Protocoale de Securitate

Rezumate de mesaje, semnaturi digitale si protocoale de securitate

Cuprins

- Rezumatul mesajelor
- Semnaturi digitale
- Certificate de securitate
- PKI
- Securitatea comunicatiei - IPsec
- Protocoale de autentificare
- Securitatea e-mail – PGP
- Securitatea Web
- Securitatea DNS

Rezumatele mesajelor

Este mai usor sa semnezi digital rezumatul decat mesajul intreg !

Folosite in semnaturi digitale datorita proprietatilor utile

1. Rezumatul lui P - MD(P) - este usor de calculat
2. Este imposibil sa se afle P din MD(P)
3. Rezumatul nu poate fi trucat: nimeni nu poate gasi P' avand un rezumat identic cu P, adica MD(P') = MD(P)
4. O schimbare de 1 bit a intrarii schimba multi biti din iesire

Functii hash

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

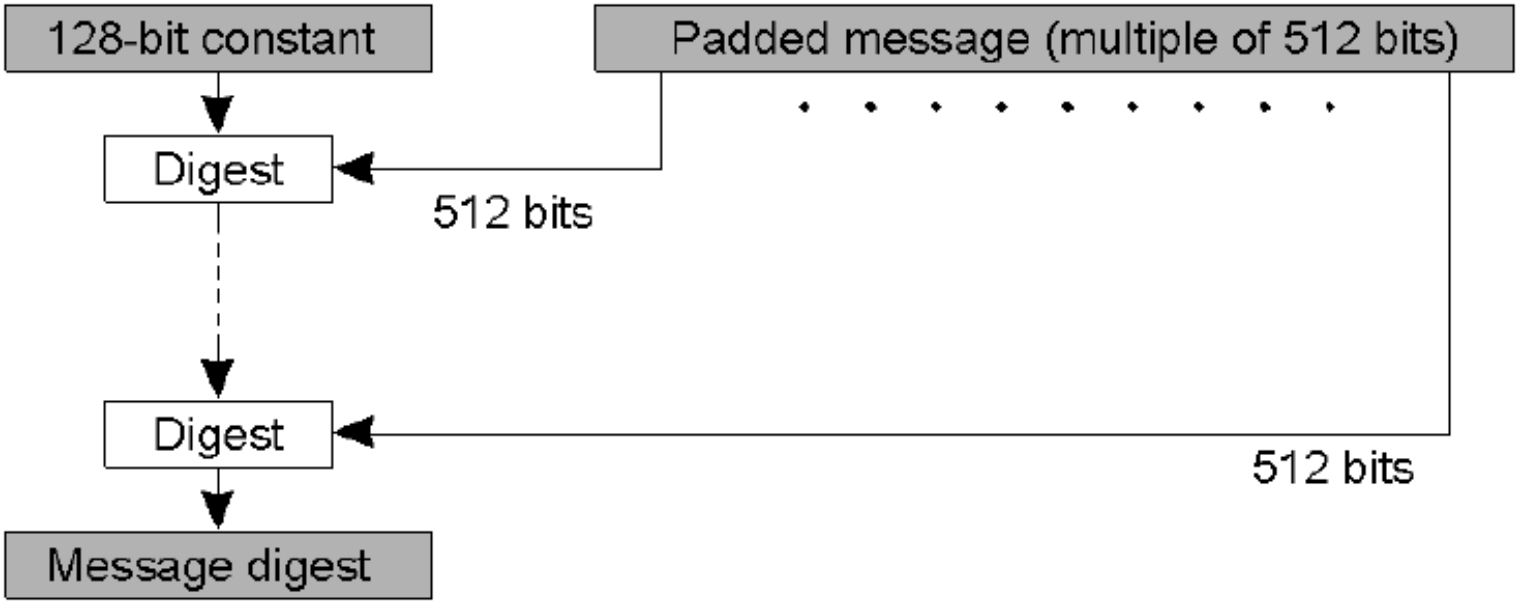
Functii Hash: MD5 - Message Digest 5

MD5 calculeaza un rezumat de 128 biti dintr-un mesaj de lungime multipla de 512 biti

- Mesajul este completat cu biti pentru a respecta regula
- Ultimii 64 biti precizeaza lungimea originala a mesajului

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)

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

p, q, r, s – variabile *digest*

<<< 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

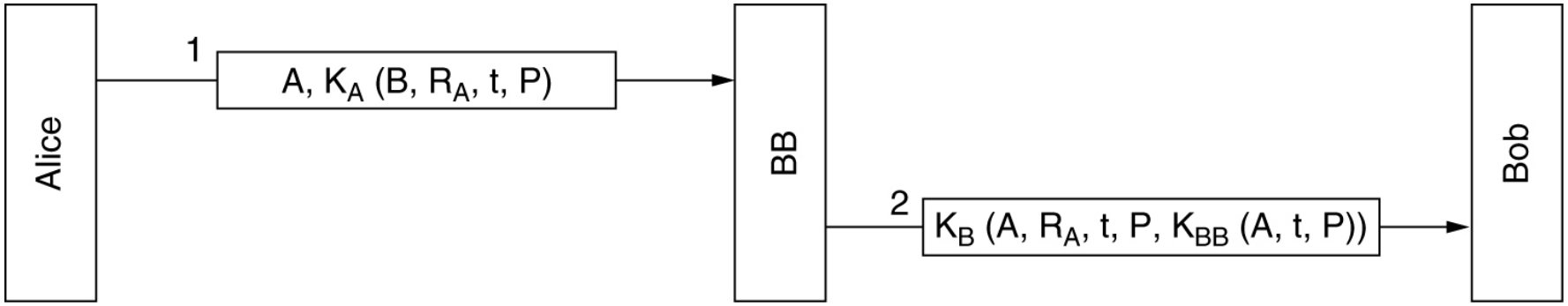
- Rezistenta la coliziuni
  - o functie H este rezistenta la coliziuni daca este foarte greu sa se gaseasca a si b, a#b astfel ca H(a) = H(b)
- In 2004 s-a aratat ca MD5 nu este rezistent la coliziuni
- S-au dezvoltat si recomandat alte functii de hash
  - SHA1, SHA2

- 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 (cunoscuta de BB)
- K_B – cheie secreta a lui B (cunoscuta de BB)
- K_{BB} – cheie secreta Big Brother (doar el o cunoaste)

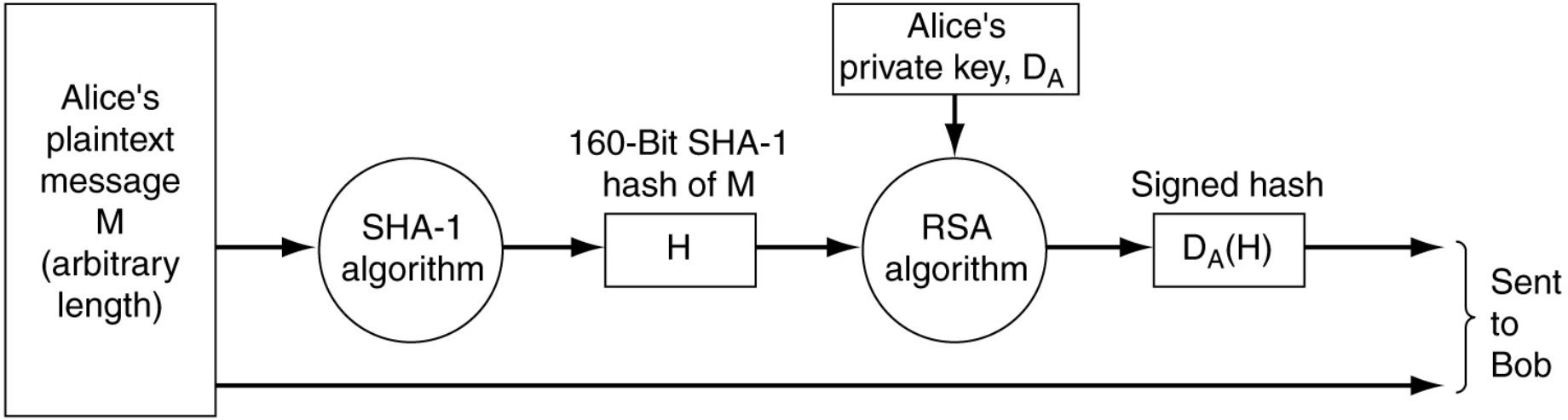
Comentarii

t si R_A folosite ptr. detectie atacuri prin replicare mesaje mai vechi

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

Semnaturi cu chei publice

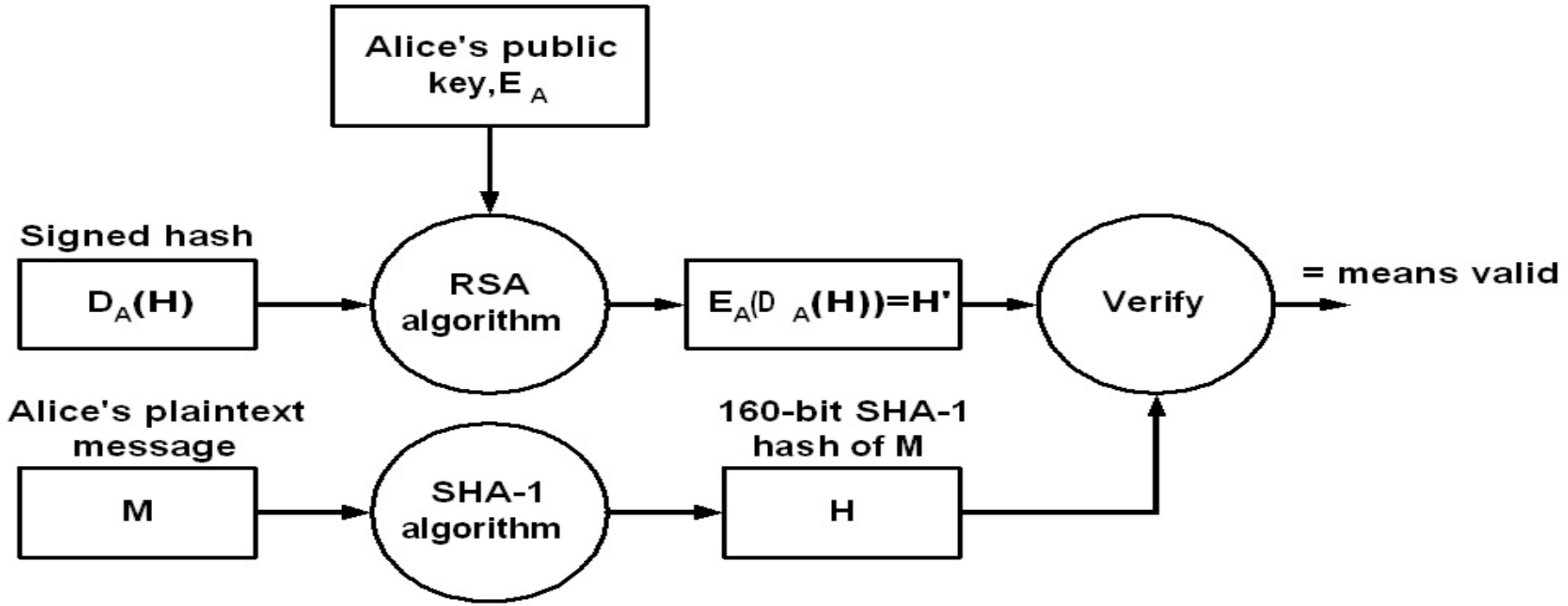
Utilizarea SHA-1 si RSA pentru semnarea mesajelor nesecrete.



