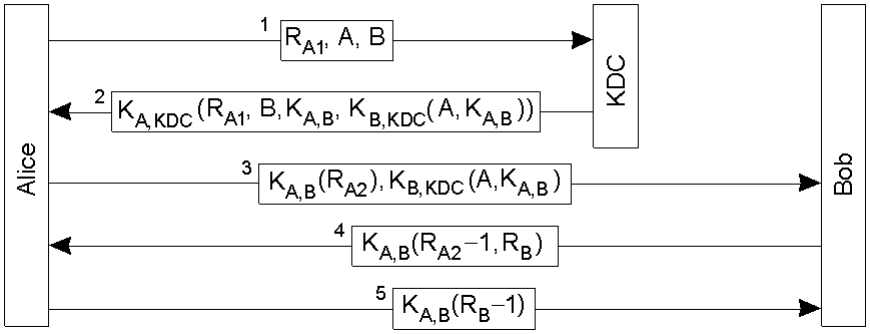
Autentificarea folosind Key Distribution Center



Prima incercare

Vulnerabil la replay attack – Trudy retransmite mesajul 2 (si un mesaj asociat criptat cu K_S)

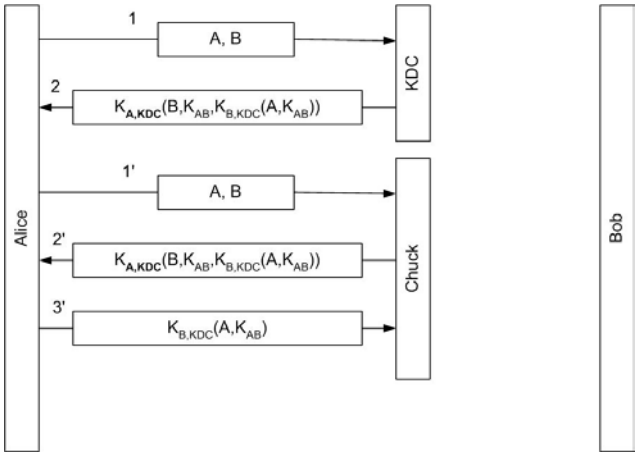
Autentificarea folosind Key Distribution Center (3)



Protocolul Needham-Schroeder

- Forma mai complexa de folosire a tichetelor
- R_{A1}, R_{A2}, R_B, - "leaga" doua mesaje intre ele

Needham-Schroeder fara "nonce"

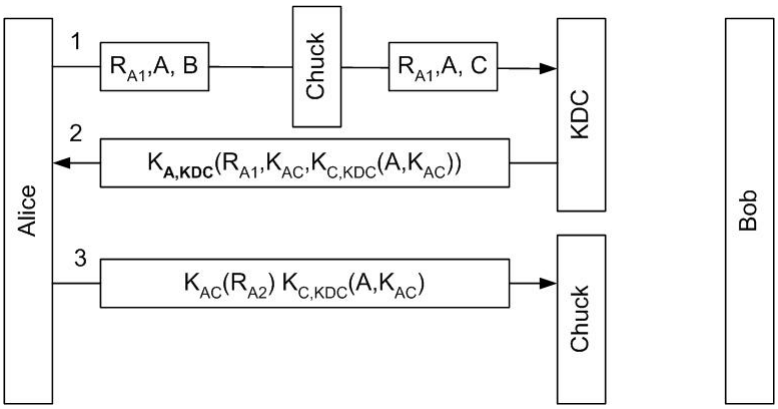


Chuck fura cheia $K_{B,KCD}$ si intercepteaza mesajul 2

Intre timp, Bob a negociat o alta cheie secreta cu KDC, $K^{new}_{B,KCD}$

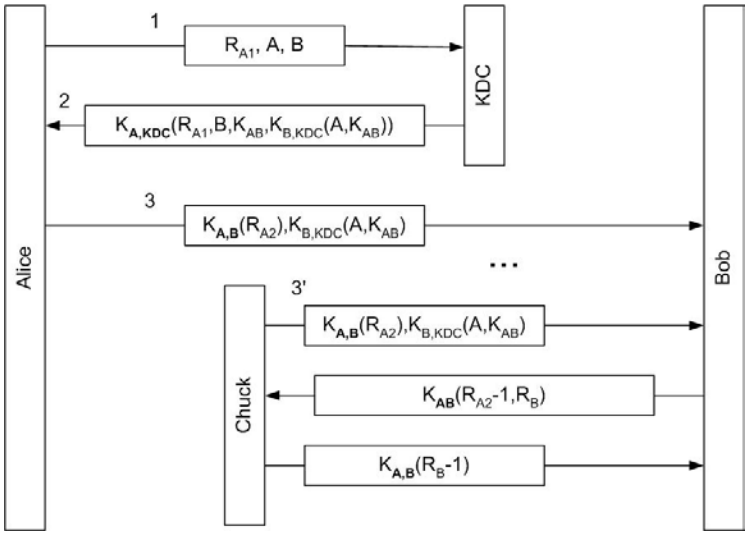
La o noua incercare a lui Alice (1') rejoaca 2 (2') si afla K_{AB}

