Protocoale de Securitate

Rezumate de mesaje, semnaturi digitale si protocoale de securitate

Rezumatele mesajelor

Folosite datorita Proprietatilor utile

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

Functii hash

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

Functii Hash: MD5

MD5 – Message Digest 5

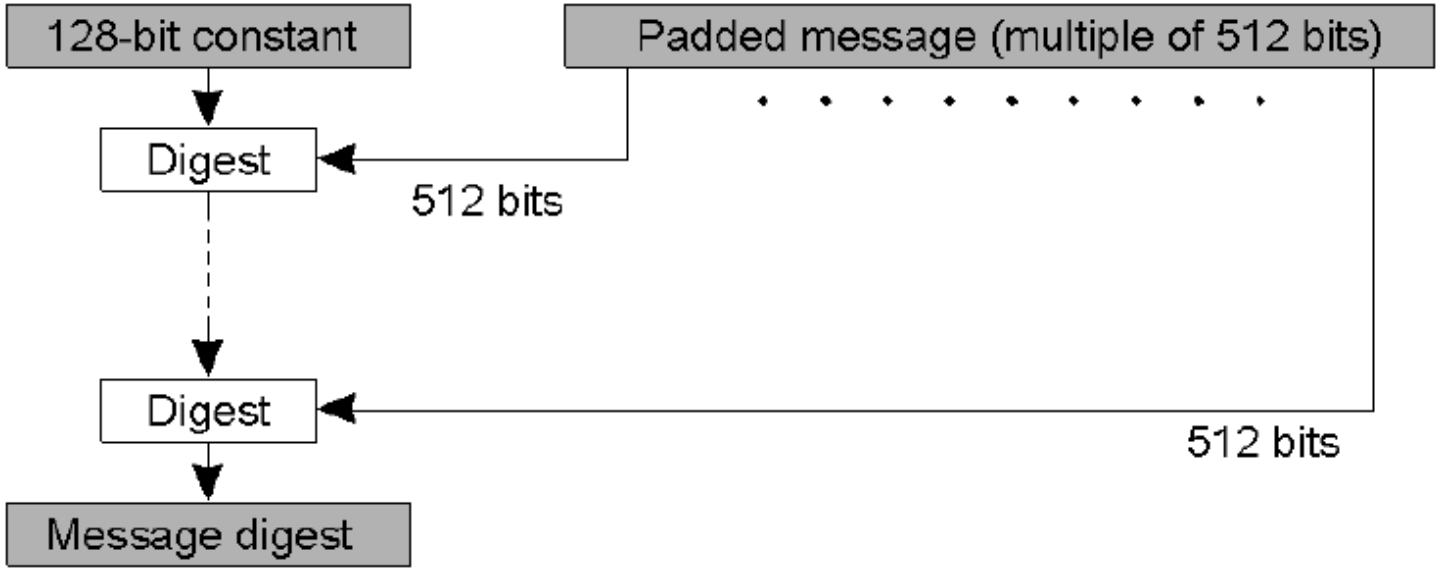
Calculeaza un rezumat de mesaj de 128 biti

Mesajul este completat pana la o lungime de 448 mod 512 biti

Se adauga lungimea originala a mesajului, pe 64 biti

In fiecare faza algoritmul calculeaza un nou rezumat din rezumatul anterior si rezumatul unui bloc de 512 biti.

Primul rezumat este o constanta de 128 biti



Functii Hash: MD5 (2)

O **faza** transforma un **bloc** de mesaj de 512 biti. Are 4 runde.

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))

O runda are 16 **iteratii**.

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

p, q, r, s – variabile *digest*

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

<<< denota rotatie stanga

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

Comentarii

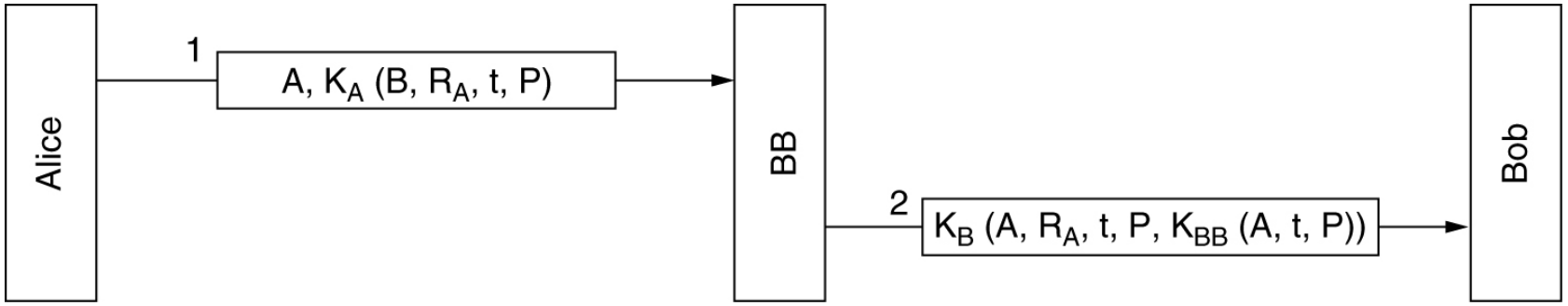
- Rezistenta la coliziuni
  - o functie H este rezistenta la coliziuni daca este foarte greu sa se gaseasca a si b, a#b astfel ca H(a) = H(B)
- In 2004 s-a aratat ca MD5 nu este rezistent la coliziuni
- S-au dezvoltat si recomandat alte functii de hash
  - SHA1, SHA2

- Obs.
  - criptare # rezumare!

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

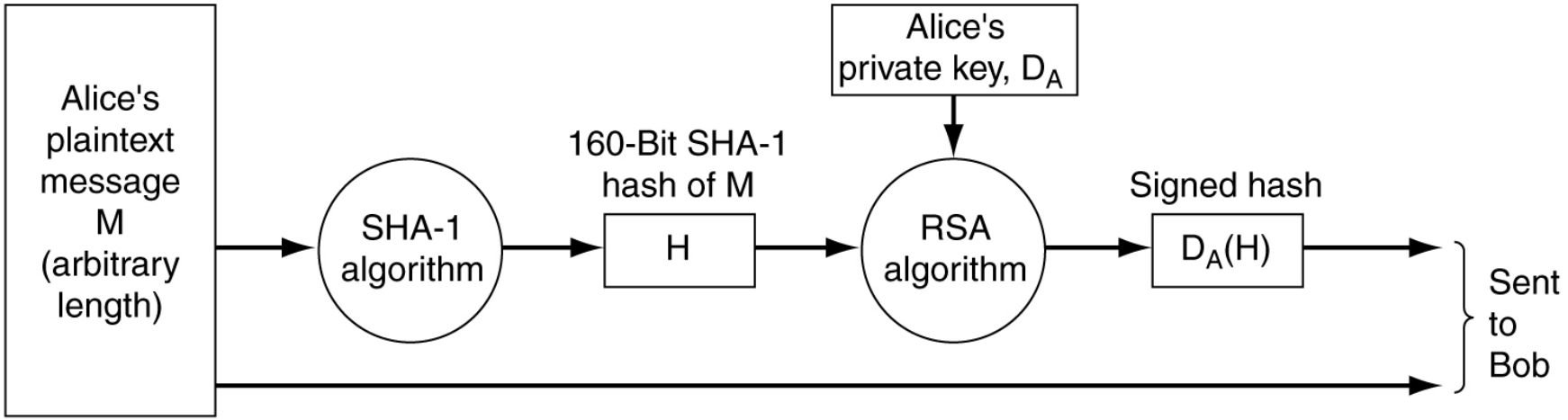
Comentarii

t si R_A folosite ptr. detectie atacuri prin replica unor mesaje vechi

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

Semnaturi cu chei publice

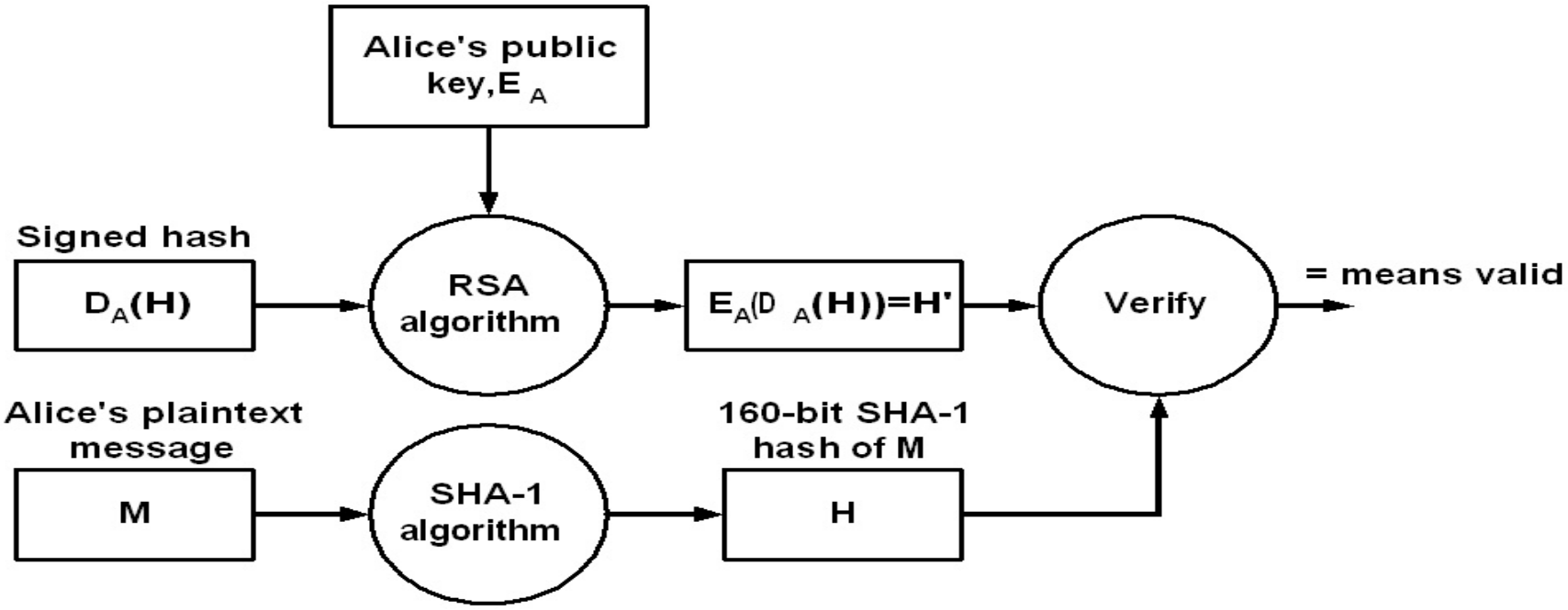
Utilizarea SHA-1 si RSA pentru semnarea mesajelor nesecrete.