Caracteristici

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

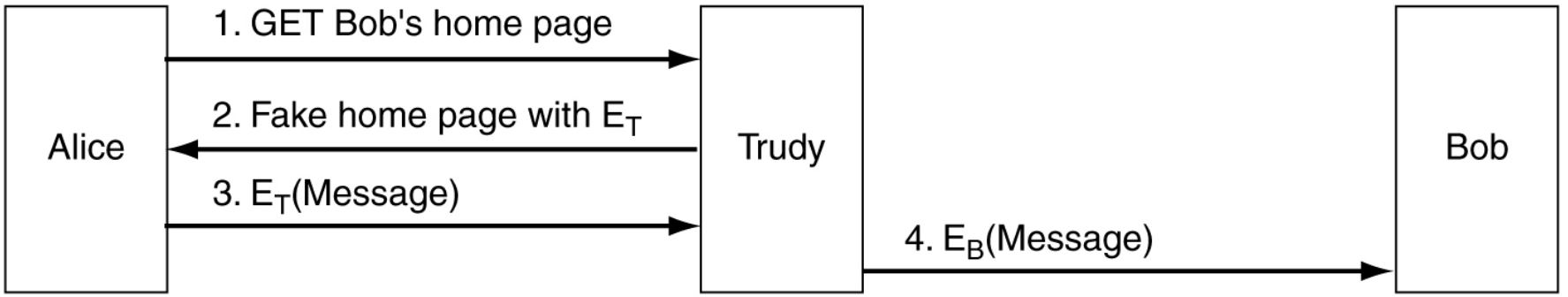
Verificare semnatura digitala



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
  - Man-in-the-middle attack

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 aplica cheia publica a CA asupra semnaturii

A calculeaza rezumatul SHA-1 al certificatului (fara semnatura)

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 - Certificate Authority

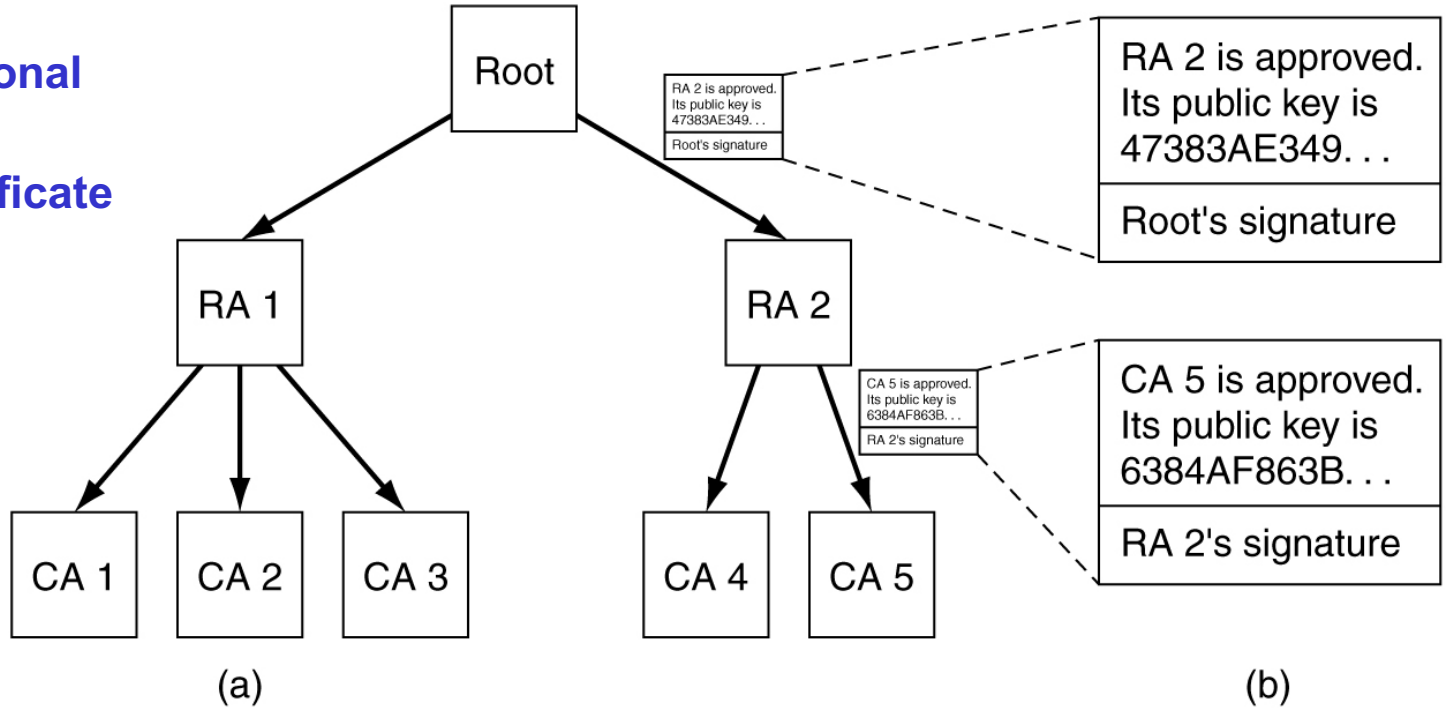
- autoritate de incredere care elibereaza certificate
  - atestă că cheia publica inclusa apartine persoanei cu numele atasat

- CA 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

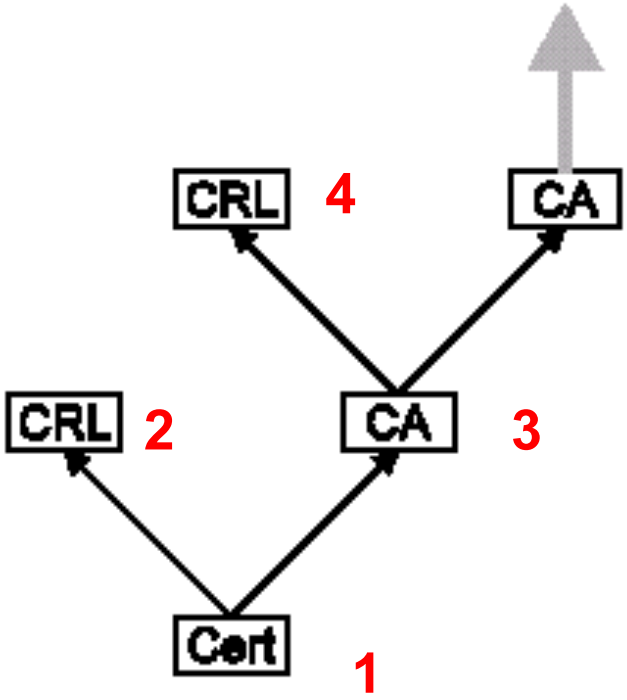
- Un certificat trebuie **revocat** cand:
  - cheia primara este **compromisa**;
  - cheia primara este **pierduta**;
  - o persoana pleaca din companie
  - altele.

- 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

1 - verifica certificat

2 - verifica CRL

repeat

3 - verifica certificatul pentru CA

4 - verifica CRL al CA

until radacina

Securitatea Comunicatiei

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

IP Security Protocol - IPSec

- Implementat la nivel IP
- Construieste o legatura securizata unidirectionala intre transmitator si receptor
  - numita Security Association - SA
  - asigura
    - autentificarea mesajelor sau
    - autentificarea si criptarea
- 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**

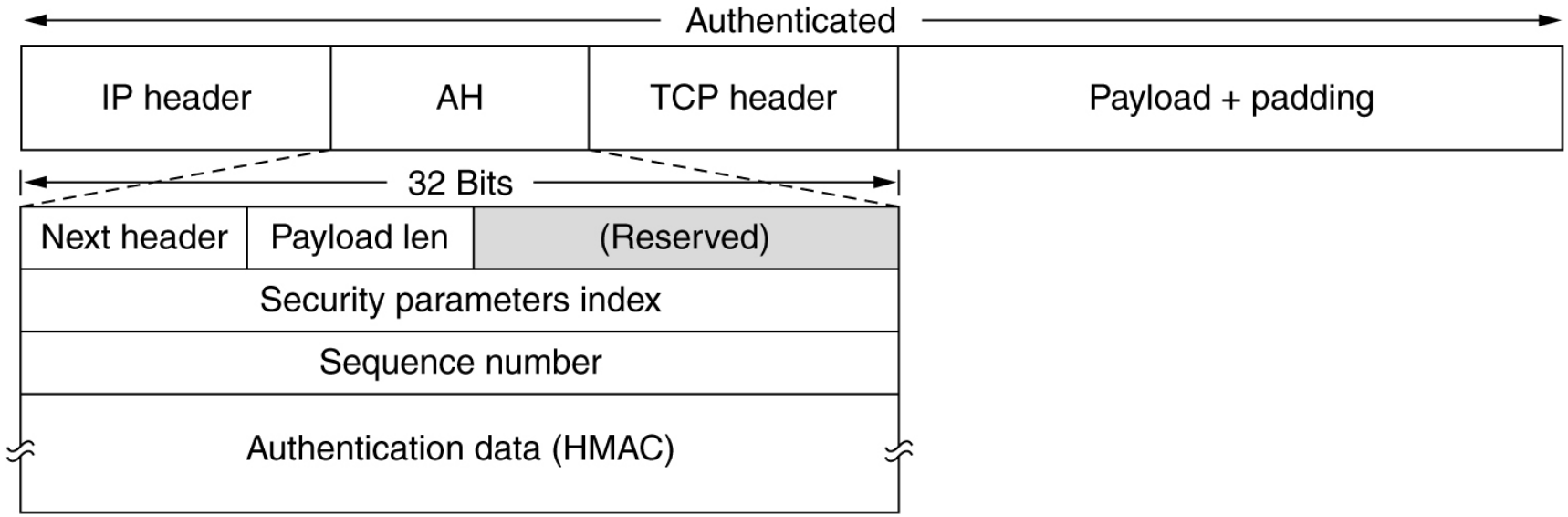
Doua protocoale de securitate:

