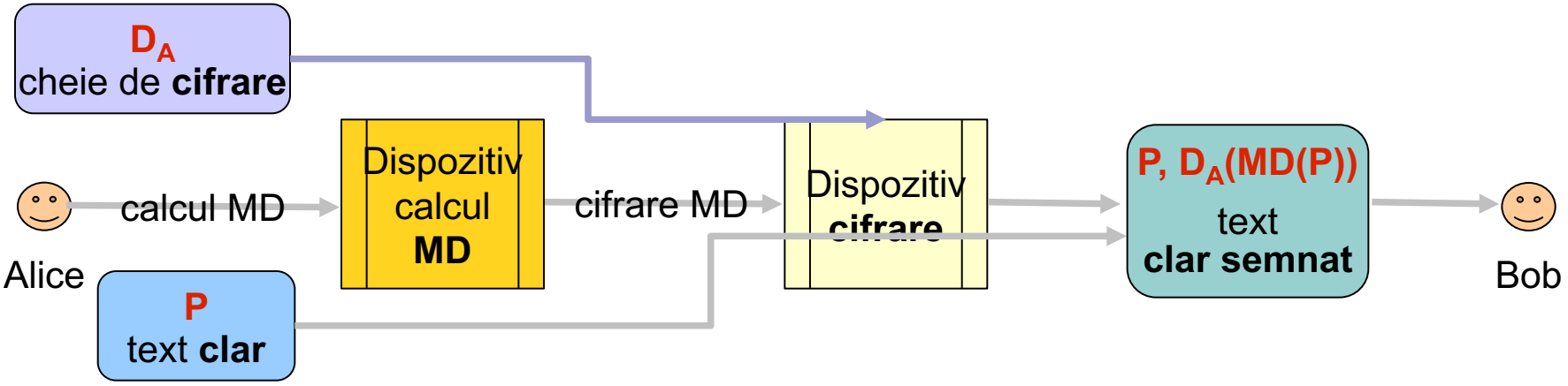
Protocoale de securitate

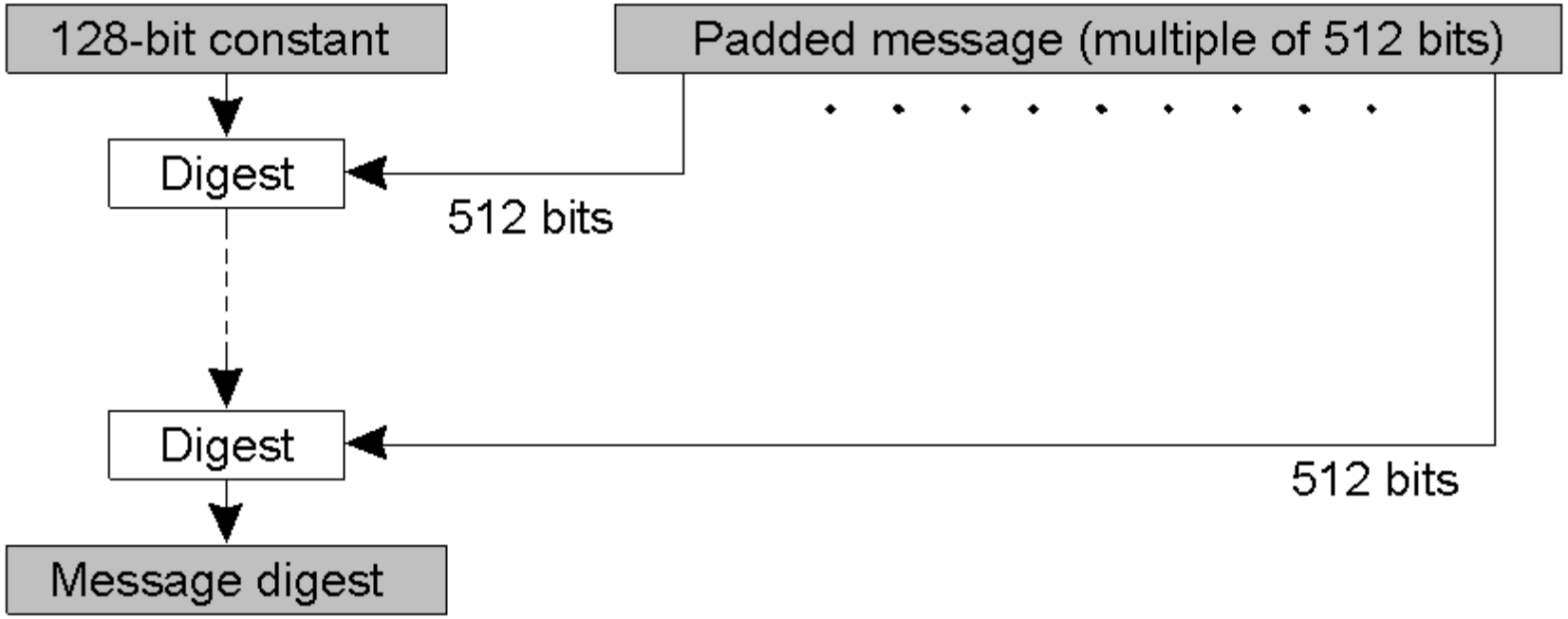
Rezumatele mesajelor

- Rezumat al mesajului (Message Digest, MD): caracterizează mesajul.
- Proprietăţi:
  - Cunoscând P, este uşor să se calculeze MD(P).
  - Cunoscând MD(P), este practic imposibil să se afle P.
  - Cunoscând P nimeni nu poate găsi P’ astfel ca MD(P’) = MD(P).
  - O schimbare de **1 bit** a intrării produce o ieşire **mult** diferită.



Funcţii hash: MD5

- MD5: Message Digest 5