Caracteristici

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

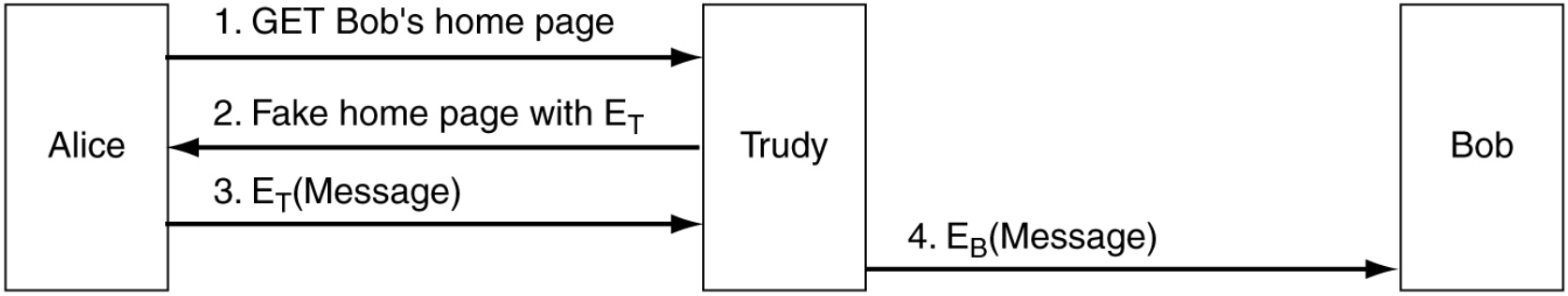
Verificare semnatura digitala



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

Certificate de securitate

- Certificate
  - Asociaza identitatea cu cheia publica
- X.509
  - Standard de certificate

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)

CA cripteaza cu cheia sa privata rezumatul certificatului

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

Campurile de baza dintr-un certificat X.509

Câmp	Semnificatie
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 (ex. MD5 cu RSA)
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 (ex. RSA)**
ID emitent	Un ID opţional identificând în mod unic emitentul certificatului (nume X.500 sau DNS)
ID subiect	Un ID opţional 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 asigura utilizarea corecta a tehnologiei de chei publice
  - programele,
  - echipamentele,
  - tehnologiile de criptare si
  - serviciile de gestiune a infrastructurii criptografice si a cheilor publice ale utilizatorilor.

CA

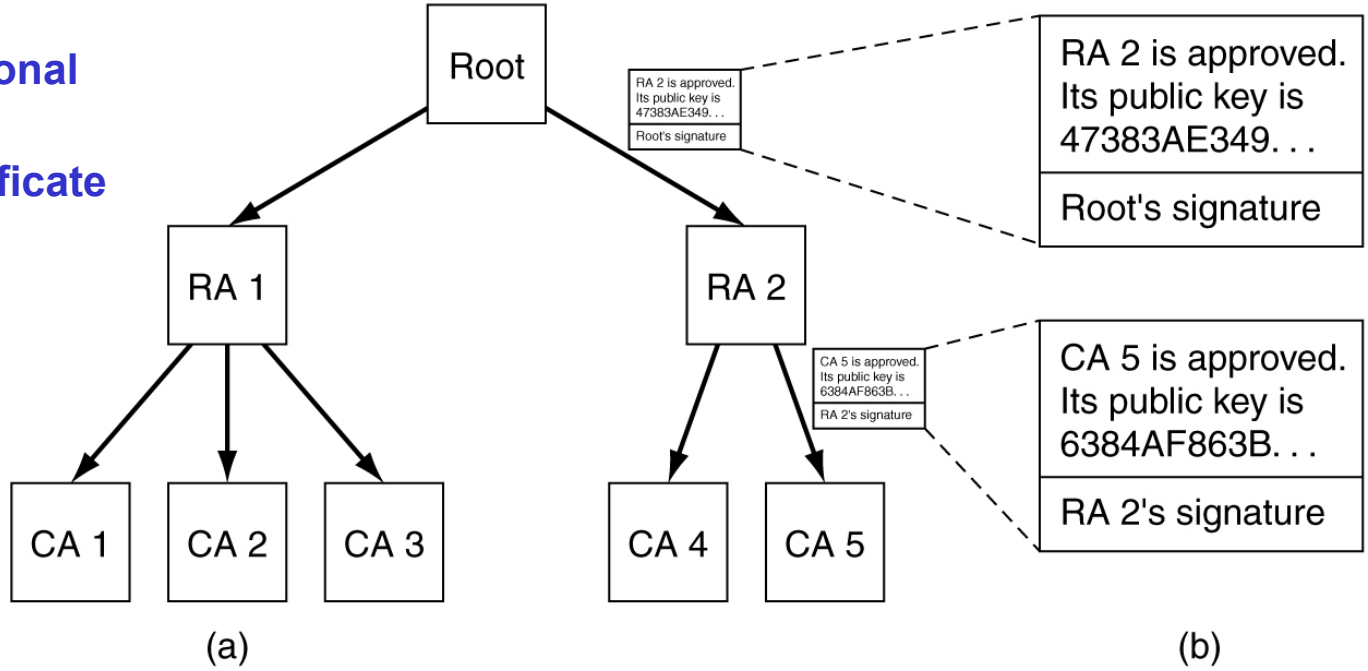
- autoritate de incredere care elibereaza certificate
  - certifica faptul ca cheia publica inclusa apartine persoanei cu numele atasat

- poate fi:
  - organizatie sau companie - pentru angajati
  - universitate - pentru studenti
  - CA publice (VeriSign) - pentru clienti

PKI – verificarea cheilor

RA – Regional Authority

CA – Certificate Authority



(a) PKI ierarhic.

(b) Un lant de incredere (certification path).

A cunoaste si are incredere 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

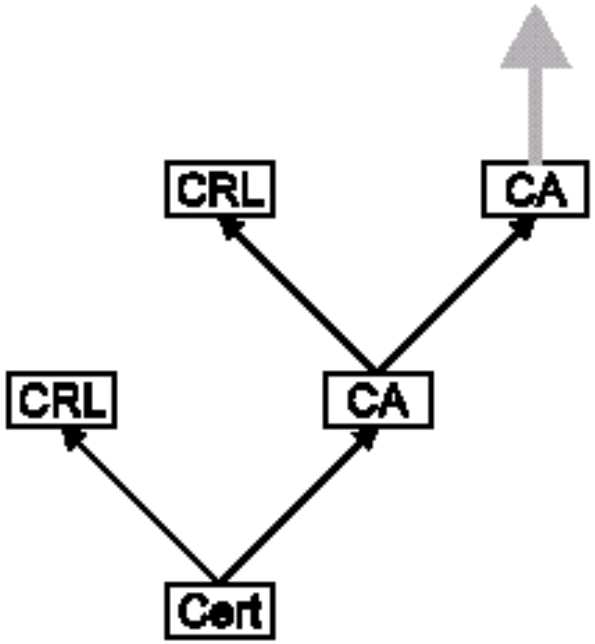
- Un certificat trebuie **revocat** cand:
  - cheia primara este **compromisa**;
  - cheia primara este **pierduta**;
  - o persoana pleaca din companie
  - altele.

- Revocarea trebuie anuntata tuturor utilizatorilor – dificil !
- Alternativa - se folosesc liste de revocare
  - **CRL – Certificate Revocation List**;

Metoda

- se verifica listele de revocare inainte de utilizarea certificatelor
- CRL sunt publicate de CA care a emis certificatele
- Listele pot fi consultate sau duplicate (cache)
  - difuzarea listelor de revocare – prin HTTP, LDAP sau alte protocoale

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
- Ca Security Association - SA
  - legatura securizata unidirectionala intre transmitator si receptor
- Securizarea ambelor sensuri → 2 x SA

Parametri de securitate

- SA nu este legata de un singur algoritm de criptare sau de o singura cheie – se pot specifica:
  - algoritmul si modul de criptare (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.

SA Database

Un sistem pastreaza o baza de date cu asociatiile de securitate

- Pentru fiecare SA pastreaza parametrii de securitate (slide precedent) si

- **contor** numere de secventa: pentru antete de securitate
- 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)

SA Database (2)

Fiecare intrare unic identificata de:

- **Security Parameters Index (SPI)**: identificare SA la receptor
- **IP Destination Address**
- **Security Protocol Identifier**: AH sau ESP

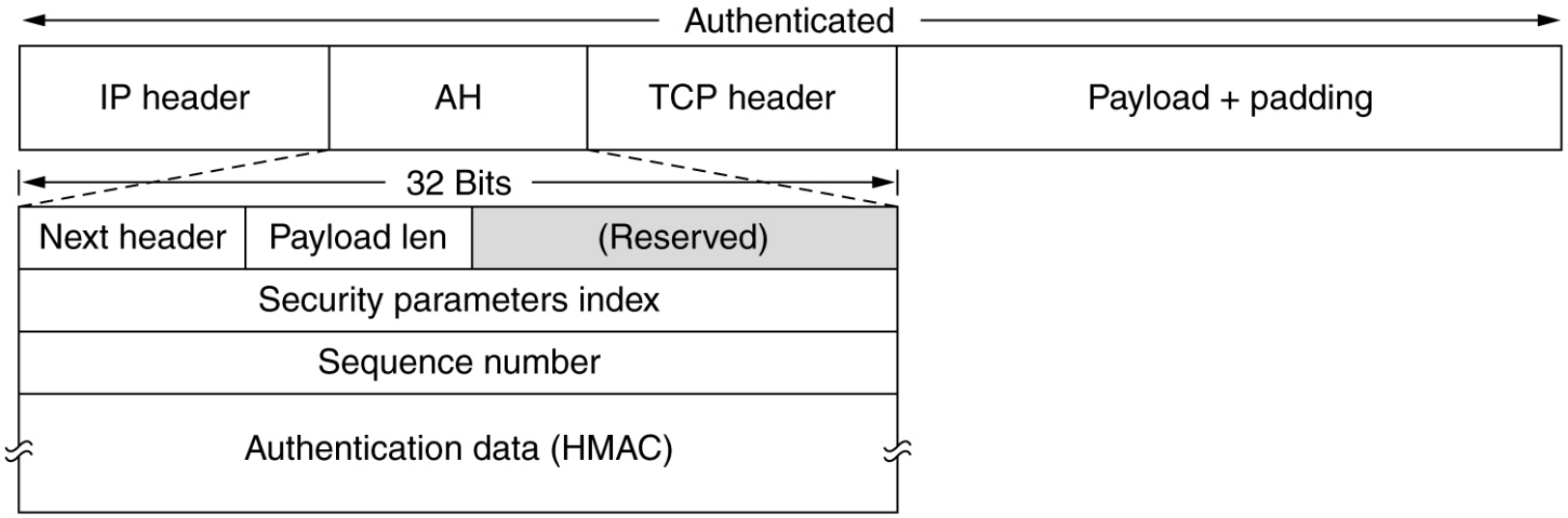
Doua protocoale de securitate:

- AH (Authentication Header) - protocol de autentificare
- ESP (Encapsulating Security Payload) - protocol combinat criptare/autentificare