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

Si doua moduri de lucru

- transport
- tunel

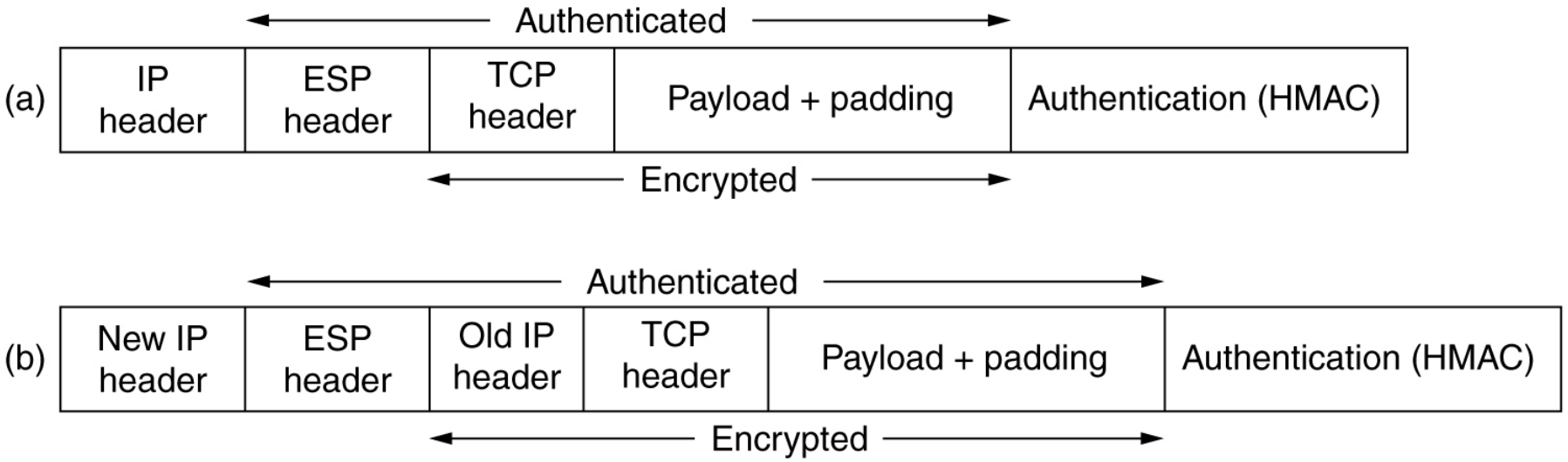
Protocol AH – in mod transport pentru IPv4



Authentication Header – inserat in datagrama IP

- Next header – preluat din IP header unde este inlocuit cu 51
- Payload len – lungime AH (nr cuvinte 32 biti) minus 2
- Security Parameters 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

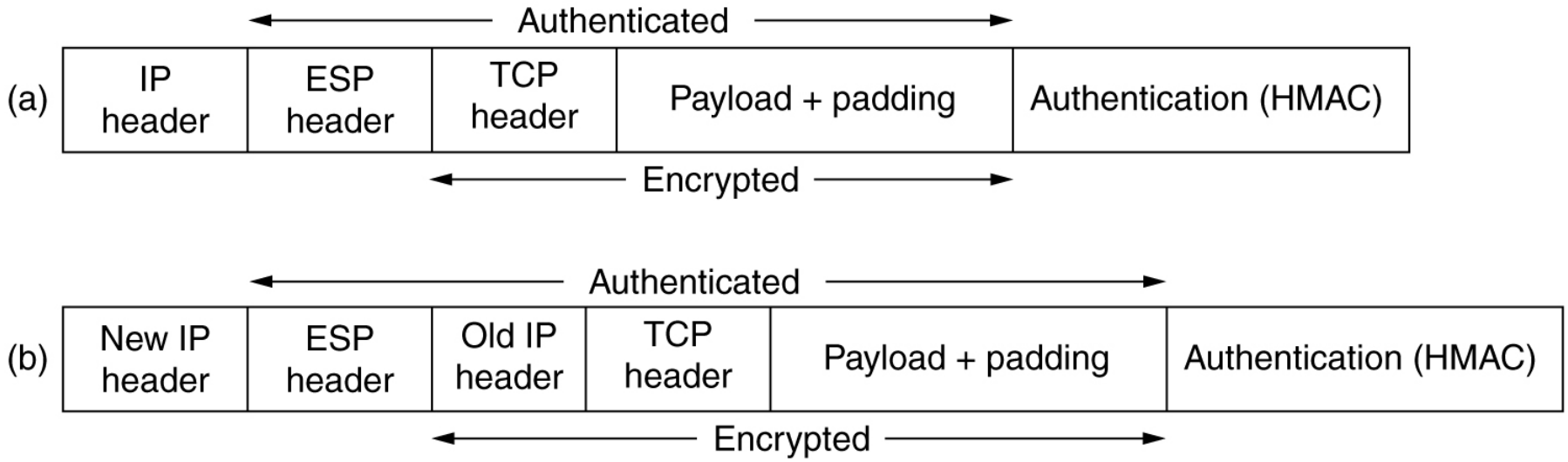
(a) ESP in mod transport.

- antetul ESP este plasat intre antetele IP si TCP
- campul “protocol” din antetul IP este modificat si arata ca urmeaza un antet IPsec

(b) ESP in mod tunel.

- la pachetul IP se adauga antetul IPsec si un nou antet IP
- tunelul se poate termina inainte de destinatie (de ex. la un firewall)

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 ESP + criptograma

ESP header include

Security Parameters Index

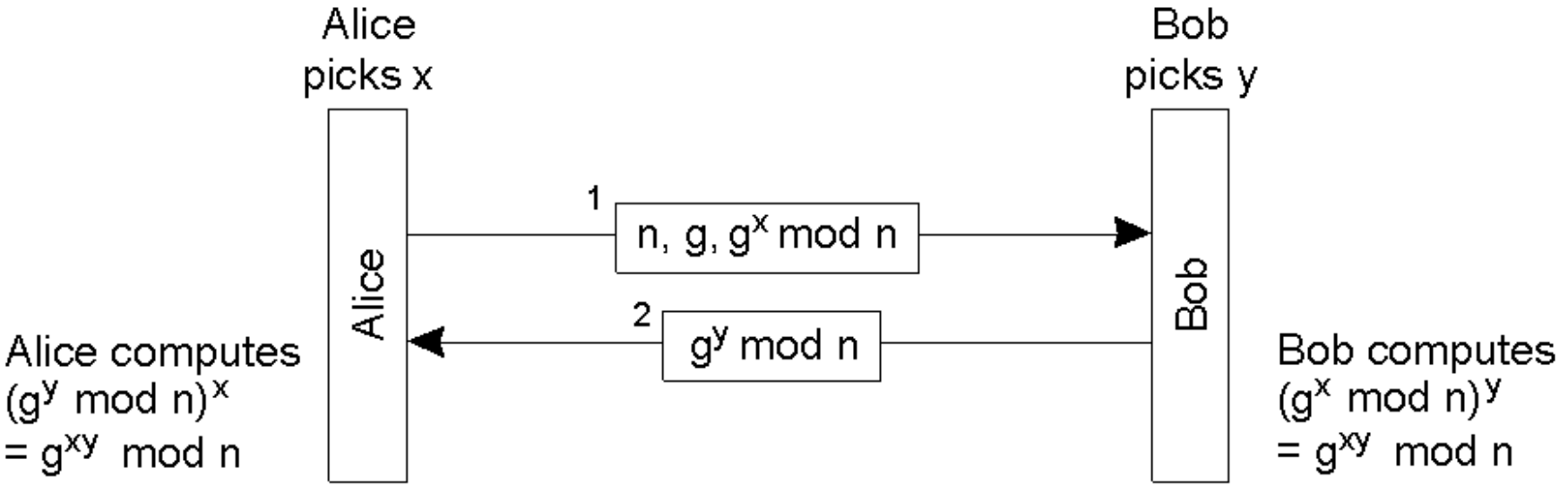
Numar de Secventa

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

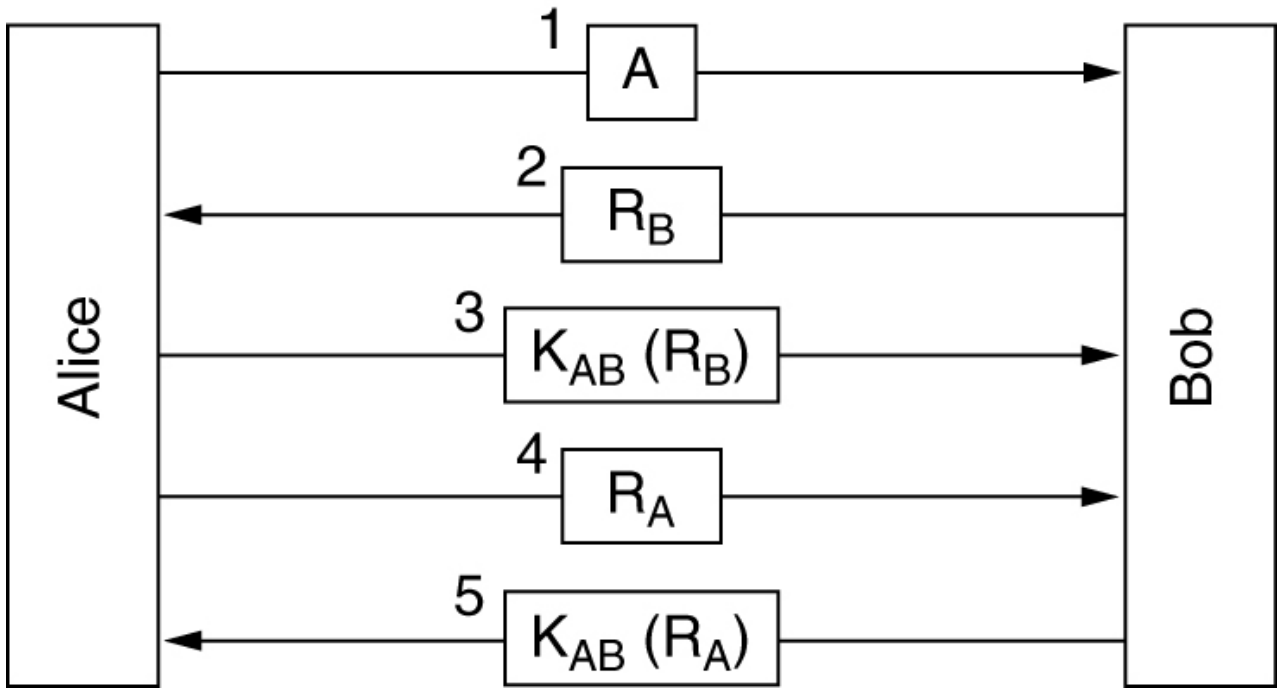
Determina daca o entitate (utilizator, proces) este cu adevarat cine / ce pretinde ca este