  - Calculează un rezumat de mesaj pe 128 biţi.
  - Structura algoritmului MD5 – faze:



Funcţii hash: MD5 (2)

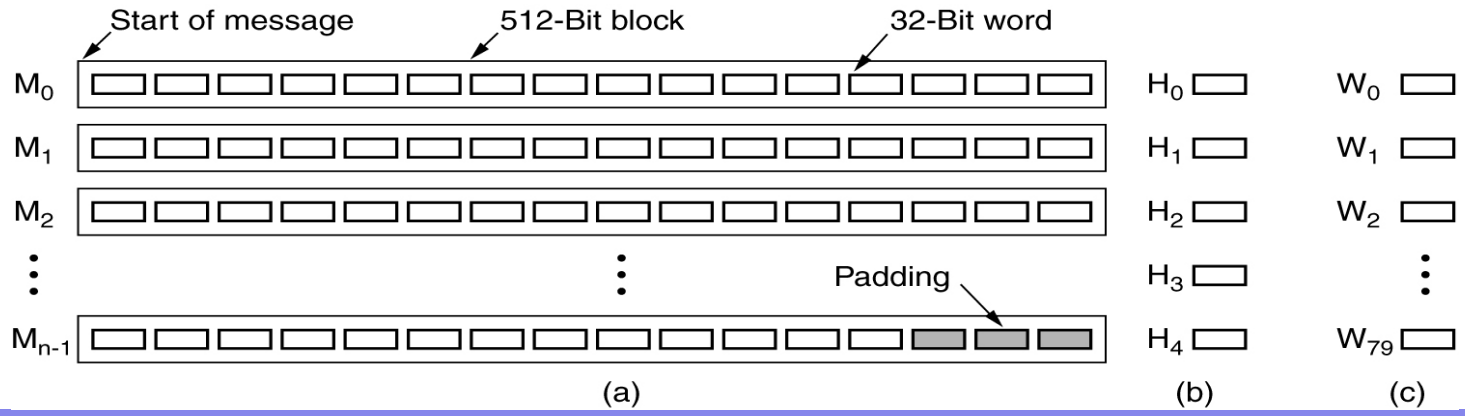
- O fază corespunde unui bloc de mesaj de 512 biţi şi are 4 runde.
  - O rundă are 16 iteraţii.
- F = funcţie utilizată în prima rundă (similar G, H, I sunt funcţii pentru rundele următoare):
  - F(x,y,z) = (x AND y) OR ((NOT x) AND z)
  - Notaţii (<<< e rotaţie stânga):
    - b0,…, b15 – sub-blocuri 32-biţi
    - p, q, r, s – variabile
    - C1. …. C16 – constante