Si doua moduri de lucru

- transport
- tunel

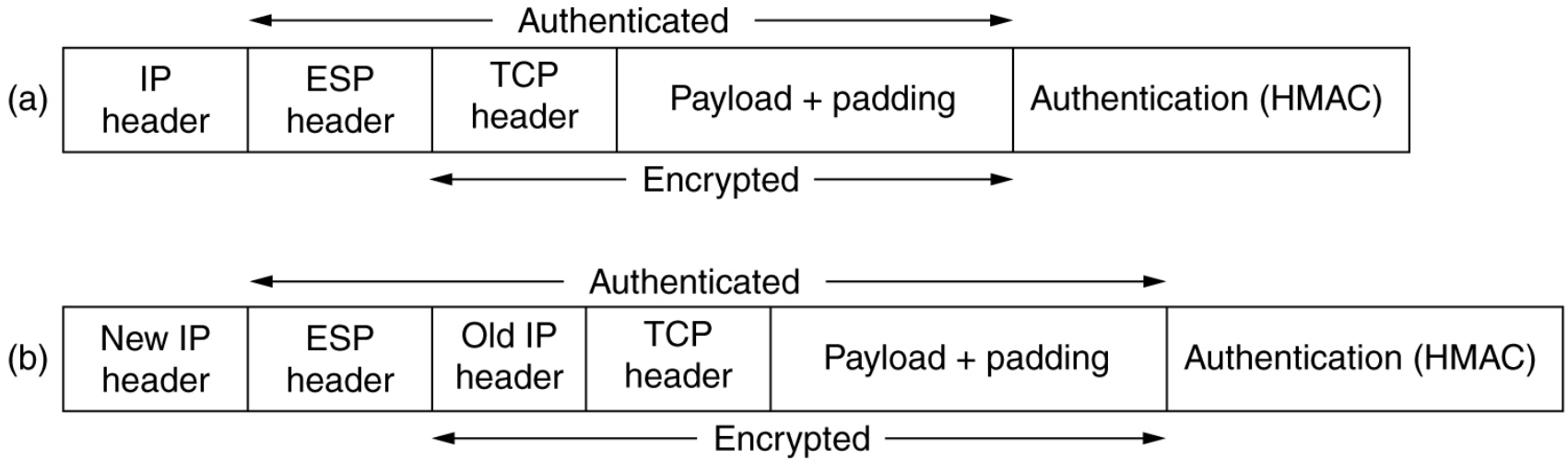
Protocol AH – in mod transport pentru IPv4



Authentication Header – inserat in datagrama IP

- Next header – preluata din IP header unde este 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.

criptarea protejeaza incarcatura; autentificarea protejeaza antet + criptograma

ESP header include

Security Parameters Index

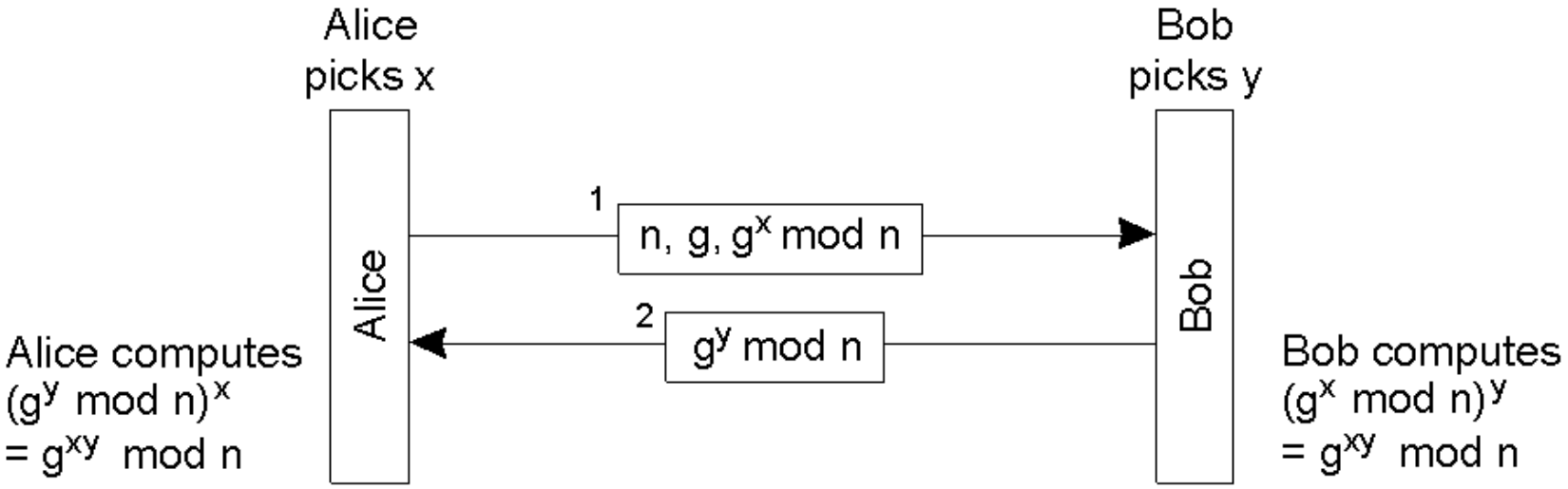
Numar de Secventa

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 Exchange)
  - 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



Caracteristici Protocol IPSEC

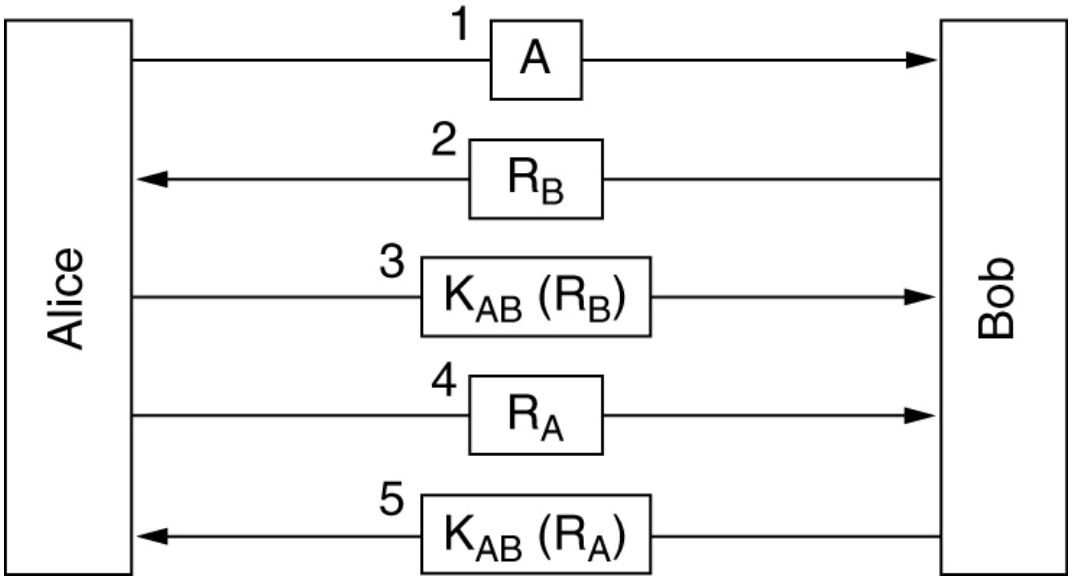
- IPSec este orientat pe conexiune (desi apartine nivelului retea)
- Permite selectia intre mai multi algoritmi
  - criptare: DES in mod CBC, 3DES, IDEA, …
  - autentificare: MD5, SHA (trunchiat la 96 biti)
  - “deschis” la adaugare algoritmi noi
- Permite stabilirea cheilor de criptare
- Permite alegerea intre mai multe servicii
  - confidentialitate
  - integritate
  - protectie la atacuri prin replica
- Permite alegerea granularitatii
  - conexiune TCP
  - toate legaturile intre doua calculatoare (tunel)
  - toate legaturile intre doua rutere, …

Protocoale de Autentificare

Folosesc

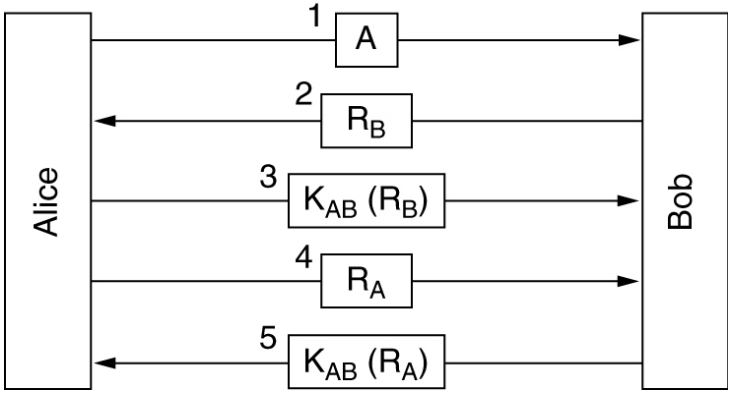
- Cheie secreta partajata
- Stabilirea unei chei partajate: Diffie-Hellman
- KDC - Key Distribution Center
- Kerberos
- Public-Key Cryptography

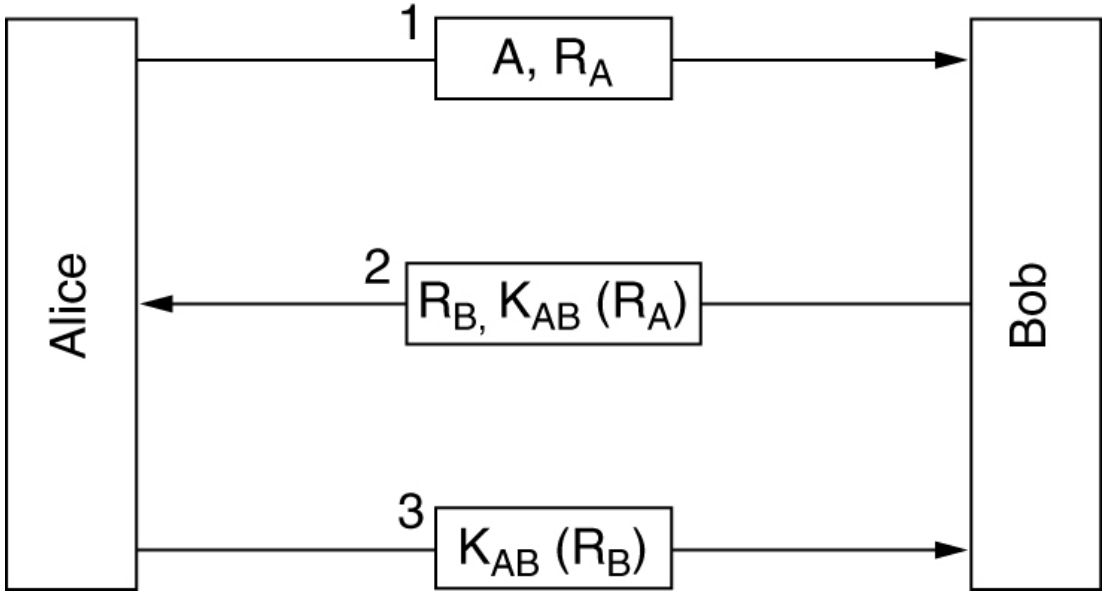
Autentificare cu cheie secreta partajata