- diferita de autorizare
- se bazeaza pe un schimb de mesaje prin Internet (prezentate, de regula, ca schimb intre Alice si Bob)
- mesajele pot fi interceptate si folosite de alte entitati (de regula Trudy)
- protocolul genereaza si o cheie de sesiune

Folosesc criptografia cu

- Chei secrete partajate
- Chei publice

Autentificare cu cheie secreta partajata

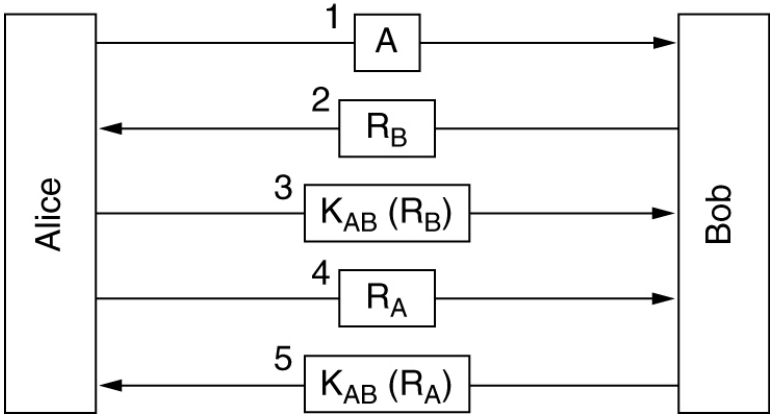


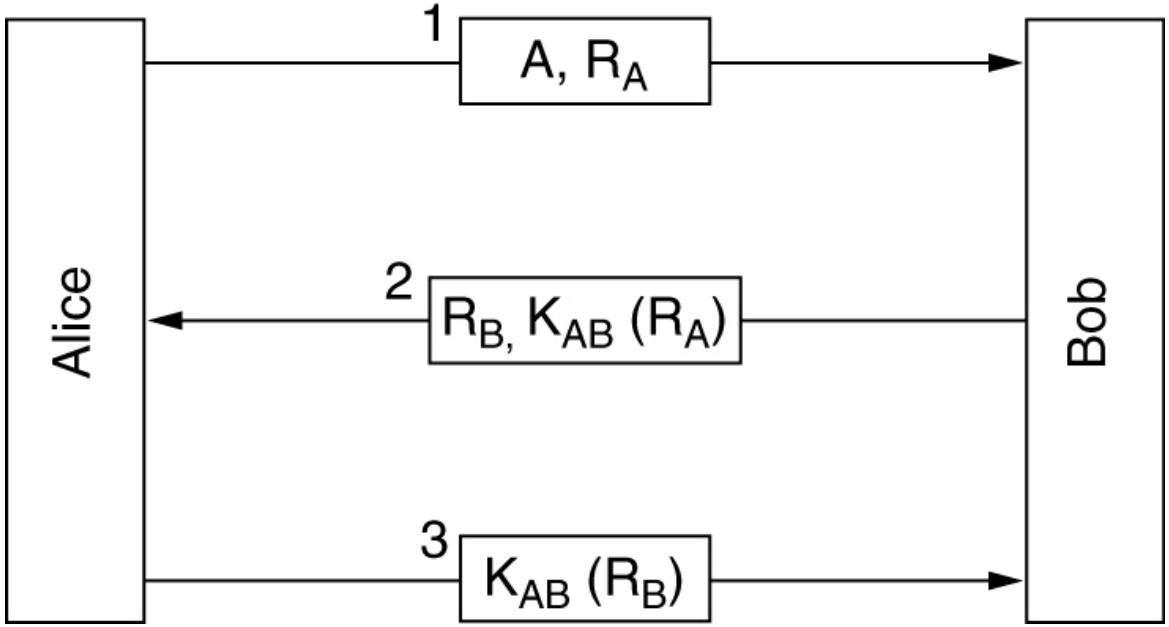
Autentificare reciproca cu un protocol challenge-response

Alice si Bob partajeaza cheia K_{AB}

R_A, R_B - numere aleatoare foarte mari, folosite contra atac prin replica

Autentificare cu cheie secreta partajata (2)





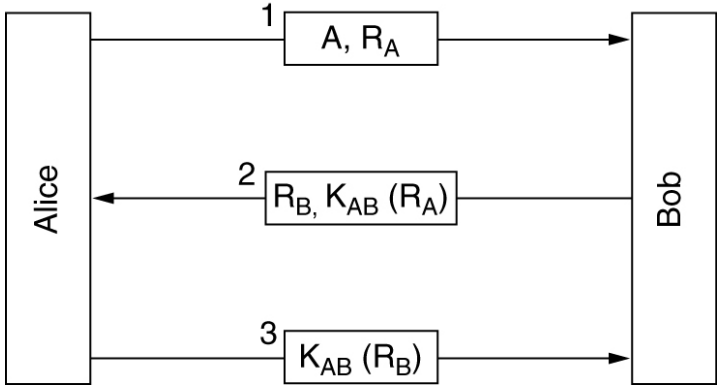
Reducere numar de pasi

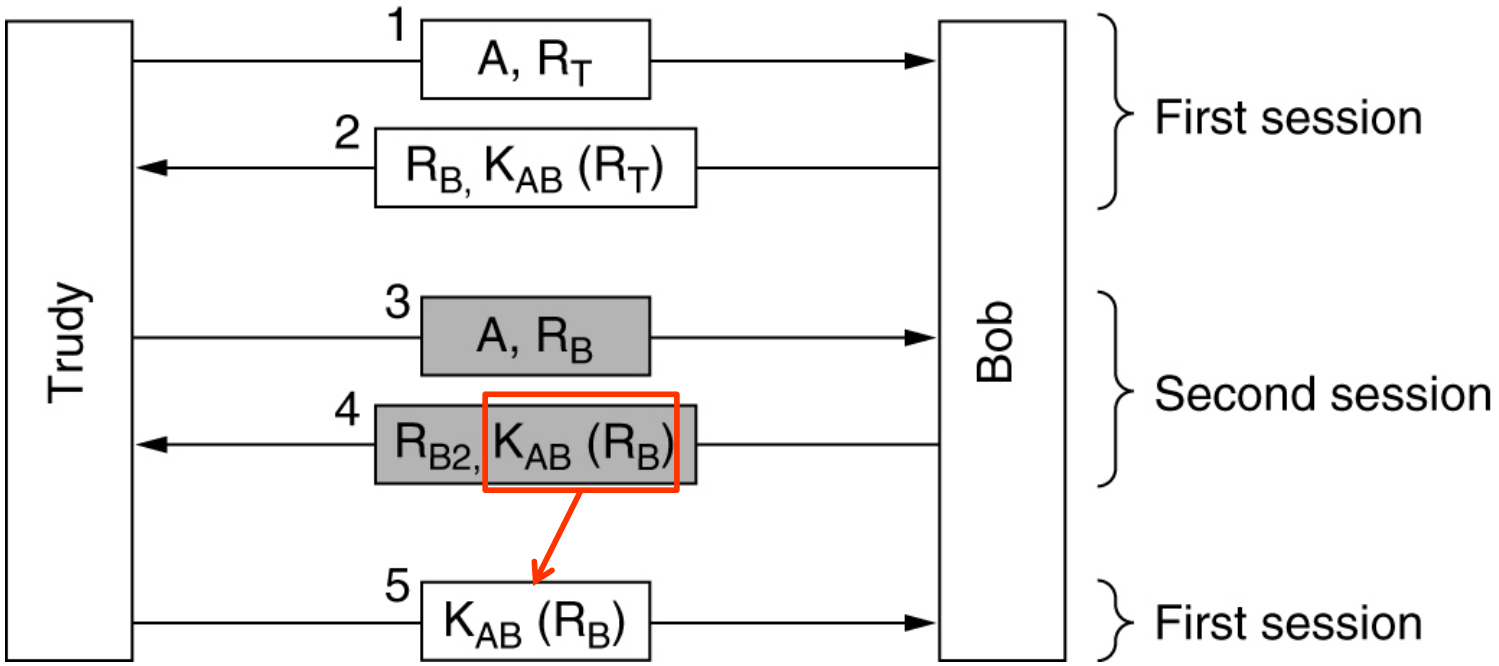
Atacul prin reflexie

Trudy nu poate cripta R_B din mesajul 2

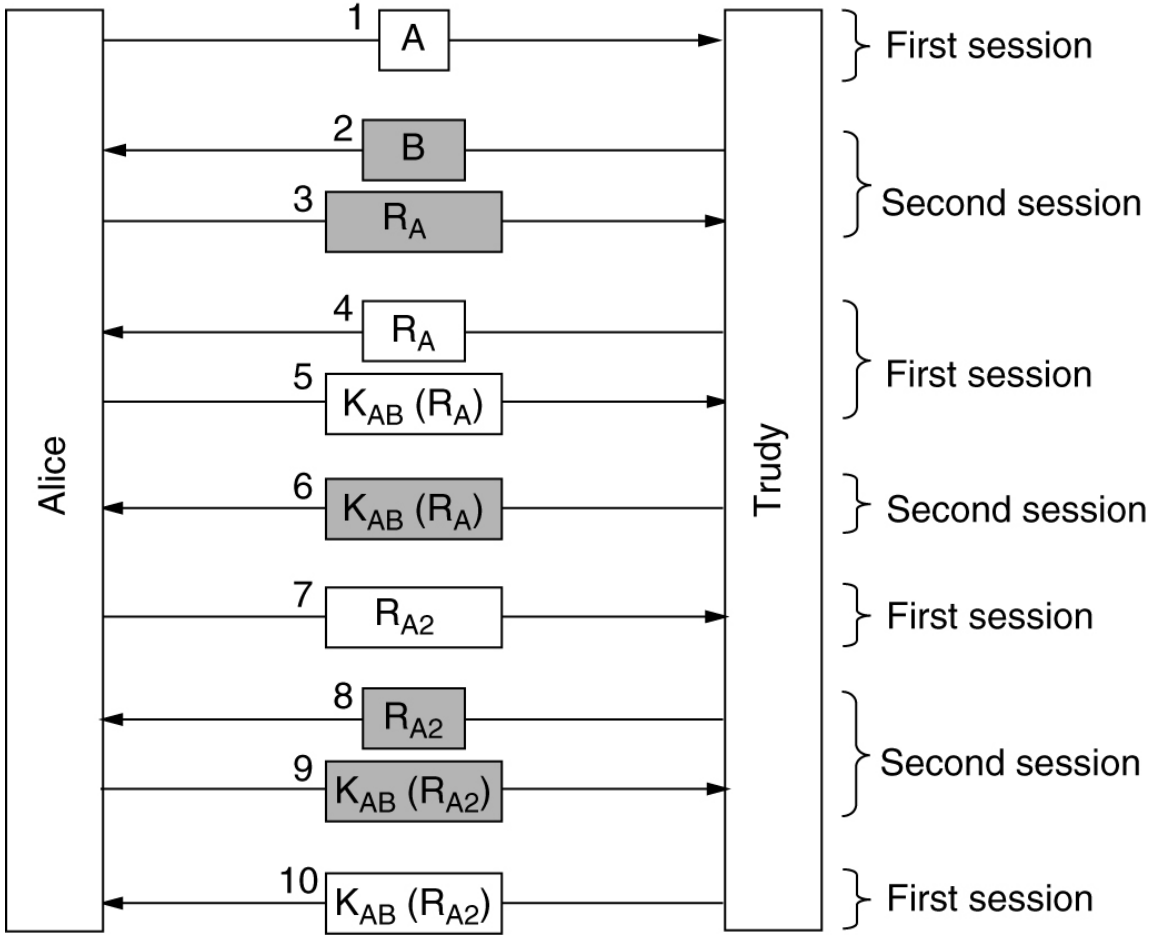
Dar retransmite un mesaj produs de Bob (4) si