Needham-Schroeder fara B



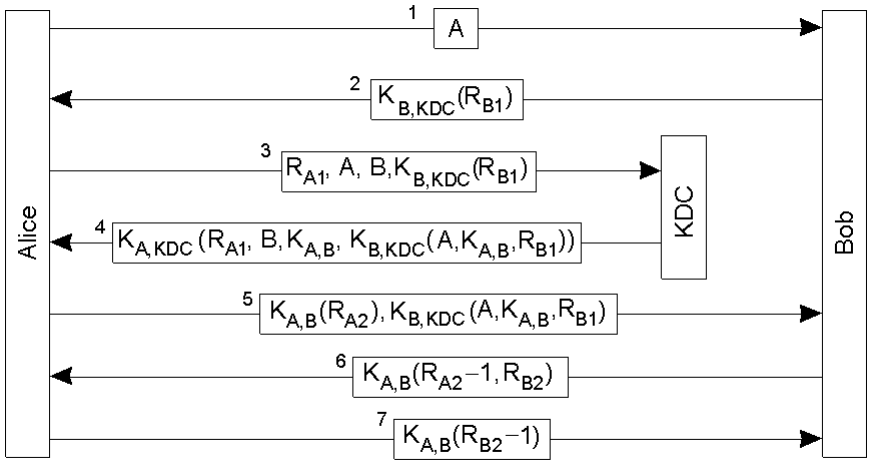
Chuk inlocuieste B in mesajul 1 si o pacaleste pe Alice

Slabiciune Needham-Schroeder



Chuck afla cheia K_{AB} si rejoaca mesajul 3

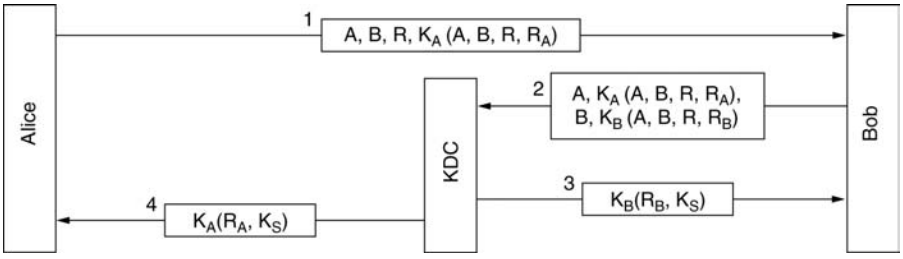
Autentificarea folosind Key Distribution Center (3)



Protectie contra reutilizarii unei chei de sesiune generata anterior in protocolul Needham-Schroeder.

Universitatea Politehnica Bucureşti - Facultatea de Automatică şi Calculatoare

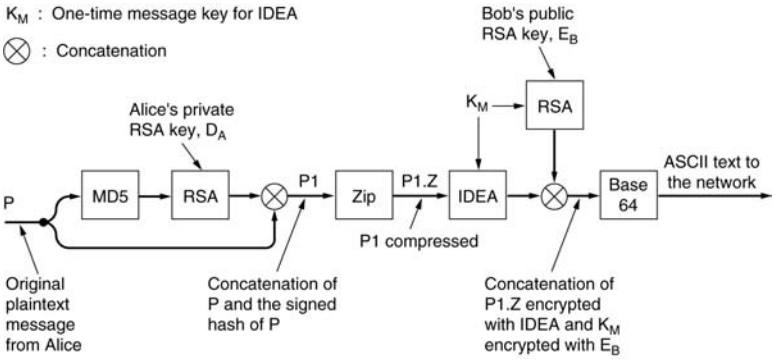
Autentificarea folosind Key Distribution Center (4)



Protocolul Otway-Rees (simplificat).