Autentificare reciproca cu un protocol challenge-response

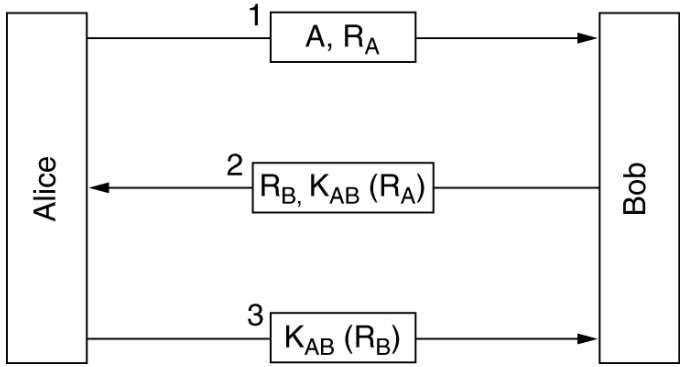
Autentificare cu cheie secreta partajata (2)

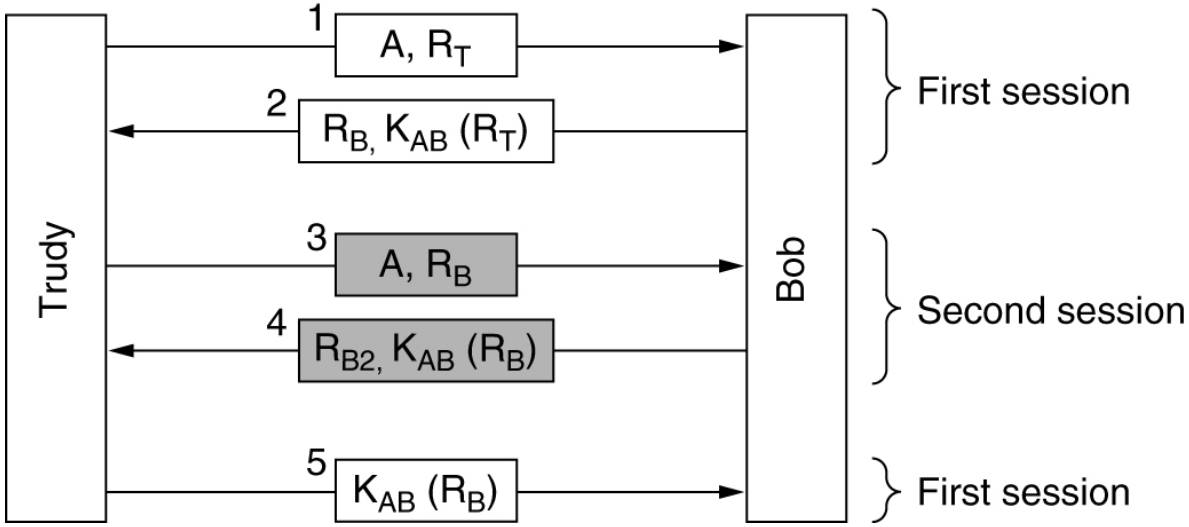




Reducere numar de pasi

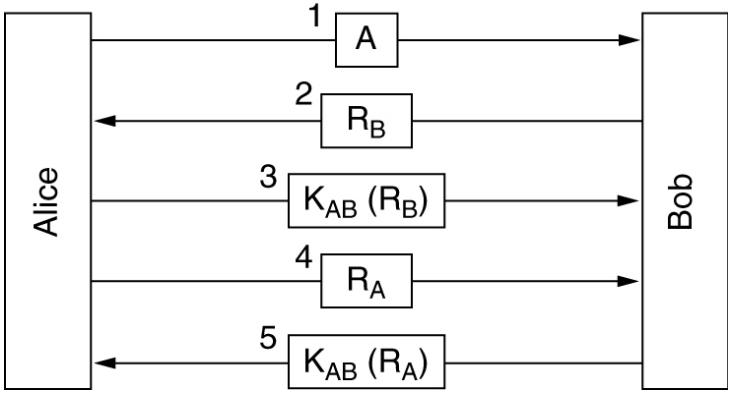
Autentificare cu cheie secreta partajata (3)

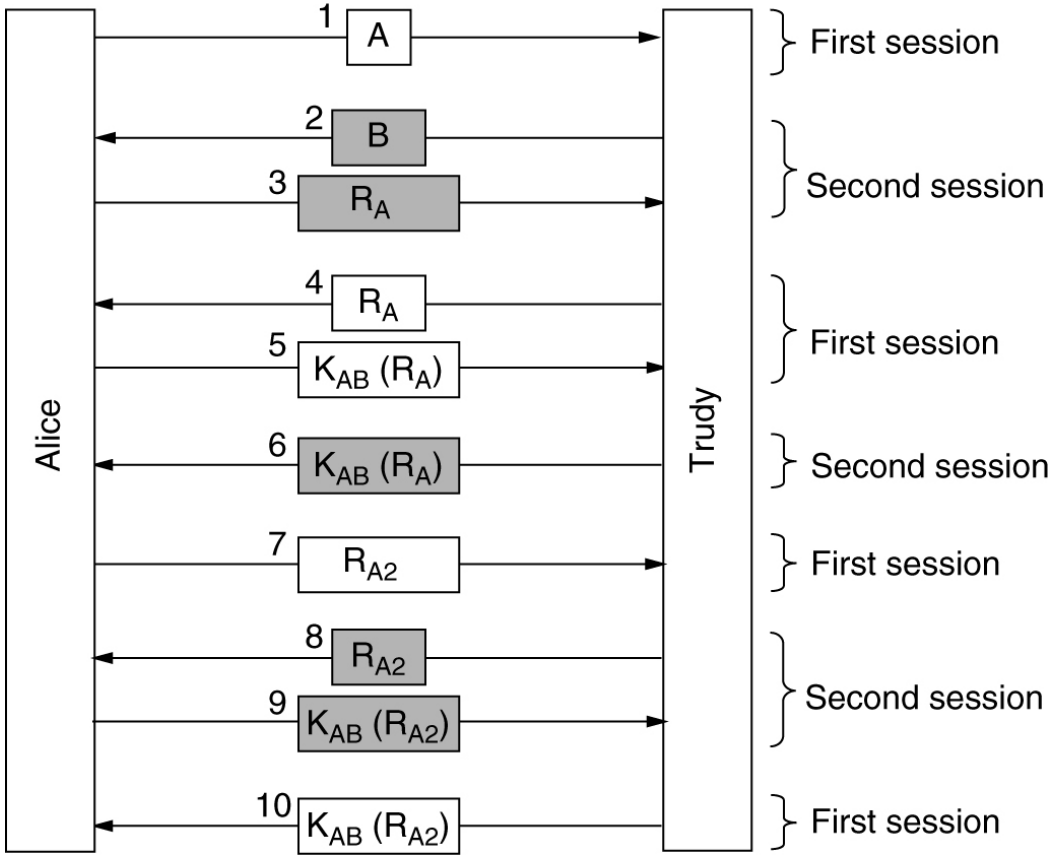




Atacul prin reflexie

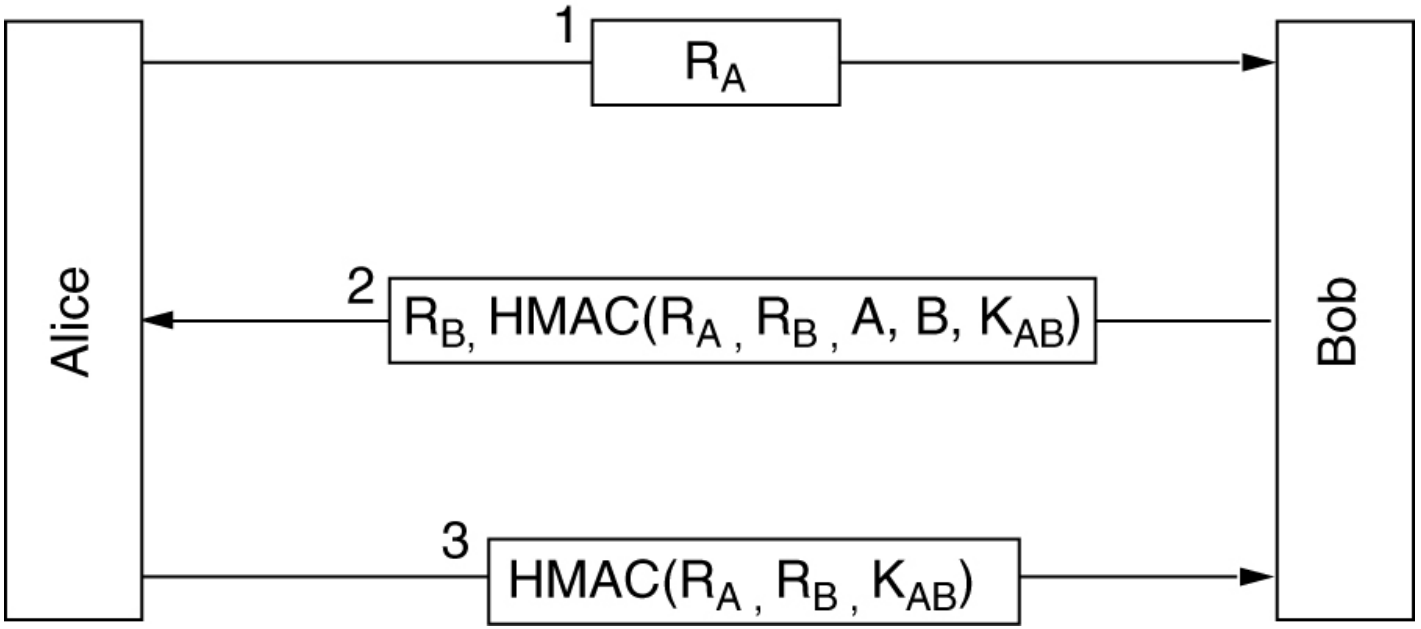
Autentificare cu cheie secreta partajata (4)





Atacul prin reflexie pe protocolul initial

Autentificarea cu HMACs

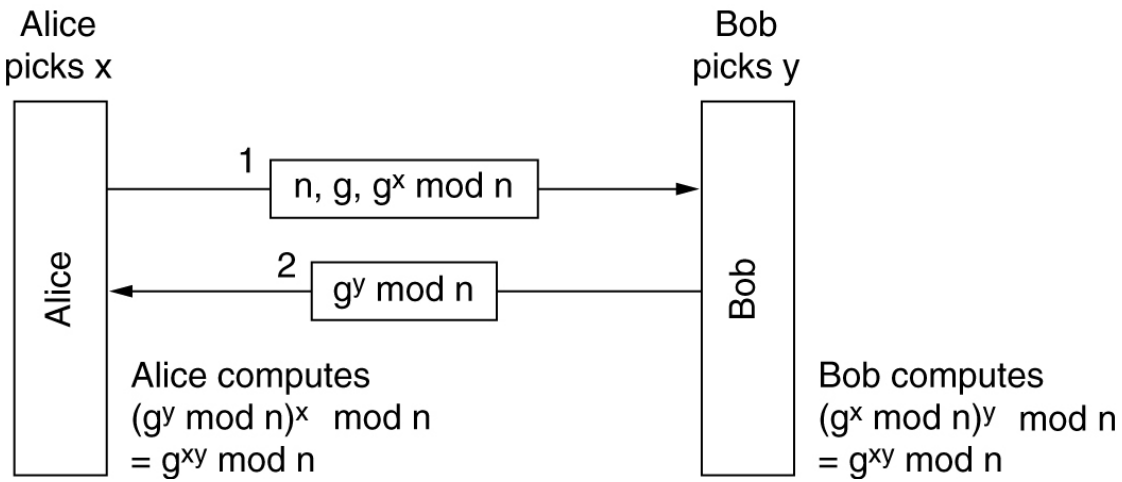


Fiecare parte poate calcula HMAC

- Hash-based Message Authentication Code (de ex. folosind SHA-1)