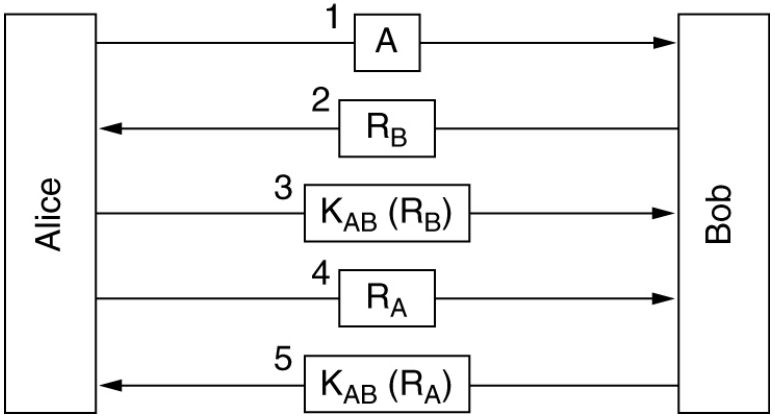
reuseste sa stabileasca o sesiune autentificata cu Bob





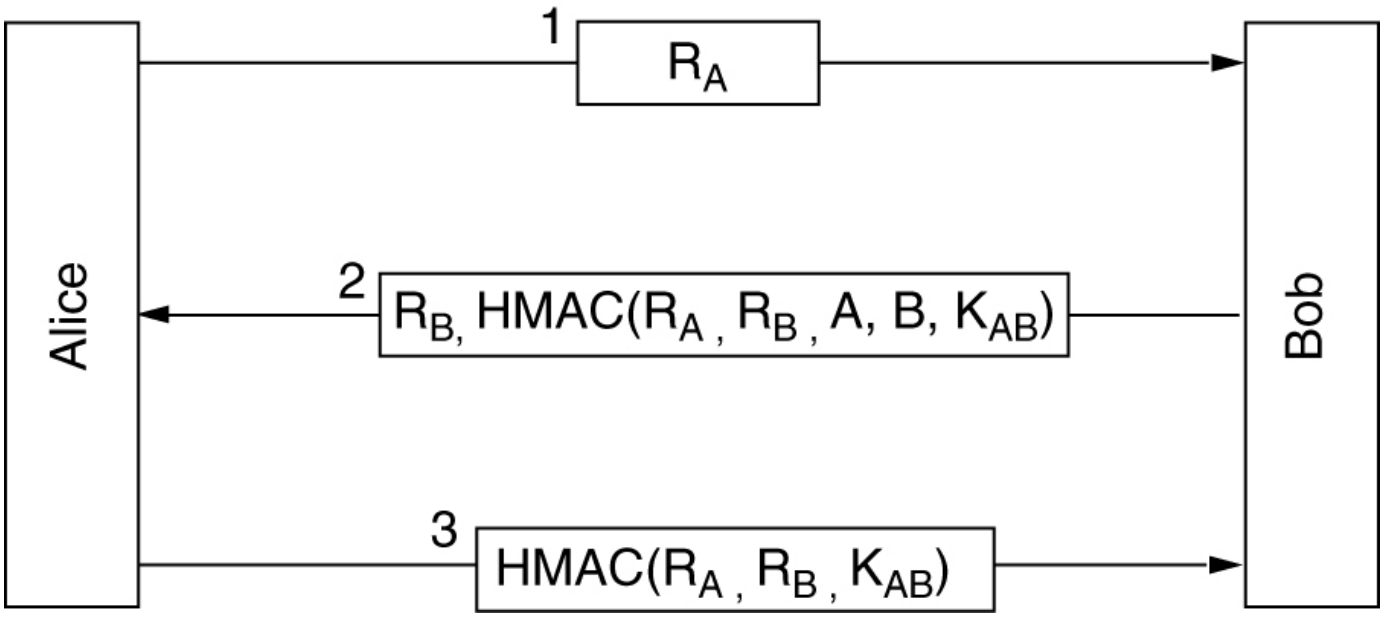
Atacul prin reflexie pe protocolul initial





Rejucand mesajele 5 si 9, Trudy reuseste sa stabileasca doua sesiuni autentificate cu Alice

Autentificarea cu HMACs



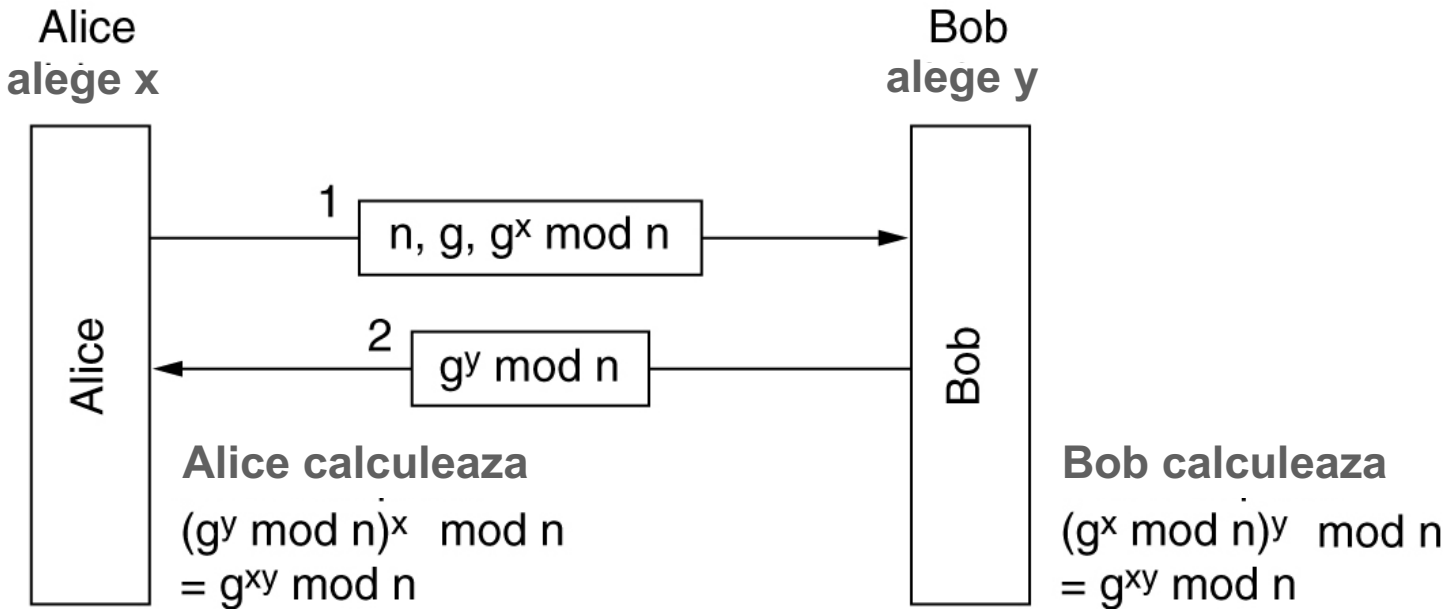
Alice si Bob partajează cheia K_{AB}

Fiecare parte poate calcula rezumatul HMAC - Hashed Message Authentication Code – (deoarece contine doar valori cunoscute)

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

Trudy nu poate forța pe Alice sau Bob să cripteze sau să rezume o valoare impusă de ea