Problema: Alice ar putea folosi cheia secreta inainte ca Bob sa afle de ea

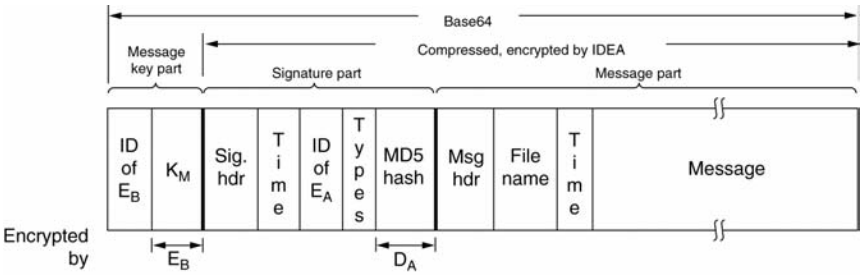
Securitatea E-Mail - PGP – Pretty Good Privacy



Folosirea PGP pentru a trimite un mesaj.

Autor: Phil Zimmermann
Cripteaza date folosind IDEA (International Data Encryption Algorithm)
K_M cheie de sesiune 128-biti produsa dintr-un text introdus de Alice

PGP – Pretty Good Privacy (2)



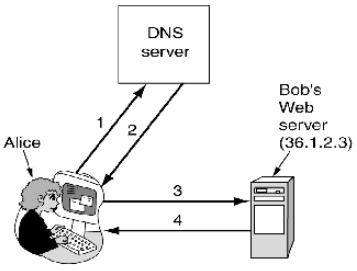
Mesaj PGP.

ID E_B – B poate avea mai multe chei
Types – identifica algoritmul de criptare
File name – nume implicit al fisierului de utilizat la receptie
Management chei
- **Private key ring (key, identifier)**
- **Public key ring (key, trust indicator)**
- **Versiunile actuale PGP folosesc certificate X.509**

Securitatea Web

- Atacuri
  - inlocuire Home page
  - Denial-of-service
  - Citire mail-uri
  - Furt numere credit card
- Solutii
  - Secure Naming
  - SSL – The Secure Sockets Layer

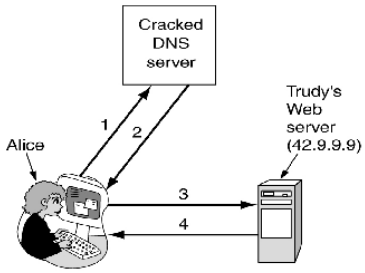
Secure Naming



1. Give me Bob's IP address
2. 36.1.2.3 (Bob's IP address)
3. GET index.html
4. Bob's home page

(a)

Situatie Normala.

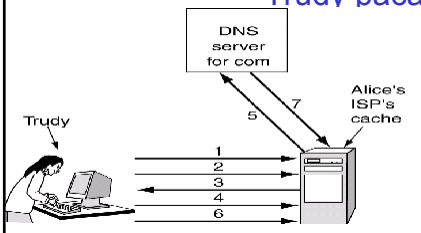


1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page

(b)

Un atac bazat pe modificarea inregistrarii lui Bob in DNS.

Trudy pacaleste ISP-ul lui Alice



•DNS foloseste **sequence numbers** (pentru a mapa cererile si raspunsurile)
- Trudy inregistreaza un domeniu ***trudy-the-intruder.com*** (IP 42.9.9.9) si
- Instaleaza un server ***dns.trudy-the-intruder.com*** (aceeasi IP 42.9.9.9)

1. Cauta adresa ***foobar.trudy-the-intruder.com*** pentru a forta ***dns.trudy-the-intruder.com*** in cache-ul ISP-ului lui Alice
2. Cere ISP-ului ***www.trudy-the-intruder.com***
3. ISP intreaba DNS-ul lui Trudy; intrebarea are un numar de secventa, **n** asteptat de Trudy
4. Repede, cere adresa **bob.com** (fortand ISP sa intrebe serverul **com** in pasul 5)
5. ISP transmite cererea pentru bob.com cu nr secv **n+1**
6. Trudy transmite un raspuns fals: Bob este 42.9.9.9, nr secv = n+1; raspunsul este pus in cache
7. ISP rejecteaza raspunsul adevarat

Secure DNS

Domain name	Time to live	Class	Type	Value
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7B73F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A8B848F5272E53930C...

Un exemplu de RRSet (Resource Record Set) pentru *bob.com*.

Fiecare zona DNS are o pereche de chei public/private

Informatiile trimise sunt semnate cu cheia privata

DNS records sunt grupate in RRSs

Se adauga noi tipuri de inregistrari

***KEY* record – cheia publica a unei zone, utilizator, host, etc.**

***SIG* record - hash semnat (criptat) pentru inregistrari *A* si *KEY* pentru verificare autenticitate.**

Clientii primesc un RRS semnat

aplica cheia publica a zonei pentru a decripta hash-ul

calculeaza hash-ul separat

compara cele doua valori (calculata si decriptata)