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

Funcţii hash: SHA-1

- Secure Hash Algorithm 1:
  - (a) Mesaj completat la multiplu de 512 biţi.
  - (b) Variabilele de iesire H_0 .. H_4 (5*32 biţi – acumulează rezumatul).
  - (c) Tabloul de cuvinte W_0-W_{79}.
  - Algoritm:

```
Blocul M0 copiat în W0 .. W15
Alte 64 cuvinte umplute cu combinaţii ale primelor cuvinte
Variabilele A .. E iniţializate cu H0 .. H4 şi mixate cu combinaţii
  ale W0-W79
Rezultatele din A .. E sunt mixate cu H0 .. H4
Operaţii repetate pentru M1 .. Mn-1
```

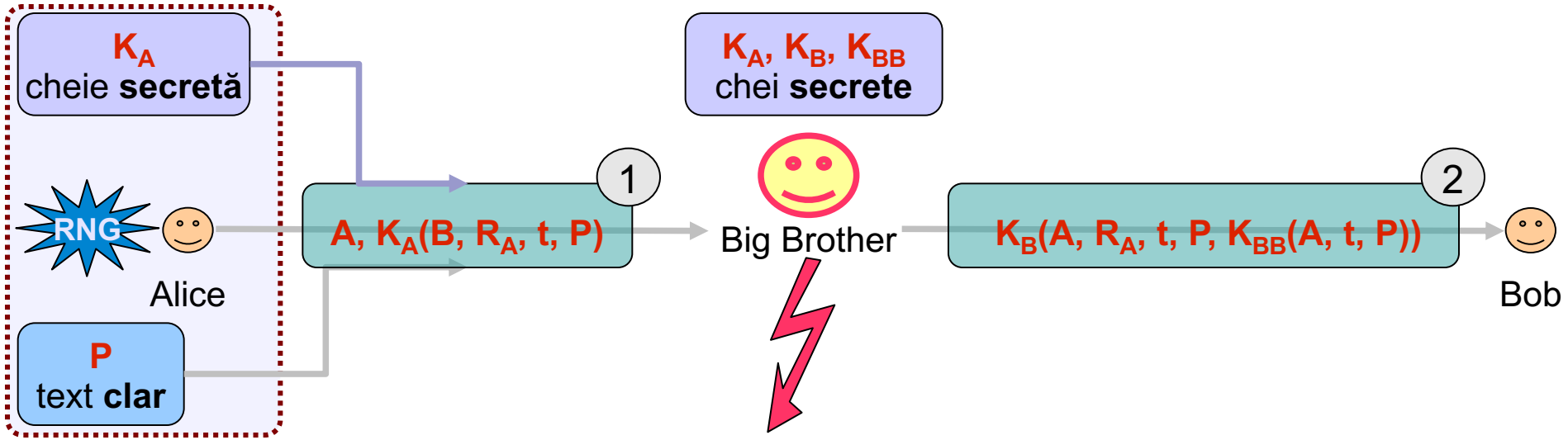


Semnături digitale

- Echivalentul unei semnături pe hârtie, în format electronic.
- Bazate pe:
  - Chei simetrice.
  - Chei publice.
- Rezumate de mesaje.
- Semnătura poate fi trimisă:
  - Împreună cu textul clar, într-un singur mesaj.
  - Separată de textul clar, în 2 mesaje.