Stabilire cheie partajata: Diffie-Hellman key exchange



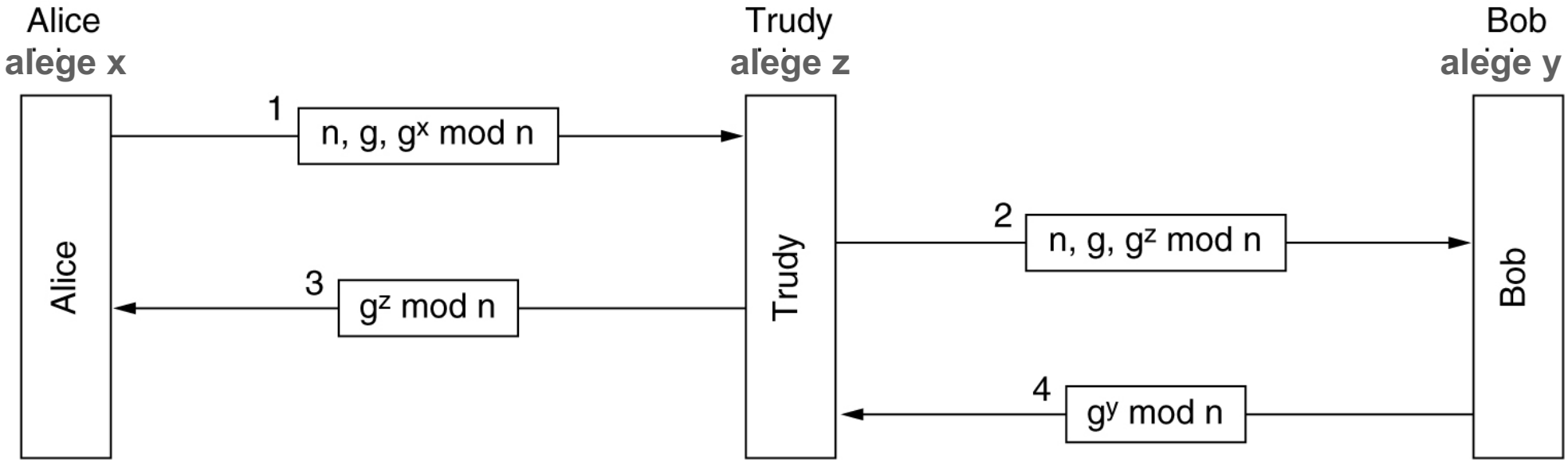
n, g – numere mari
n prim
(n-1)/2 prim

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

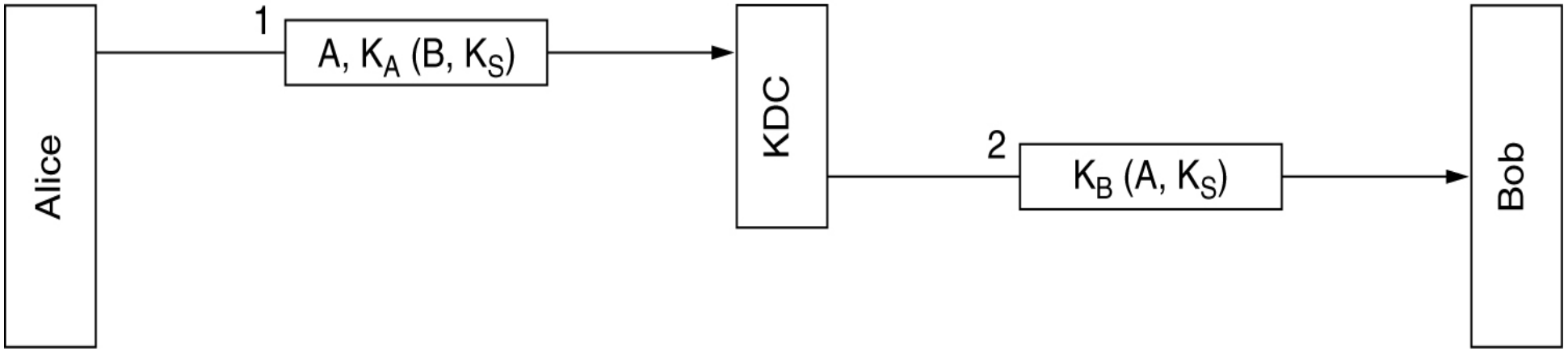


Vulnerabilitate – **g** si **n** sunt publici

- permite stabilirea a doua chei: intre Alice si Trudy - $\mathbf{g^{xz} \bmod n}$ si intre Trudy si Bob - $\mathbf{g^{zy} \bmod n}$

Rezolvare: Alice si Bob semneaza mesajele schimbate intre ei
Trudy nu poate modifica mesajele

Autentificarea folosind Key Distribution Center



Alice si Bob folosesc un Centru de distributie a cheilor

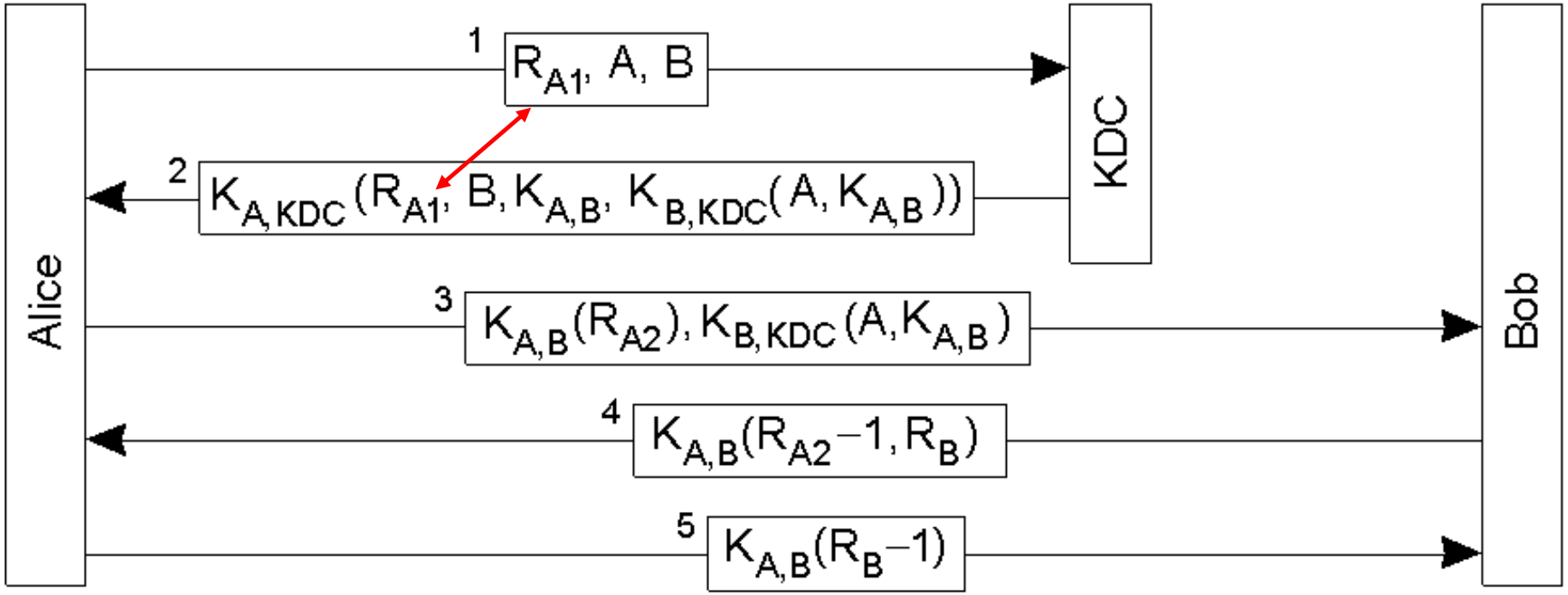
- in care au incredere
- cu care impart cheile secrete **K_A** respectiv **K_B**

Prima incercare, vulnerabila la replay attack

Trudy **retransmite** mesajul 2 si

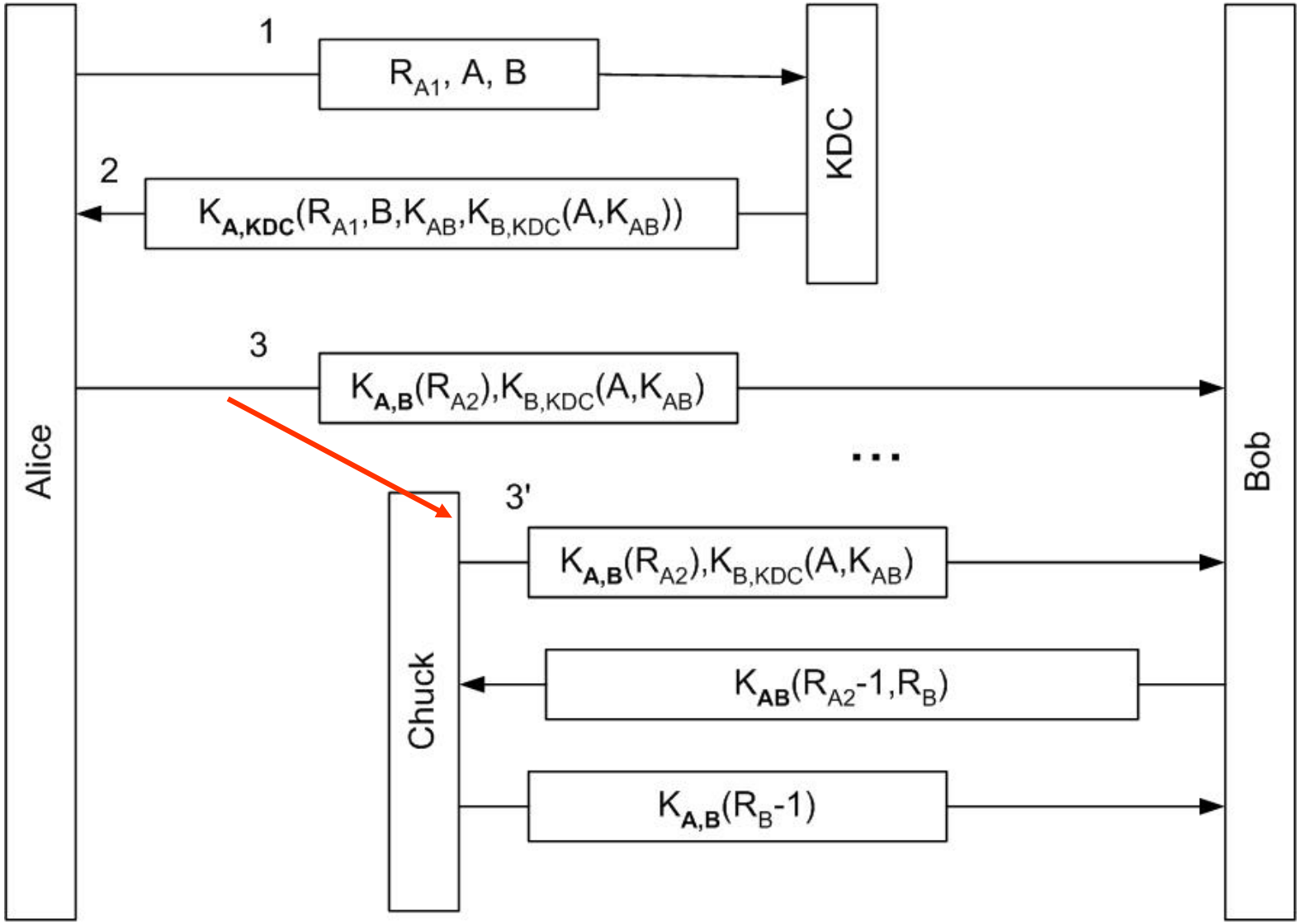
mesajul asociat cu el, criptat deja cu **K_S** (de ex. extragerea din contul lui Alice a unei sume de bani)