Trudy nu poate forta criptarea sau rezumarea unei valori impuse de ea

Stabilire cheie partajata: Diffie-Hellman



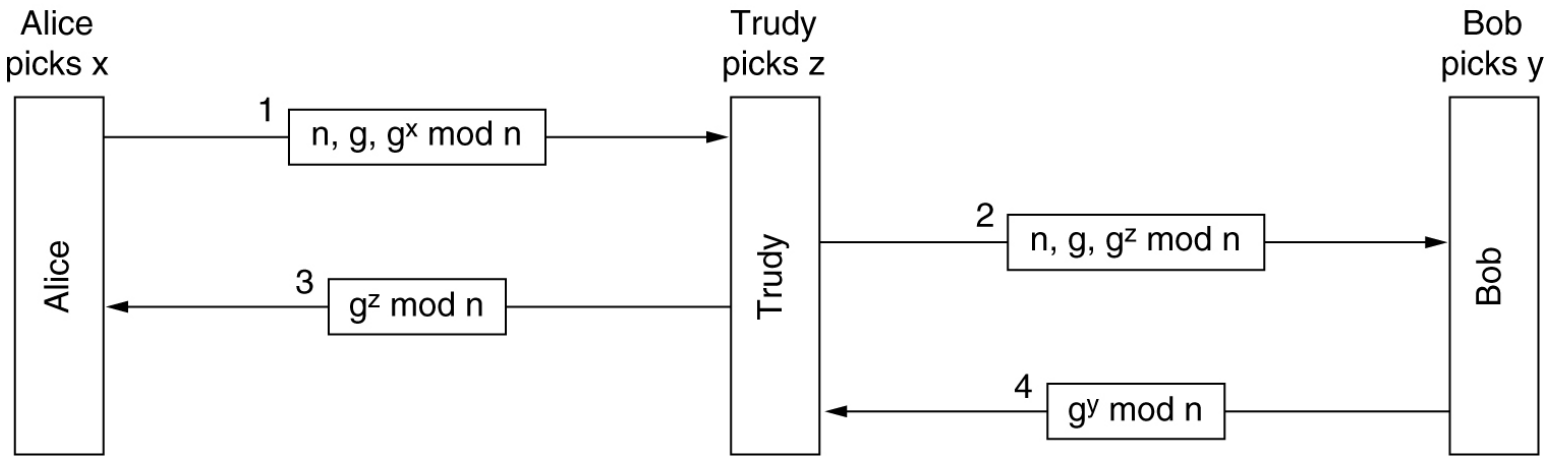
n, g – numere mari
n prim
(n-1)/2 prim

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: orice p poate fi scris ca $g^k \bmod n$

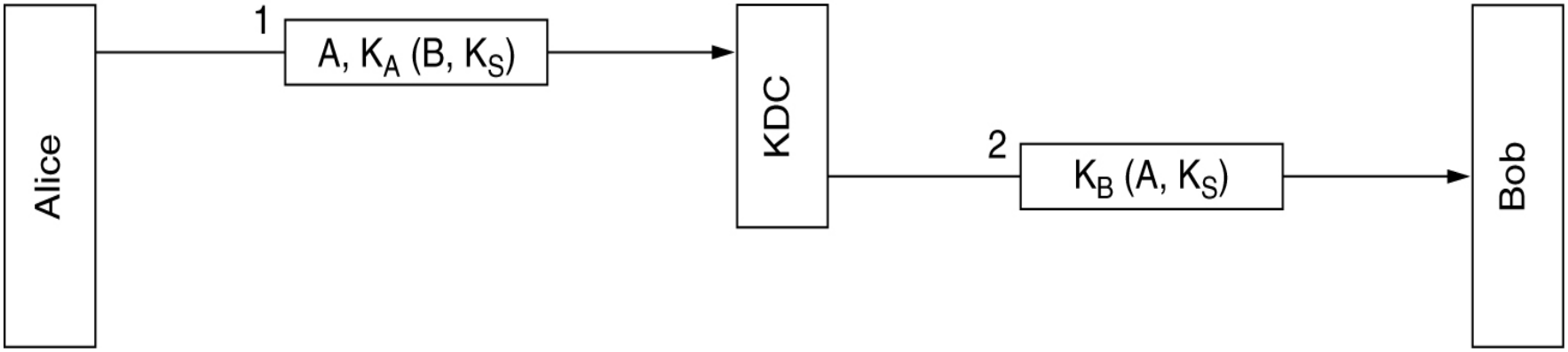
adica: pentru fiecare *p* intre 1 si *n*-1 inclusiv, exista o putere *k* a lui *g* astfel ca $p = g^k \bmod n$.

Atacul man-in-the-middle



posibil deoarece **g** si **n** sunt publici

Autentificarea folosind Key Distribution Center



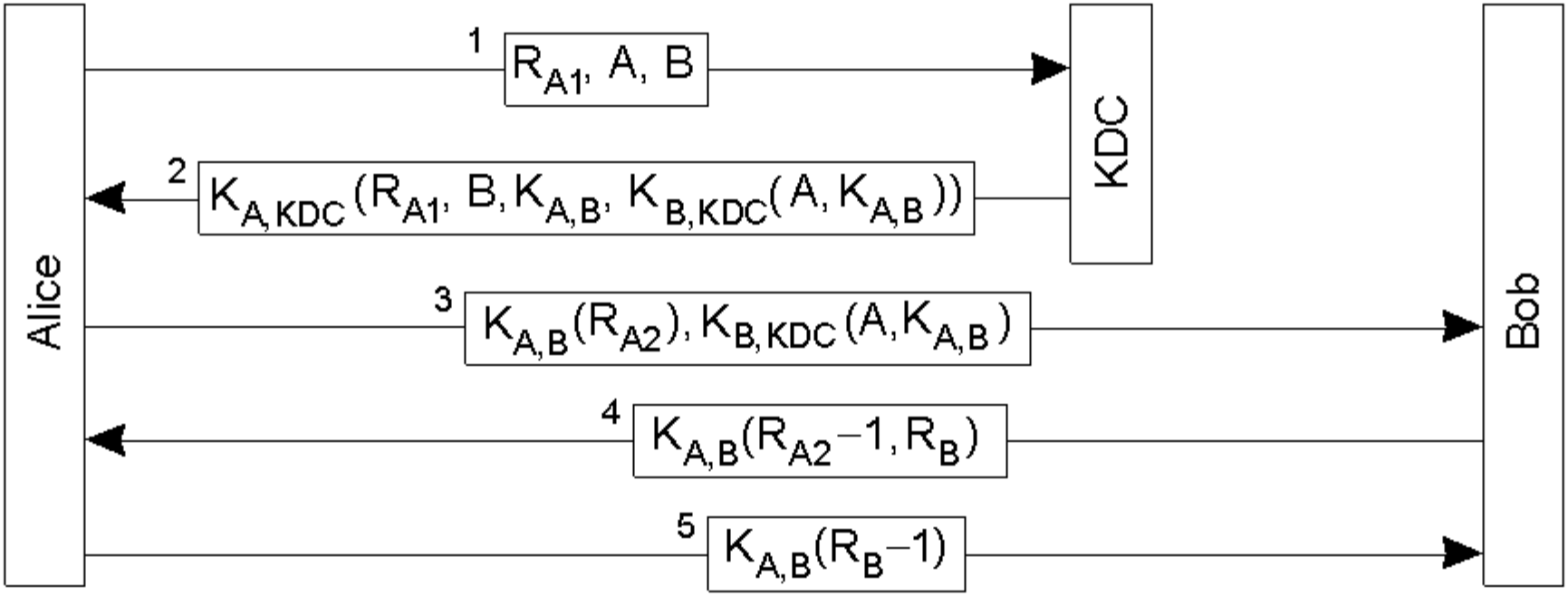
Prima incercare:

Vulnerabil la replay attack

Trudy retransmite mesajul 2 si

un mesaj asociat criptat deja cu K_S (de ex. extragerea unei sume de bani)

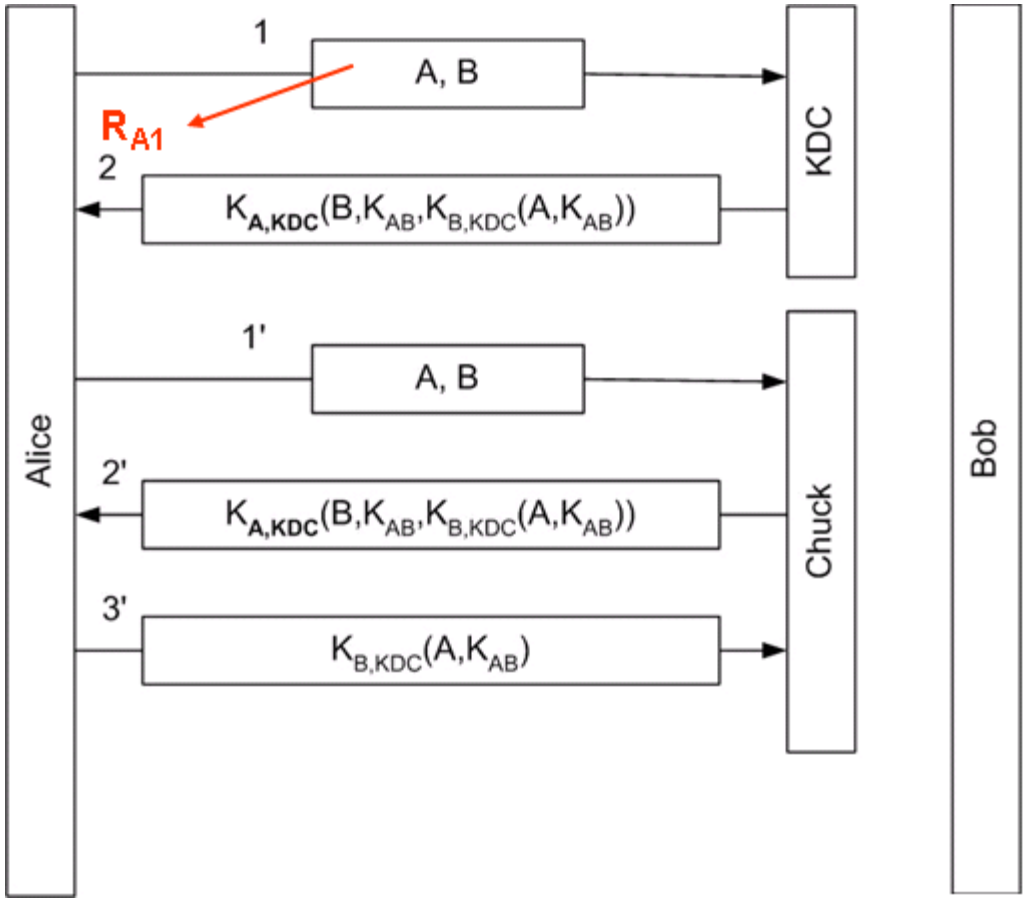
Autentificarea folosind Key Distribution Center (3)