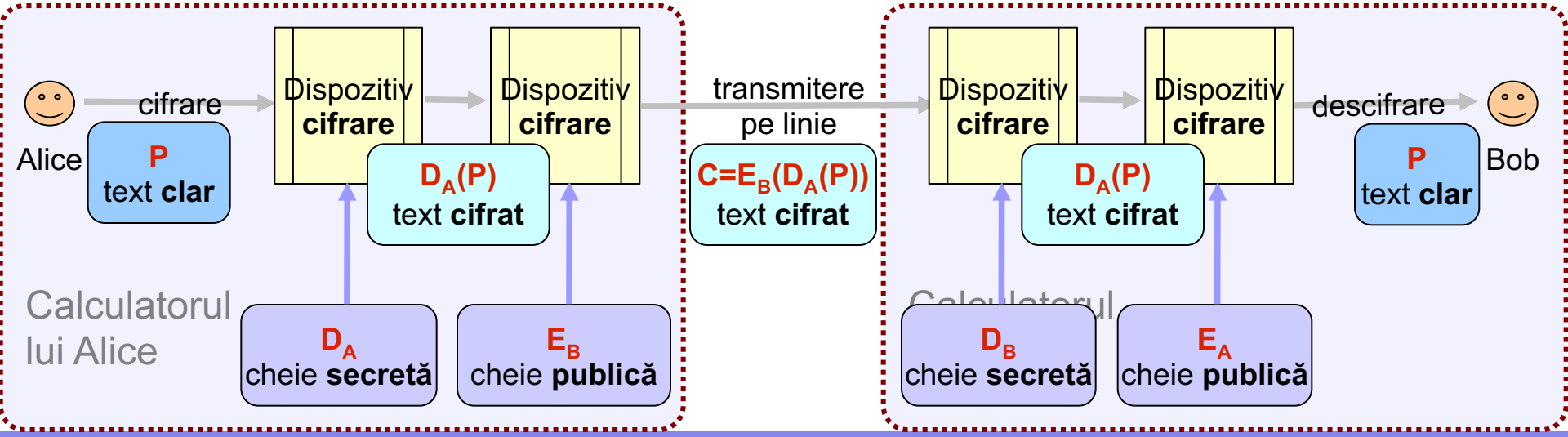
Semnături cu chei secrete (simetrice)

- Semnături digitale cu **Big Brother**:
  - R_A – număr aleator (control replici).
  - t – timestamp (mesaj recent).
  - K_A – cheia secretă a lui A.
  - K_B – cheia secretă a lui B.
  - K_{BB} – cheia secretă Big Brother.



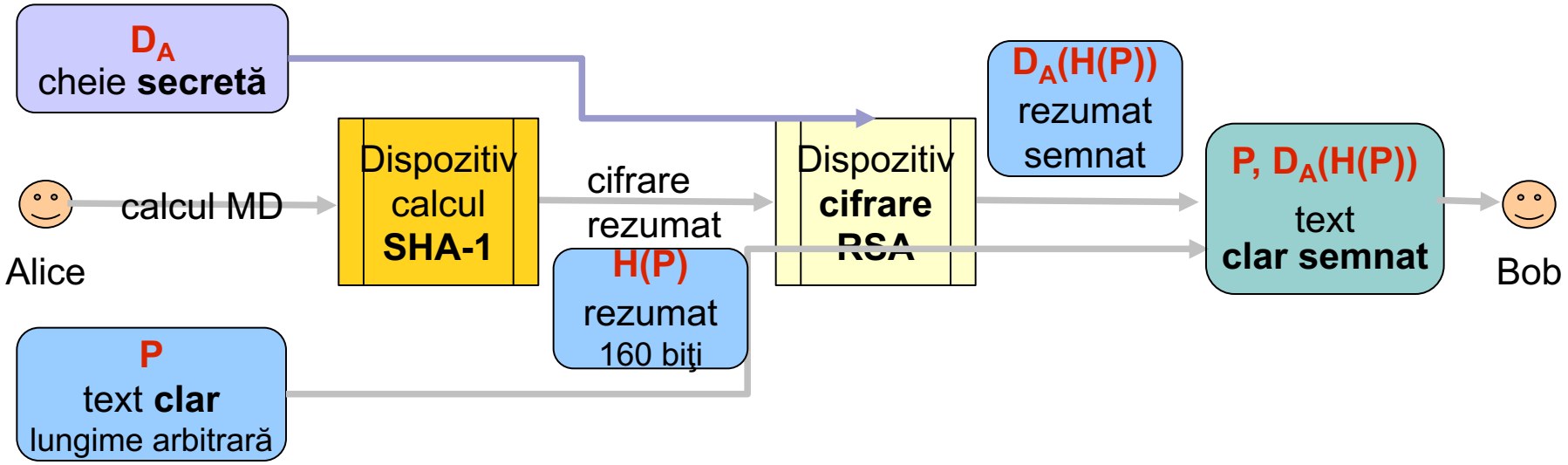
Semnături cu chei publice (asimetrice)