Autentificarea cu protocolul Needham-Schroeder



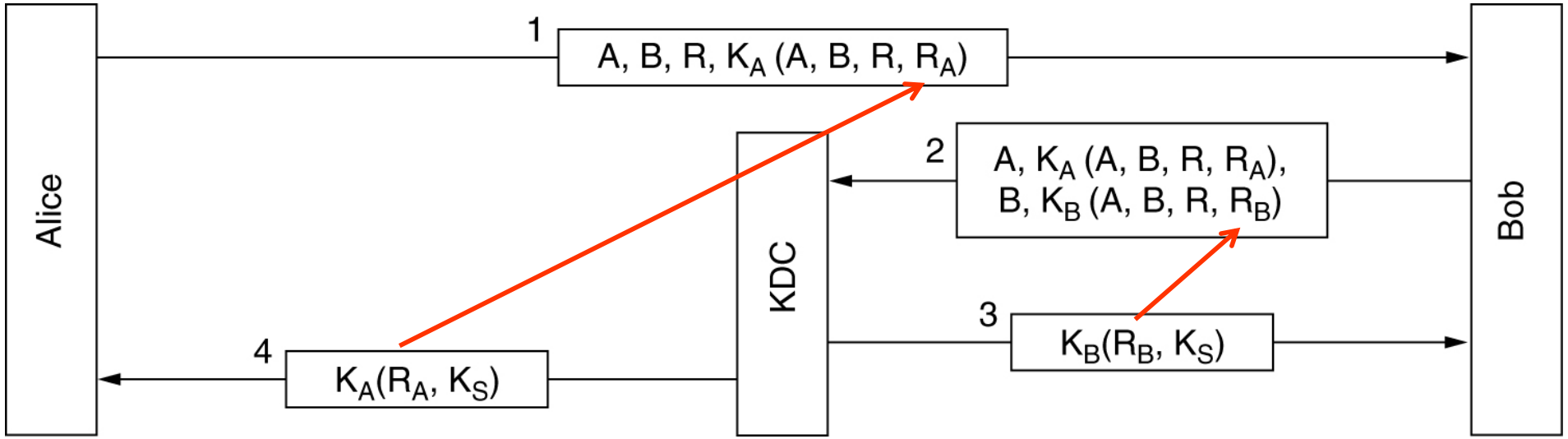
- foloseste tichete - ex. **$K_{B,KDC}(A, K_{AB})$**
  - Alice nu poate intelege sau modifica tichetul, Bob poate
  - Bob capata incredere in cheia **K_{AB}** (care vine de la KDC)
- numere aleatoare (nonce) ex. **R_{A1}**, folosite contra atac prin replica
  - ex. Alice afla ca mesajul 2 este un raspuns la 1, nu un mesaj rejucat de Trudy

Slabiciune Needham-Schroeder



Chuck afla cheia K_{AB} si rejoaca mesajul 3, pretinzând ca e Alice

Autentificarea folosind Protocolul Otway-Rees



Protocolul Otway-Rees (simplificat).

KDC trimite cheia de sesiune K_S dupa ce verifica daca identificatorul comun R apare in ambele parti criptate ale mesajului 2

R_A, R_B – numere aleatoare folosite de KDC in mesajele 3 si 4 pentru a face legatura cu mesajele 1 si 2

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

Securitatea E-Mail - PGP – Pretty Good Privacy

Autor: Phil Zimmermann

Ofera gama completa de servicii de securitate

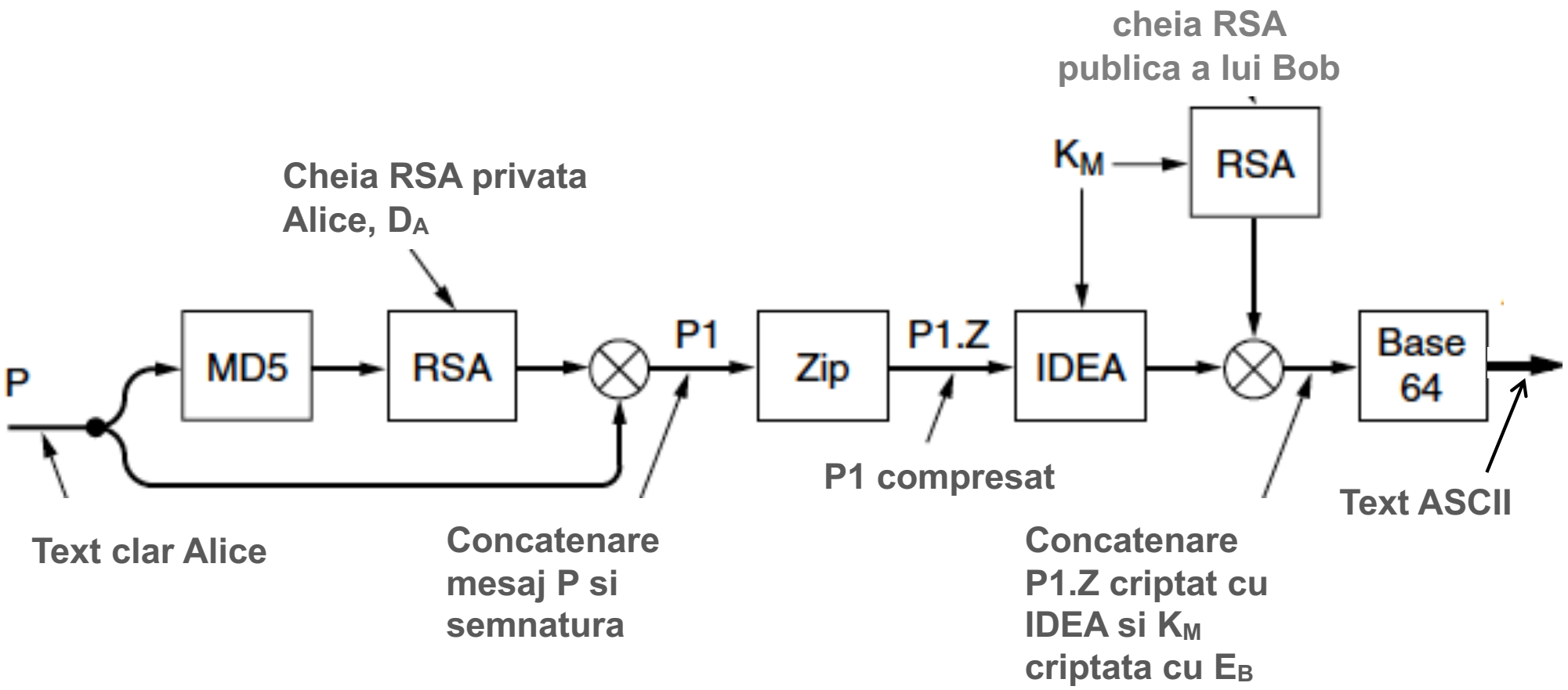
- intimitate (privacy)
- autentificare
- semnatura digitala (integritate)
- compresie

Intregul pachet PGP (inclusiv codul sursa) este distribuit gratuit pe Internet

Cripteaza date folosind IDEA (International Data Encryption Algorithm) – similar cu DES si AES

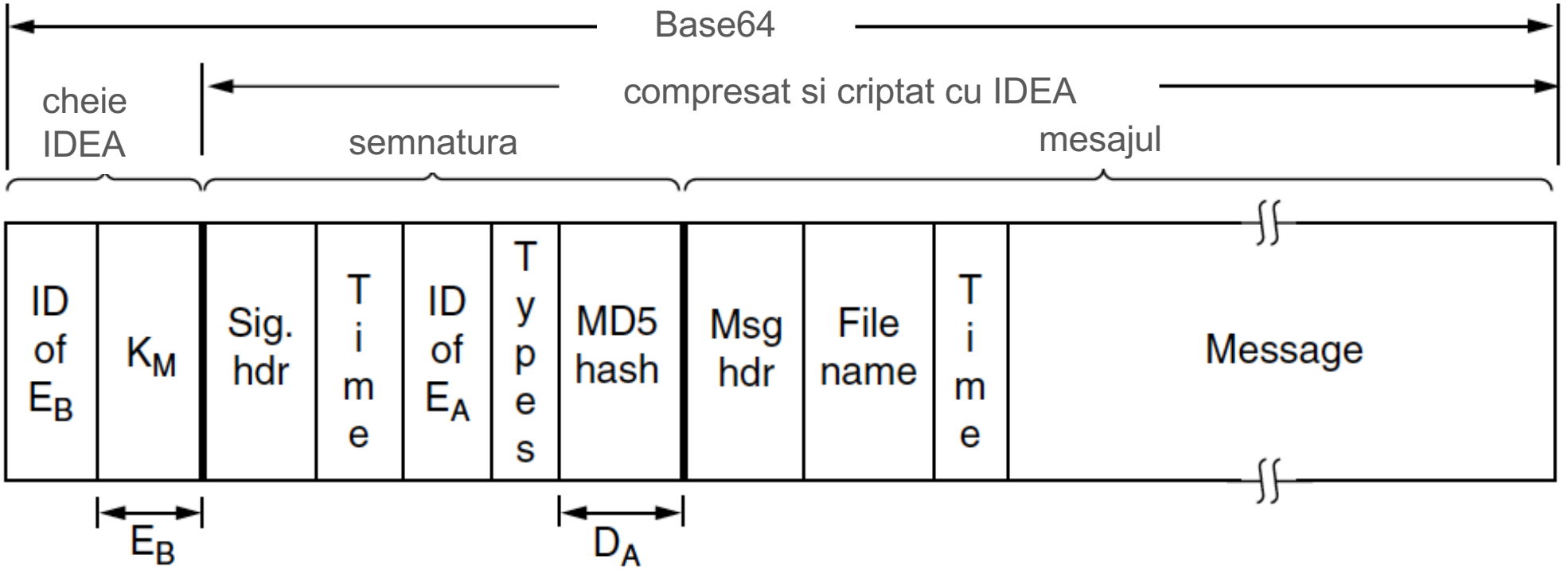
Semneaza mesajele folosind RSA

Folosirea PGP pentru a trimite un mesaj



K_M cheie de sesiune 128-biti produsa din textul introdus de Alice

PGP – Formatul mesajului



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 păstrează

- 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

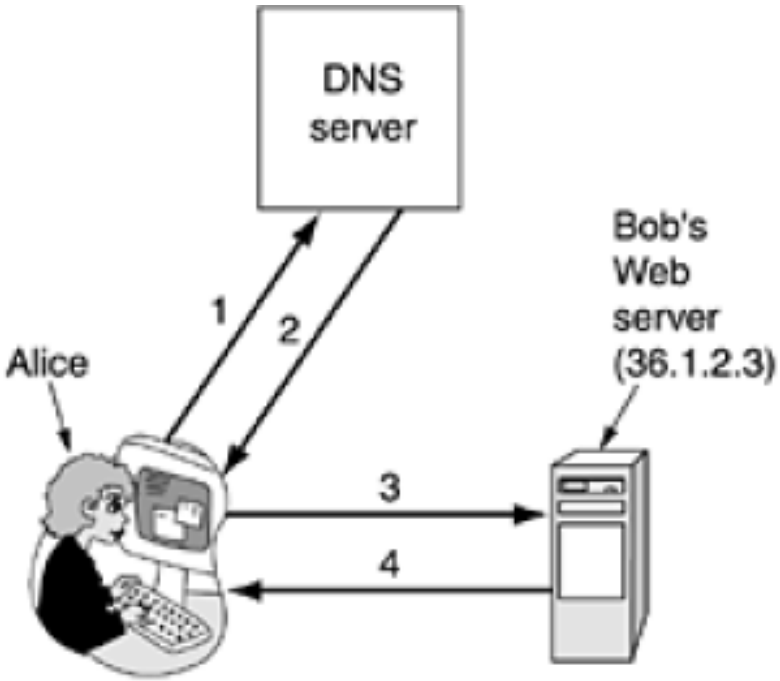
Cheile private se țin criptate cu o parola speciala