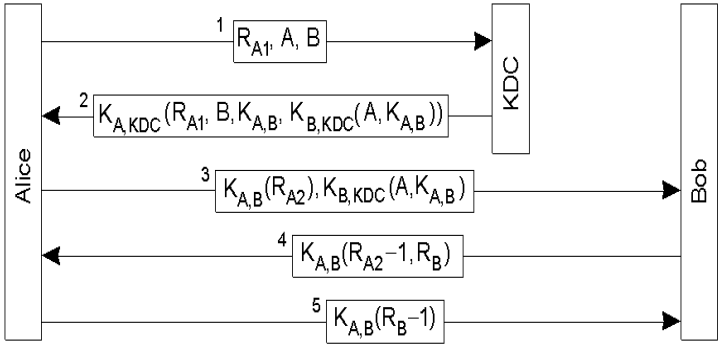


Protocolul Needham-Schroeder

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

Needham-Schroeder fara "nonce"



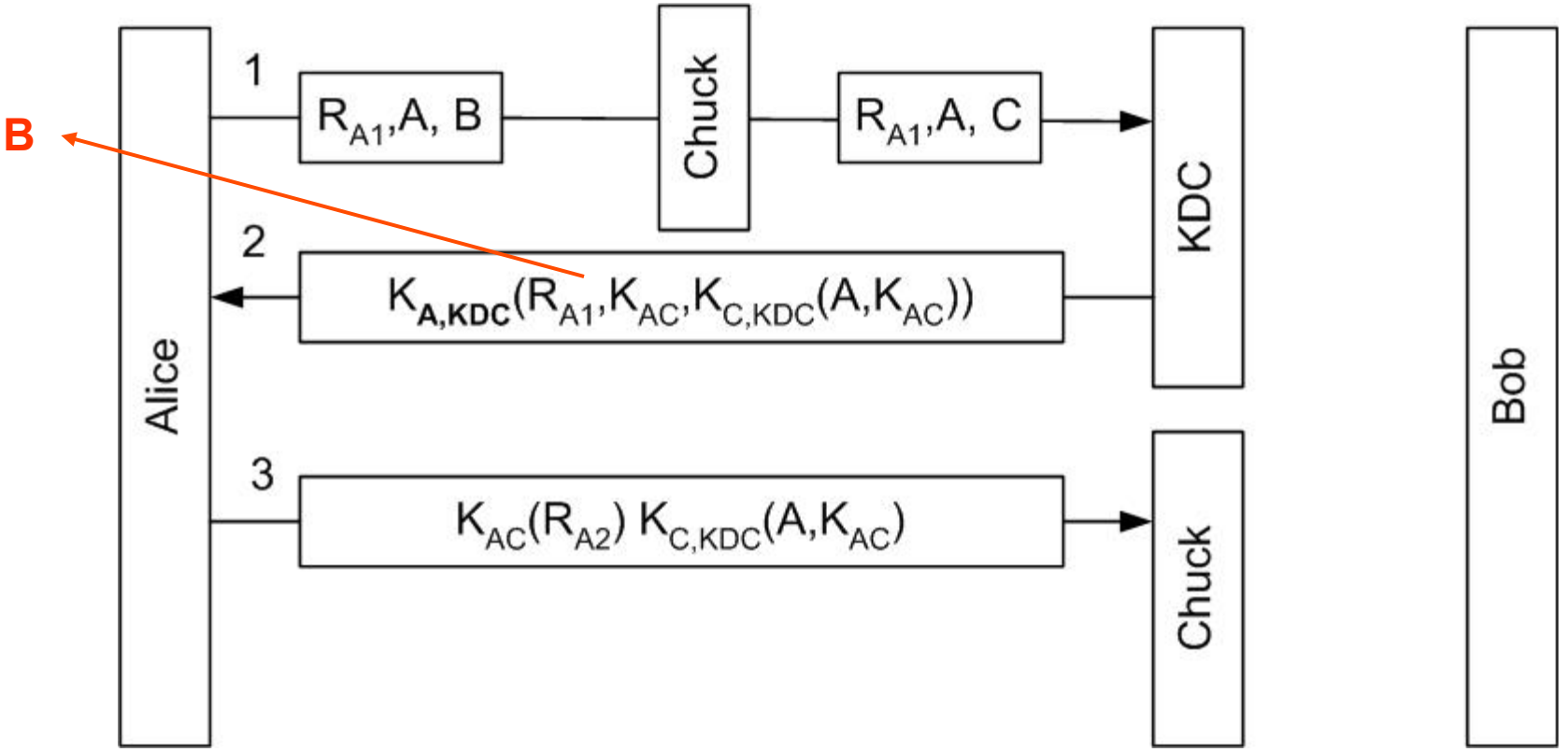


Chuck fura cheia $K_{B,KDC}$ si intercepteaza mesajul 2

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

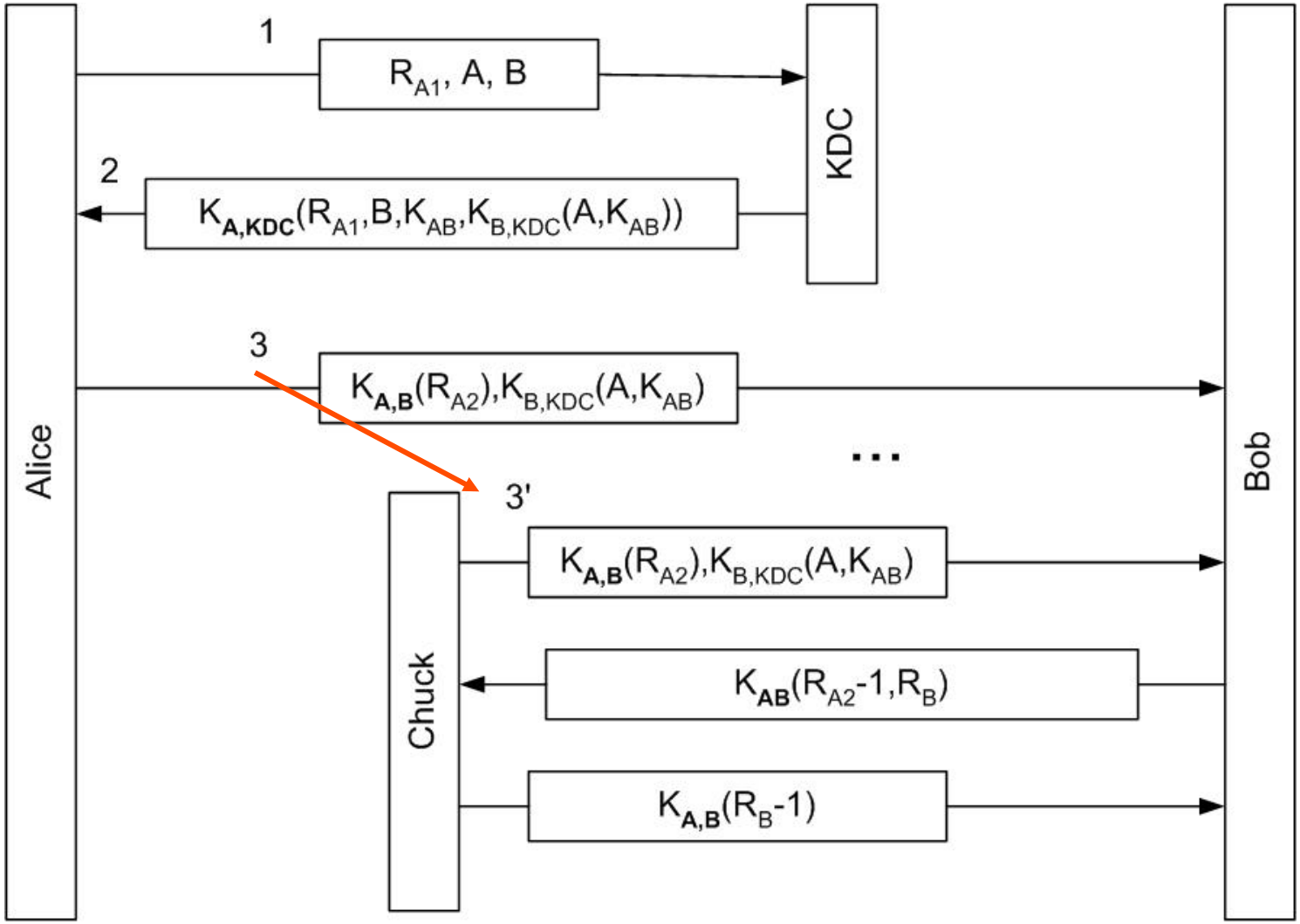
La o noua incercare a lui Alice (1') Chuck rejoaca 2 (2') si afla K_{AB}

Needham-Schroeder fara B



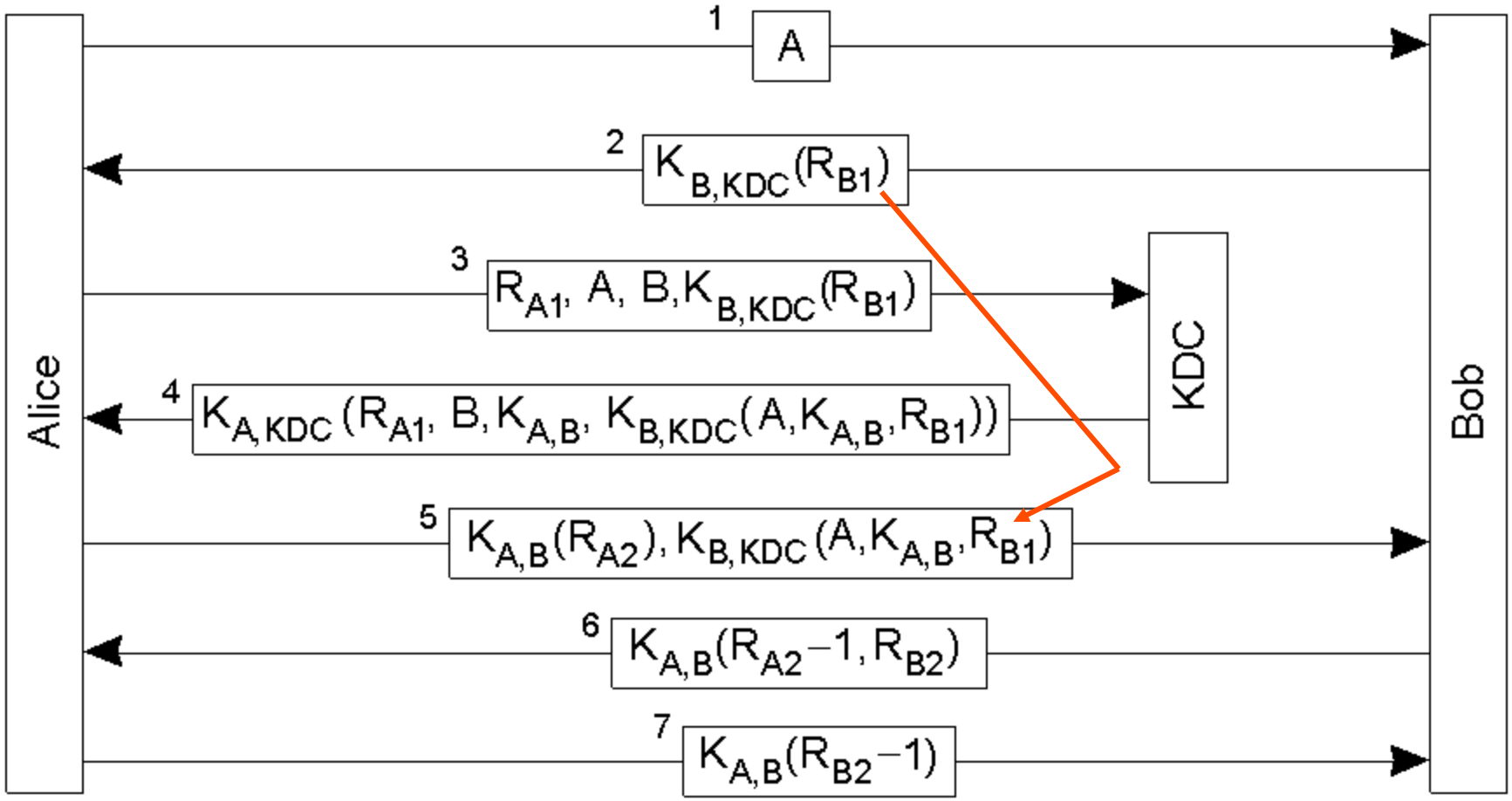
Chuk inlocuieste B in mesajul 1 si o pacaleste pe Alice