- Condiţii:
  - D(E(P)) = P
  - E(D(P)) = P
- Algoritmi:
  - RSA: bazat pe factorizare numere mari)
  - DSS (Digital Signature Standard): bazat pe logaritmi discreţi.



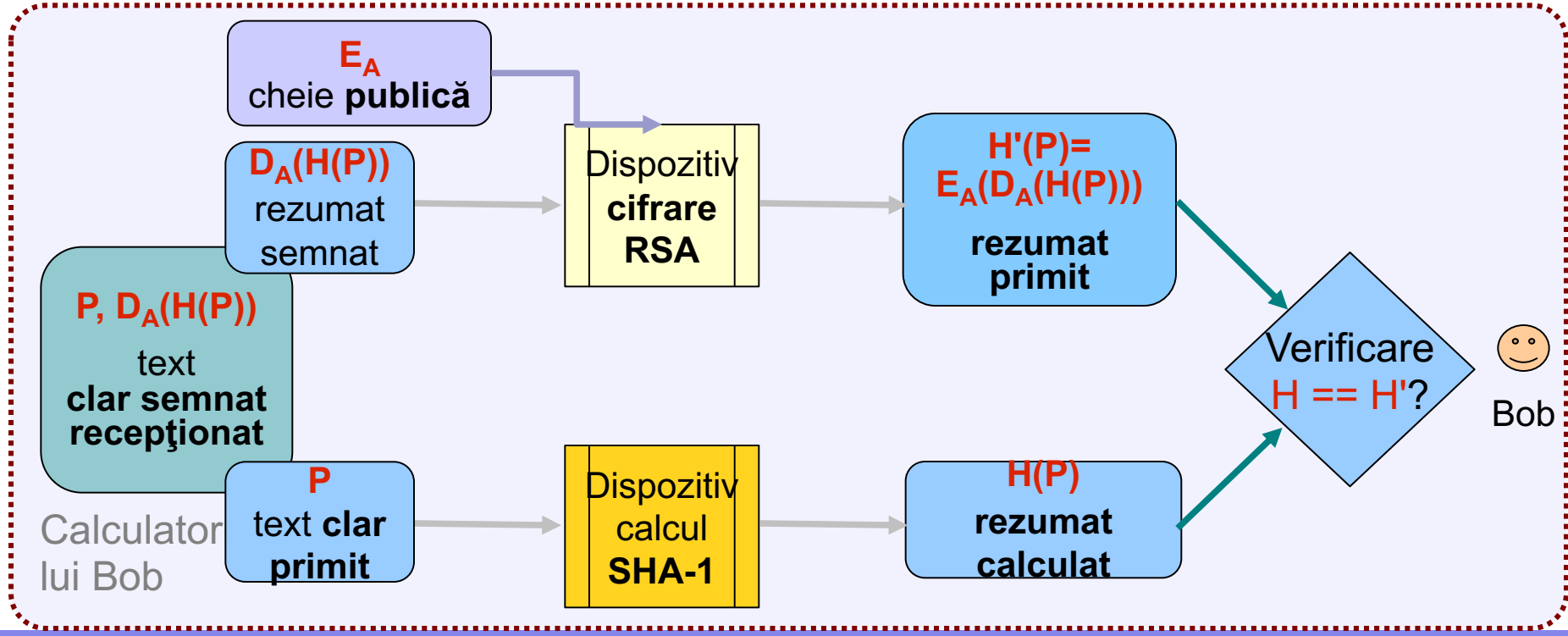
Semnare mesaje nesecrete

- Utilizarea SHA-1şi RSA pentru semnarea mesajelor nesecrete:



Verificare semnatură digitală

- Se calculează rezumatul mesajului clar recepţionat H(P).
- Se decriptează semnătura $H'(P)=E_A(D_A(H(P)))$
- Se compară cele 2 valori H'(P) şi H(P):
  - Egalitatea confirmă că mesajul este cel iniţiat de Alice.