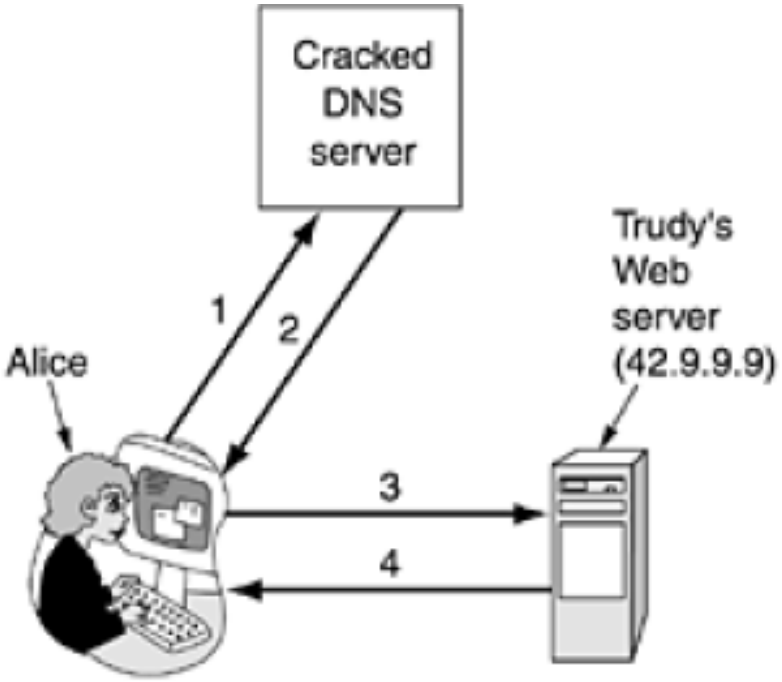
Versiunile actuale PGP folosesc certificate X.509

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



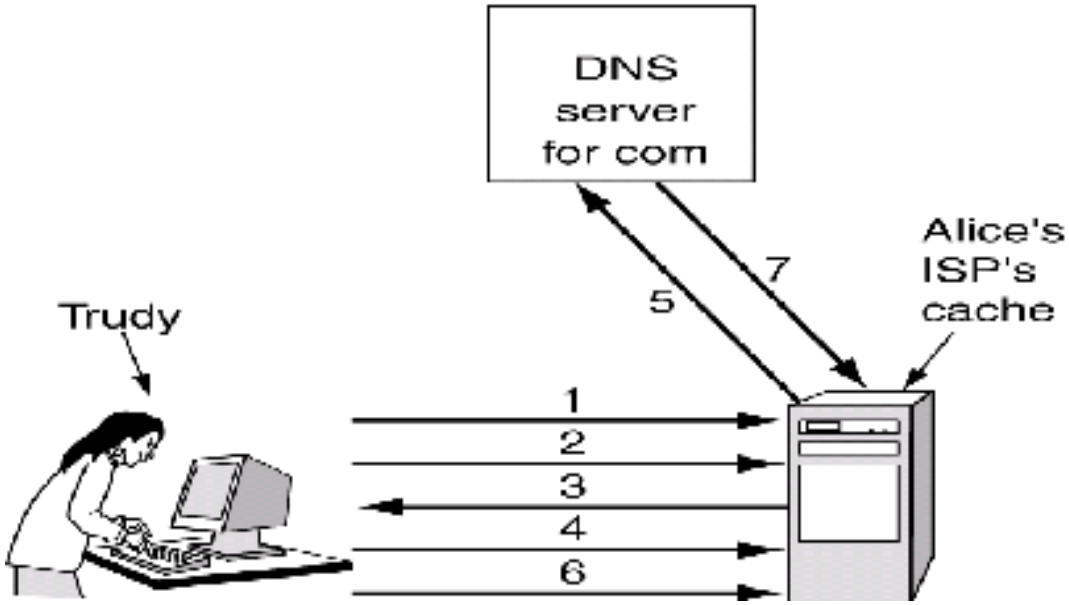


Situatie Normala.

1. Da-mi adresa IP Bob
2. 36.1.2.3 (adr IP Bob)
3. GET index.html
4. Pagina home Bob

Un atac bazat pe modificarea inregistrarii lui Bob in DNS.

1. Da-mi adresa IP Bob
2. 42.9.9.9 (adr IP Trudy)
3. GET index.html
4. Pagina Bob falsificata de Trudy



Trudy pacaleste ISP-ul lui Alice

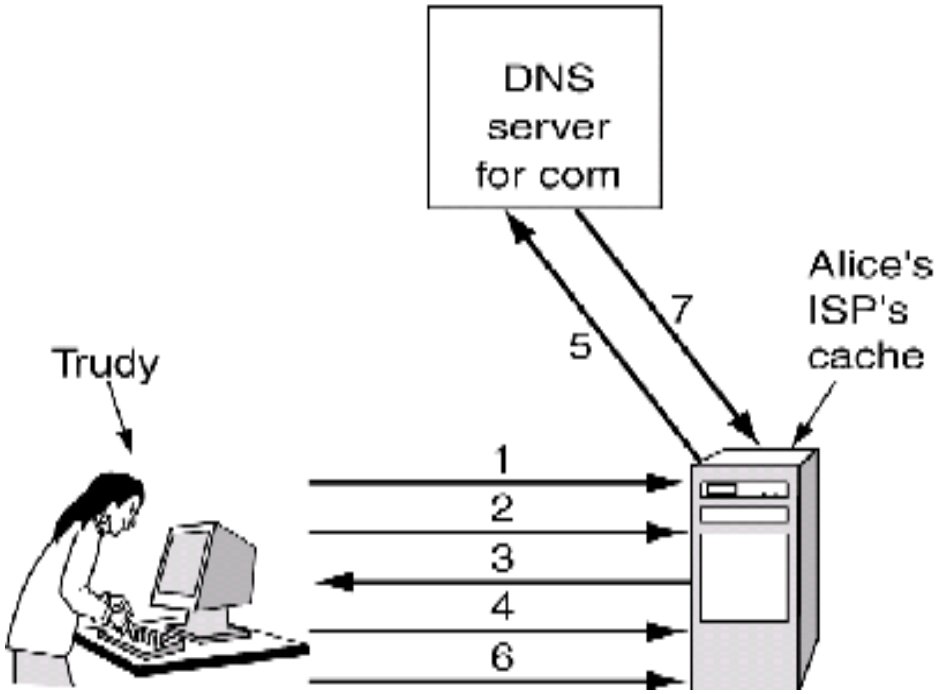
Probleme: ISP verifică adresa IP de la care vin răspunsurile DNS

- Trudy poate folosi adresa IP a unui server DNS de nivel inalt (care este publica) pentru a construi un raspuns fals

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
- Creaza un server DNS ***dns.trudy-the-intruder.com*** (aceeasi IP 42.9.9.9)

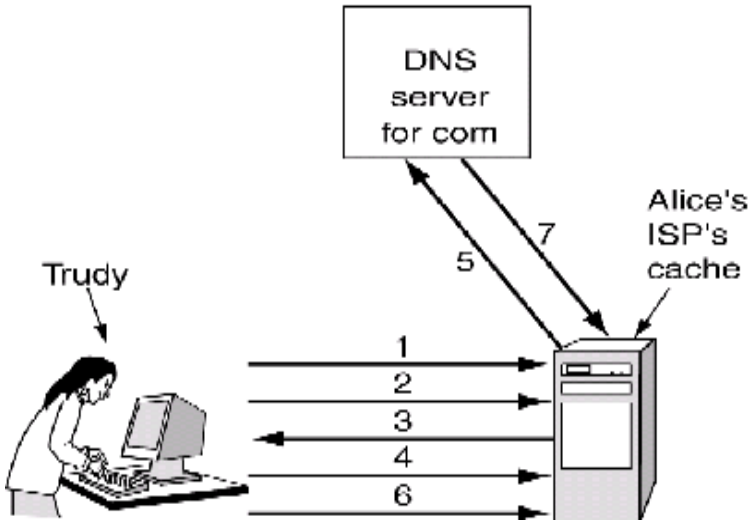


Trudy pacaleste ISP-ul lui Alice (2)

1. Cere adresa ***foobar.trudy-the-intruder.com*** - ISP-ul lui Alice afla de la serverul **com** despre noul ***dns.trudy-the-intruder.com*** si il pune in cache

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 cu nr secv n+1 catre serverul **com**
6. Trudy transmite repede un **raspuns fals** cu nr secv = **n+1**, adresa IP a serverului **com** drept sursa raspunsului si adresa sa 42.9.9.9 drept adresa lui Bob; raspunsul este considerat bun si este pus in cache-ul ISP
7. Cand soseste raspunsul adevarat, ISP il rejecteaza

Cand Alice cauta **bob.com** primeste **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 al inregistrarilor *A* si *KEY* pentru verificarea autenticitatii.

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 cu semnatura SIG

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

Studiu individual

A. S. Tanenbaum Reţele de calculatoare, ed 4-a, BYBLOS 2003

8.4 SEMNĂTURI DIGITALE
8.5 GESTIONAREA CHEILOR PUBLICE
8.6 SECURITATEA COMUNICAŢIEI
8.7 PROTOCOALE DE AUTENTIFICARE
8.8 CONFIDENŢIALITATEA POŞTEI ELECTRONICE
8.9 SECURITATEA WEB-ULUI

A. S. Tanenbaum Computer networks, 5-th ed. PEARSON 2011

8.4 DIGITAL SIGNATURES
8.5 MANAGEMENT OF PUBLIC KEYS
8.6 COMMUNICATION SECURITY
8.7 AUTHENTICATION PROTOCOLS
8.8 EMAIL SECURITY
8.9 WEB SECURITY