Slabiciune Needham-Schroeder



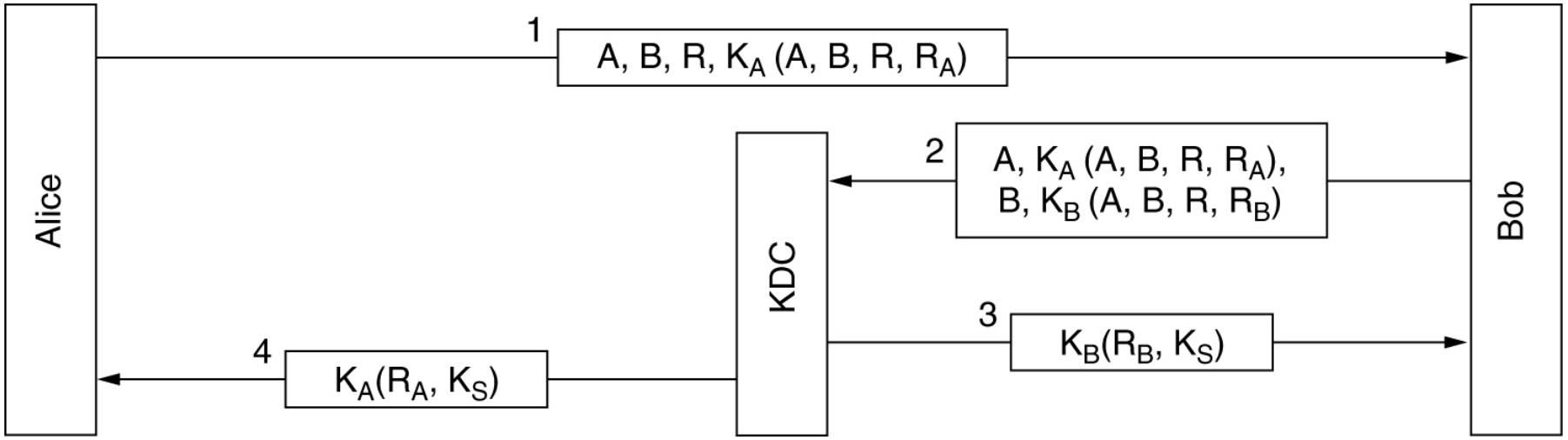
Chuck afla cheia K_{AB} si rejoaca mesajul 3

Autentificarea folosind Key Distribution Center (3)



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

Autentificarea folosind Key Distribution Center (4)



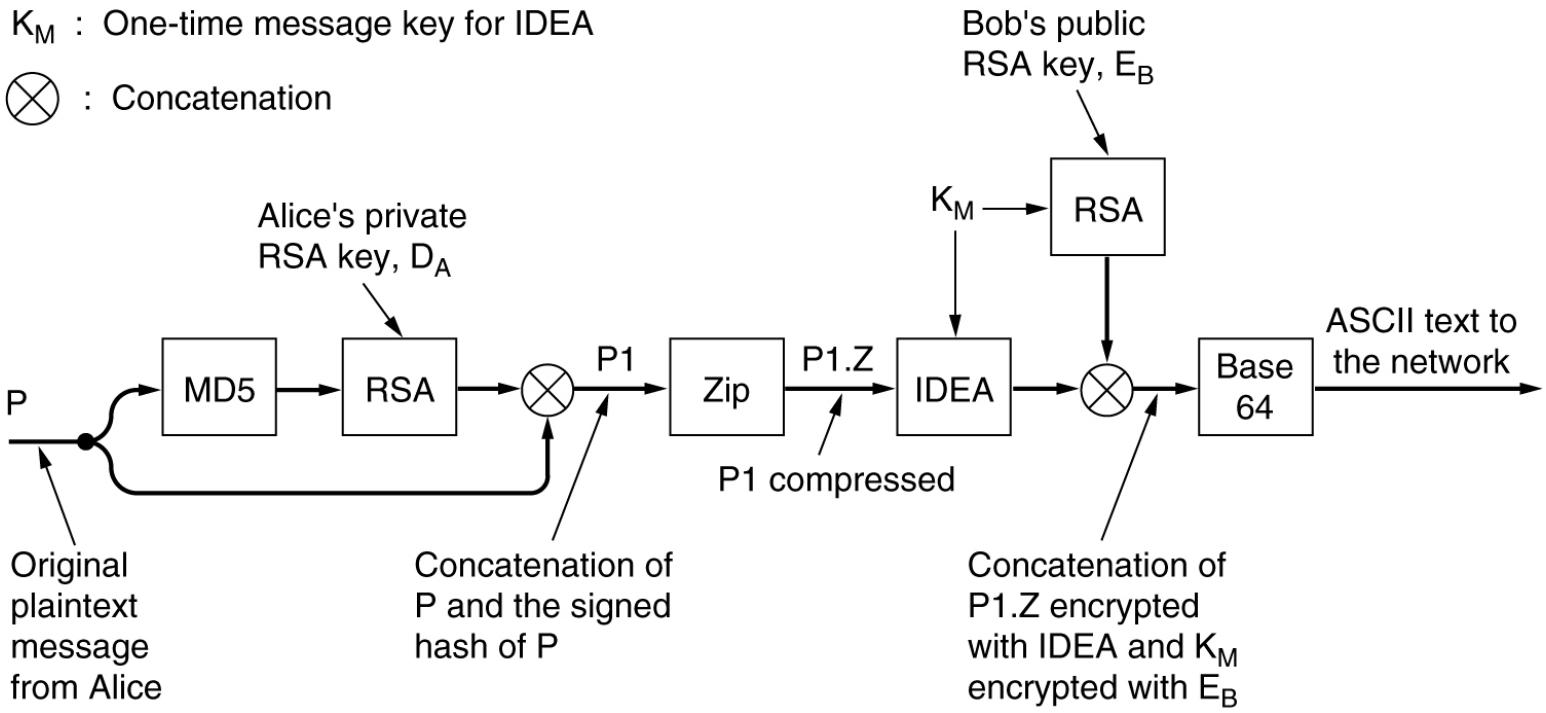
Protocolul Otway-Rees (simplificat).

R – identificator comun, KDC verifica daca R apare in ambele parti criptate ale mesajului 2

R_A, R_B folosite in mesajele 3 si 4

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

Securitatea E-Mail - PGP – Pretty Good Privacy



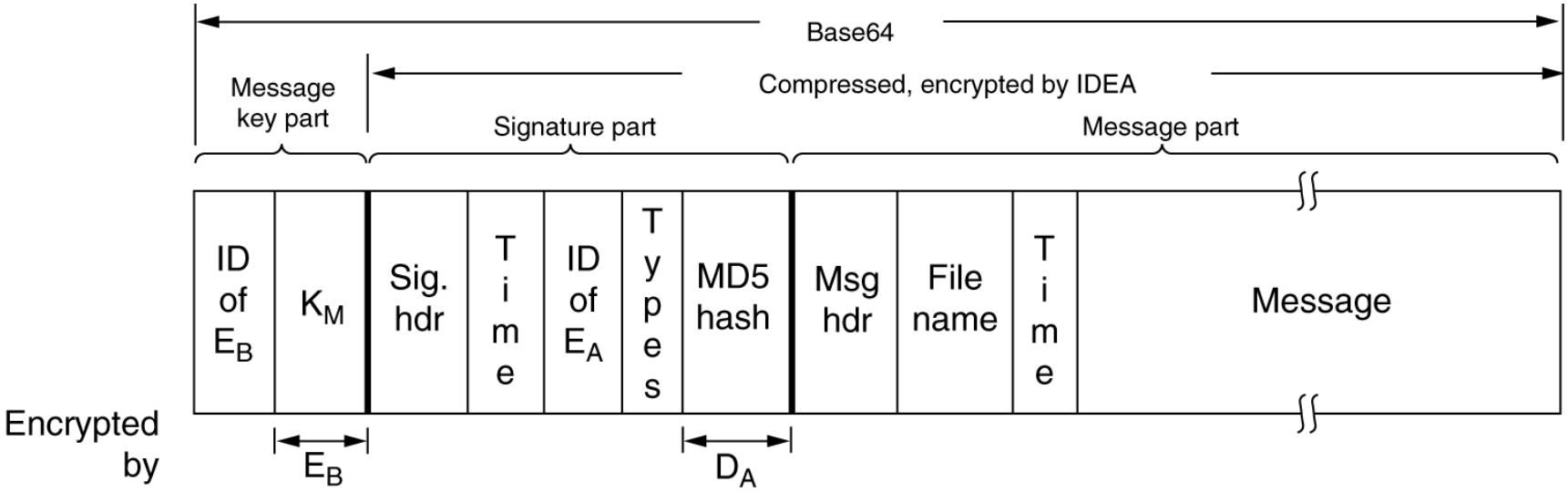
Folosirea PGP pentru a trimite un mesaj.