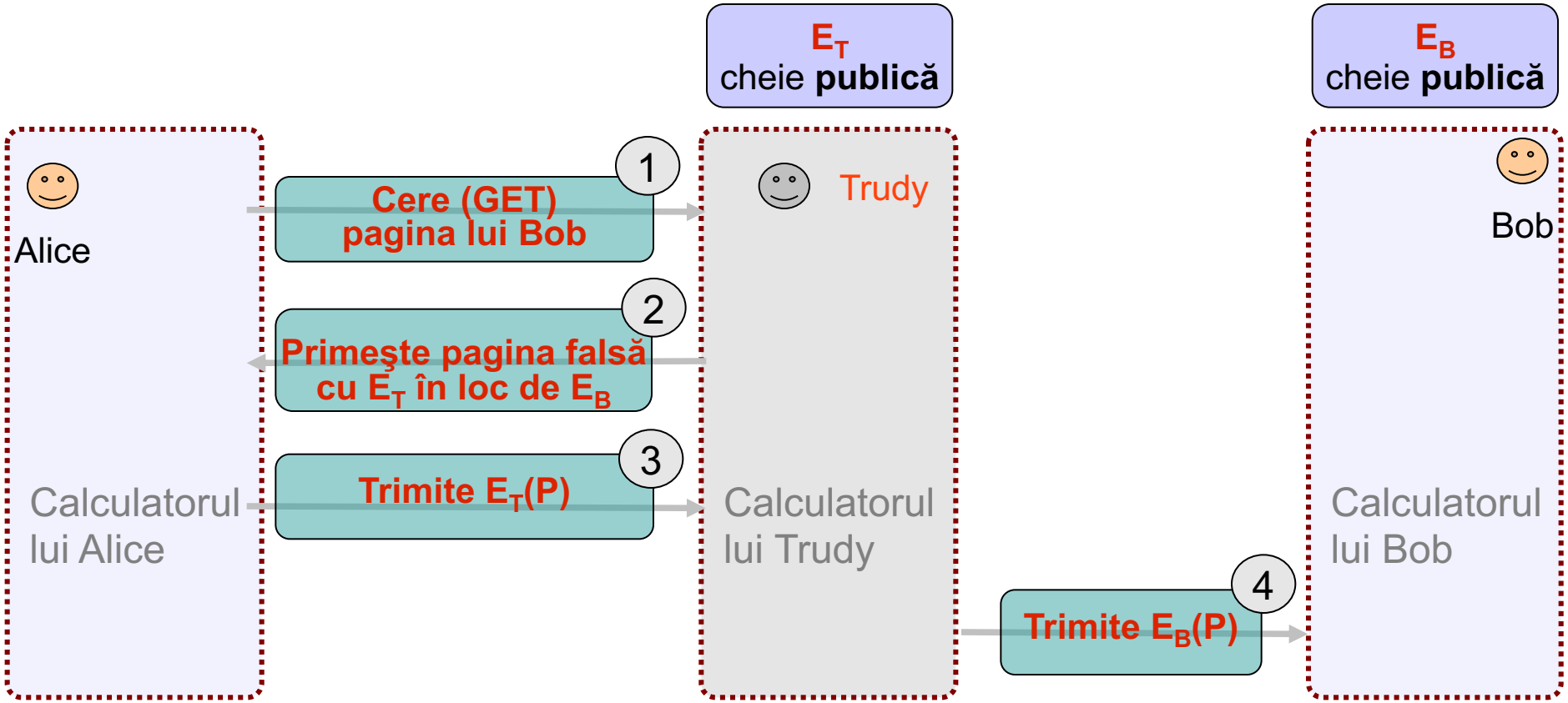


Managementul cheilor publice

- Certificate.
- X.509.
- PKI (Public Key Infrastructure).

Probleme cu cheile publice

- Problema: difuzarea cheii publice prin pagina de referinţă a proprietarului.



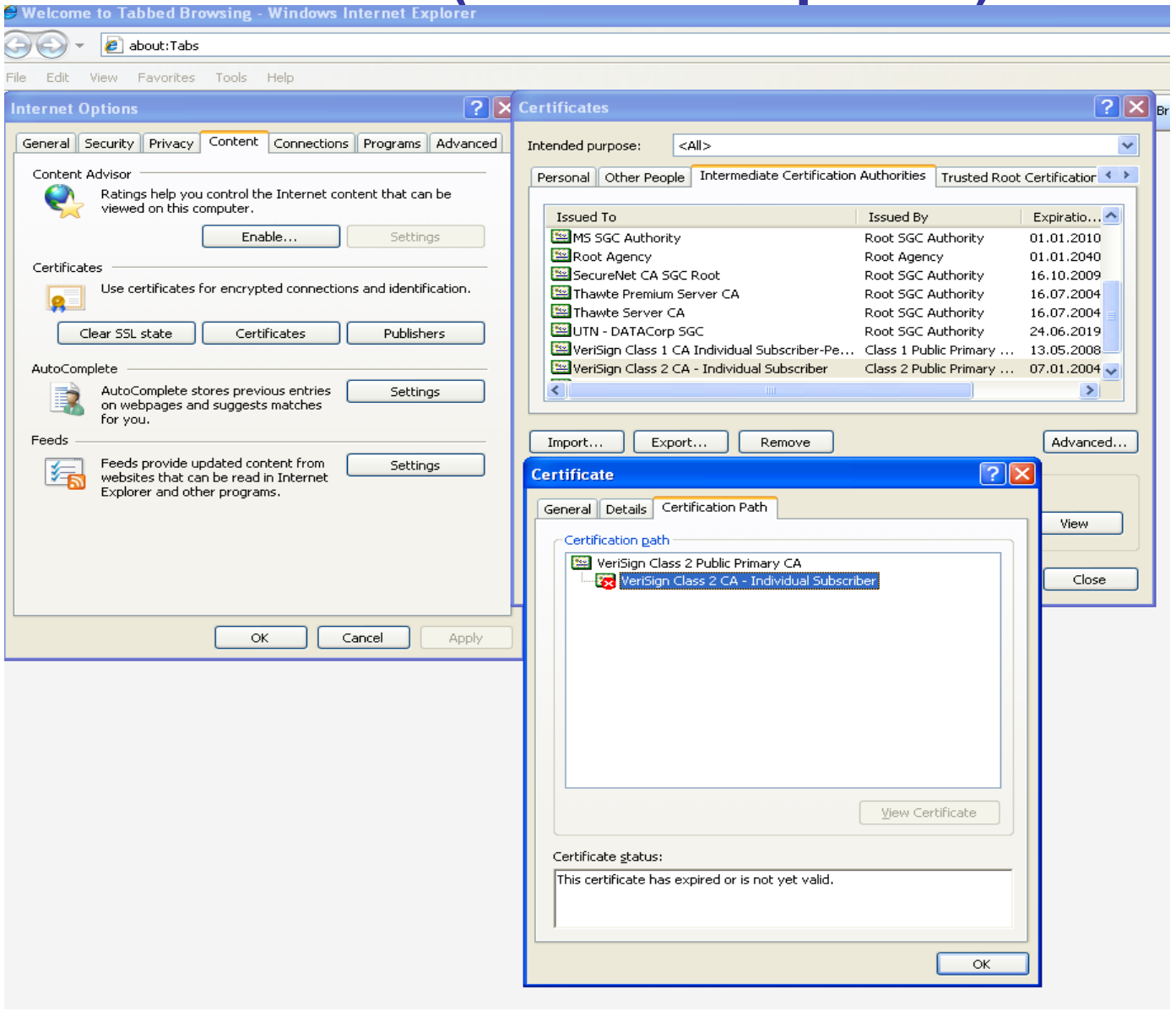
Certificate

- Un certificat e semnat de o autoritate de certificare CA (Certificate Authority).
- Rol: leagă cheia publică de un proprietar (principal) sau de un atribut.