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

File name – nume implicit al fisierului de utilizat la receptie

Types – identifica algoritmul de criptare

ID of E_A – A poate avea mai multe perechi de chei publica/privata E_A/D_A; fiecare pereche are un identificator ID (ultimii 64 biti ai cheii publice)

ID of E_B – fiecare B poate avea mai multe chei publice; fiecare cheie are un identificator, ID (64 biti) si un indicator de trust (cata incredere are A in aceasta cheie

Management chei

Foloseste doua fisiere in care se pastreaza

- Private key ring contine propriile perechi de chei (publica, privata) impreuna cu identificatorii lor
- Public key ring contine perechi (key, trust indicator) ptr cheile publice ale partenerilor

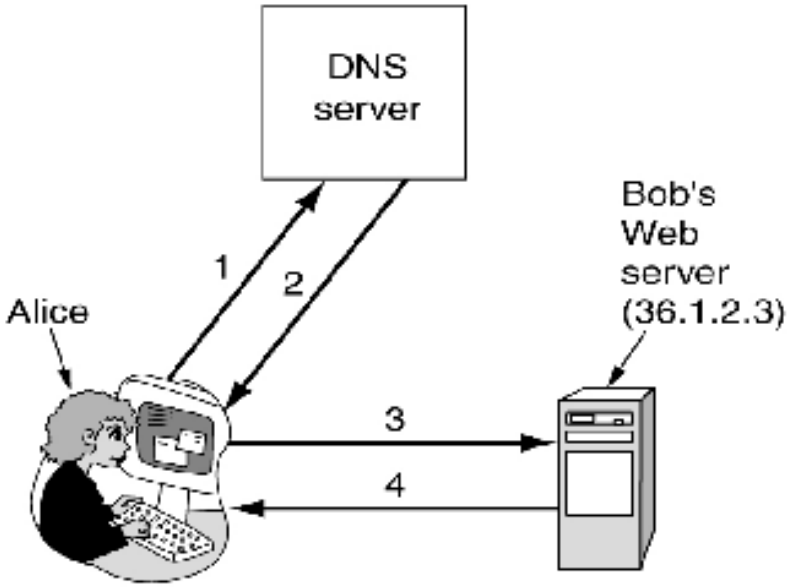
Cheile private se tin criptate cu o parola speciala

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

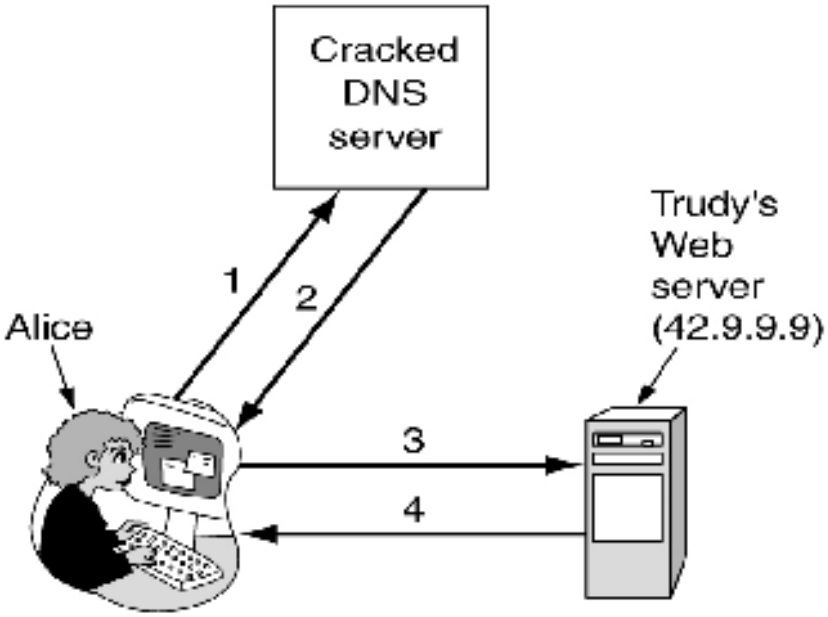
Necesitate Secure Naming



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.

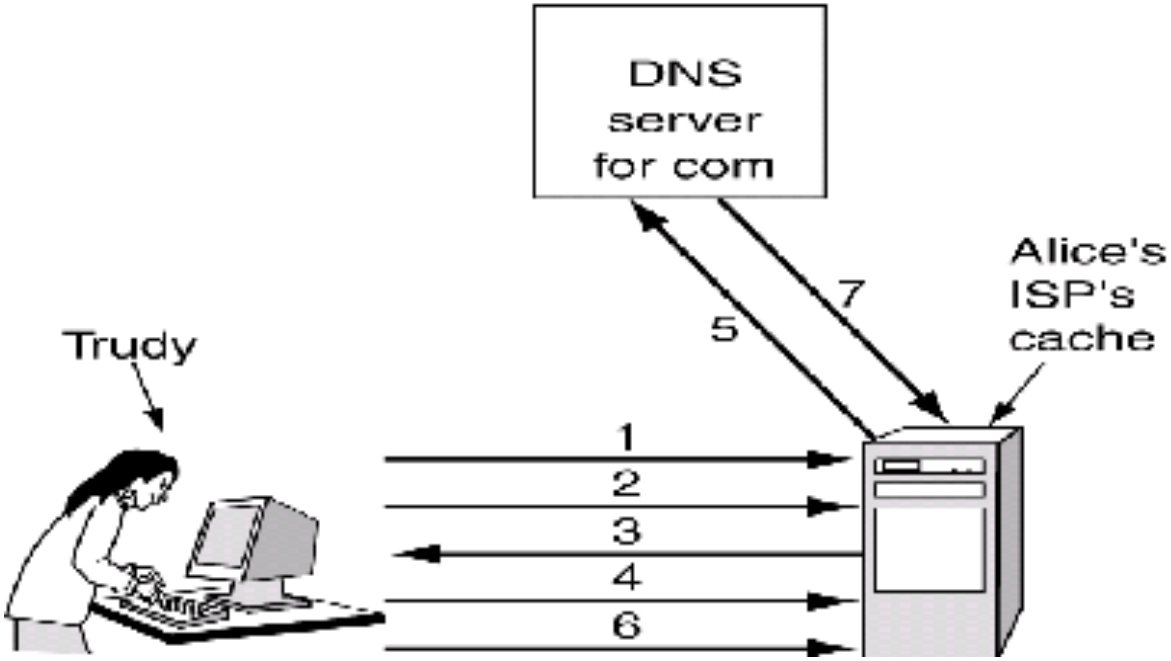


1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page

(b)

Un atac bazat pe modificarea inregistrarii lui Bob in DNS.

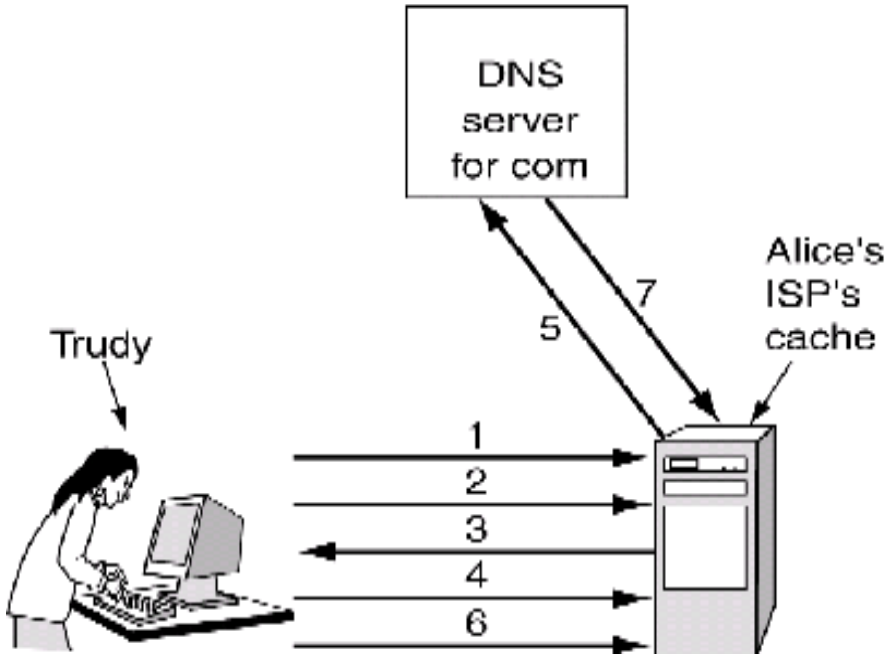
Trudy pacaleste ISP-ul lui Alice



Hint: DNS se bazeaza pe UDP ➔ DNS foloseste
sequence numbers pentru a mapa cererile si raspunsurile

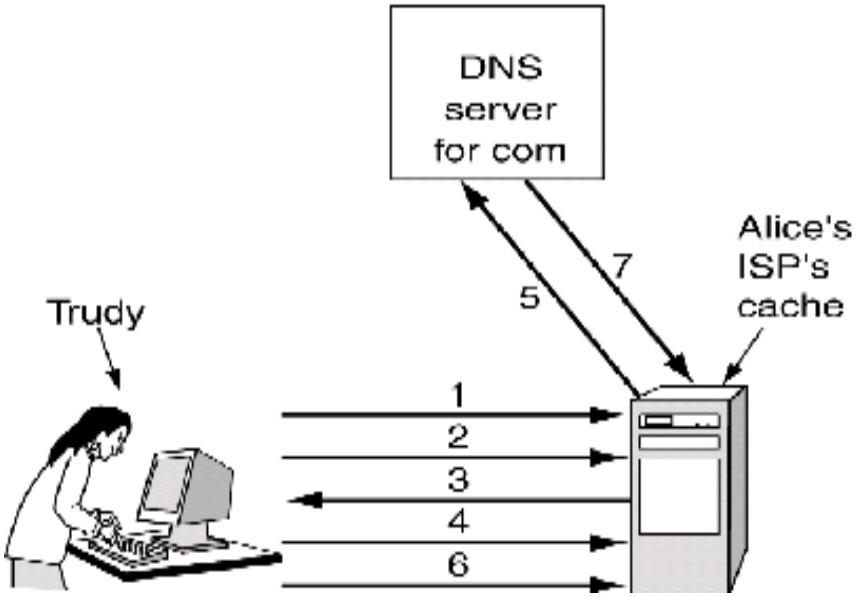
- Trudy inregistreaza un domeniu ***trudy-the-intruder.com*** (IP 42.9.9.9) si
- Instaleaza un server ***dns.trudy-the-intruder.com*** (aceeasi IP 42.9.9.9)

Trudy pacaleste ISP-ul lui Alice (2)



1. Cere adresa ***foobar.trudy-the-intruder.com*** pentru a forta noul ***dns.trudy-the-intruder.com*** in cache-ul ISP-ului lui Alice
2. Cere ISP-ului adresa pentru ***www.trudy-the-intruder.com***
3. ISP intreaba DNS-ul lui Trudy; intrebarea are un numar de secventa, **n** asteptat de Trudy

Trudy pacaleste ISP-ul lui Alice (3)



4. Repede, cere adresa **bob.com** (fortand ISP sa intrebe serverul **com** in pasul 5)

5. ISP transmite cererea catre serverul **com** cu nr secv **n+1**

6. Trudy transmite repede un **raspuns fals** cu nr secv = **n+1**: adresa lui Bob este 42.9.9.9.; raspunsul este considerat bun (Trudy pune adresa IP a serverului com drept sursa raspunsului) si este pus in cache

7. Cand soseste raspunsul adevarat, ISP il rejecteaza

➔ cand Alice va cauta **bob.com** va primi **adresa falsa** din cache ISP

Secure DNS

Inregistrarile din DNS au forma

Domain name	Time to live	Class	Type	Value
bob.com.	86400	IN	A	36.1.2.3

Pentru securitate

fiecarei zone DNS i se aloca o **pereche de chei** publica/privata

Se adauga doua 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.

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...

Secure DNS (2)

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...

Gruparea obtinuta se numeste RRSet (Resource Record Set)

Clientii primesc de la DNS un RRS semnat cu cheia privata

- **aplica cheia publica a zonei pentru a decripta SIG**
- **calculeaza hash-ul pentru A si KEY**
- **compara cele doua valori (calculata si decriptata)**