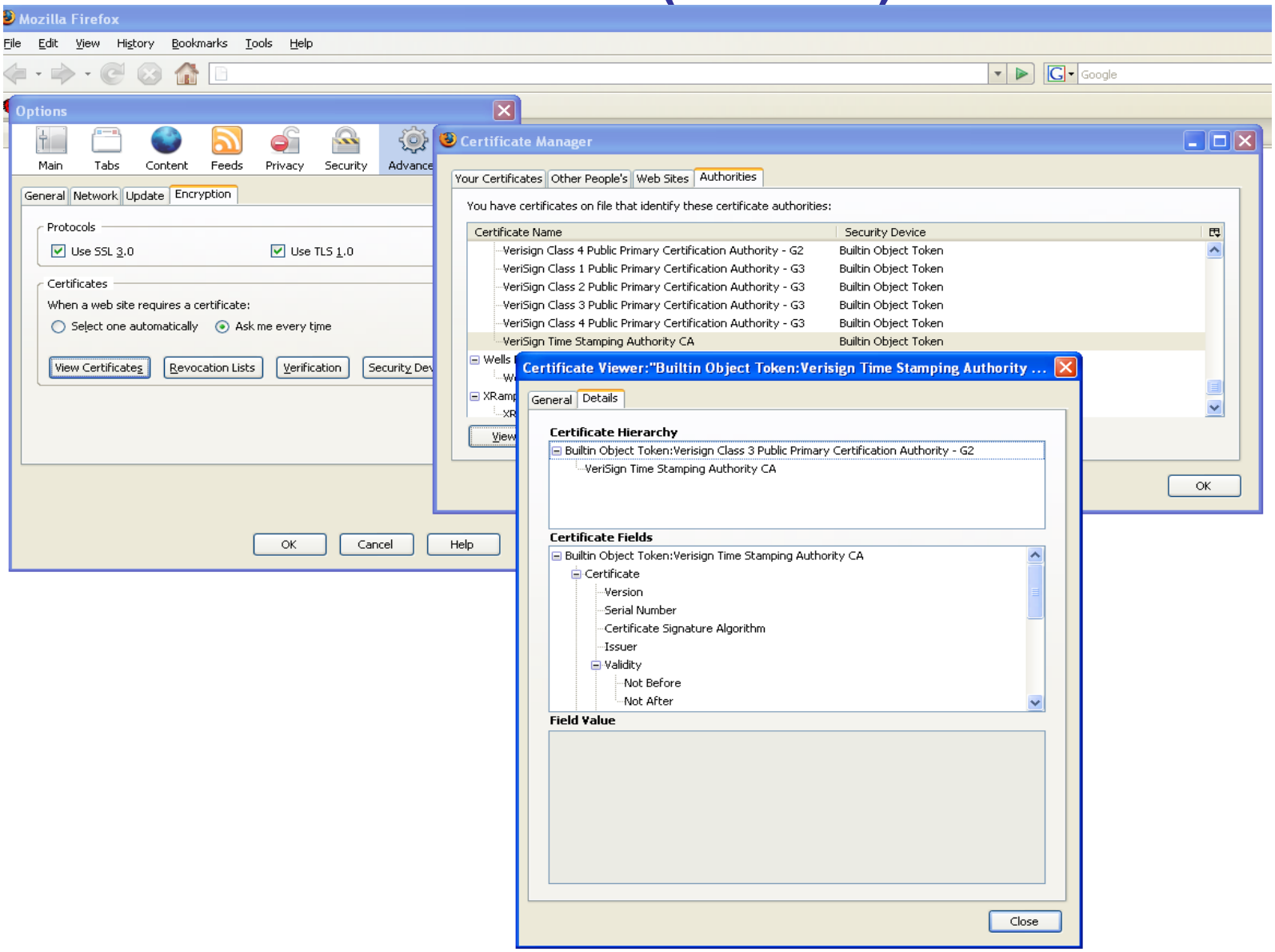
I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

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

Certificate (Internet Explorer)



Certificate (Firefox)



X.509

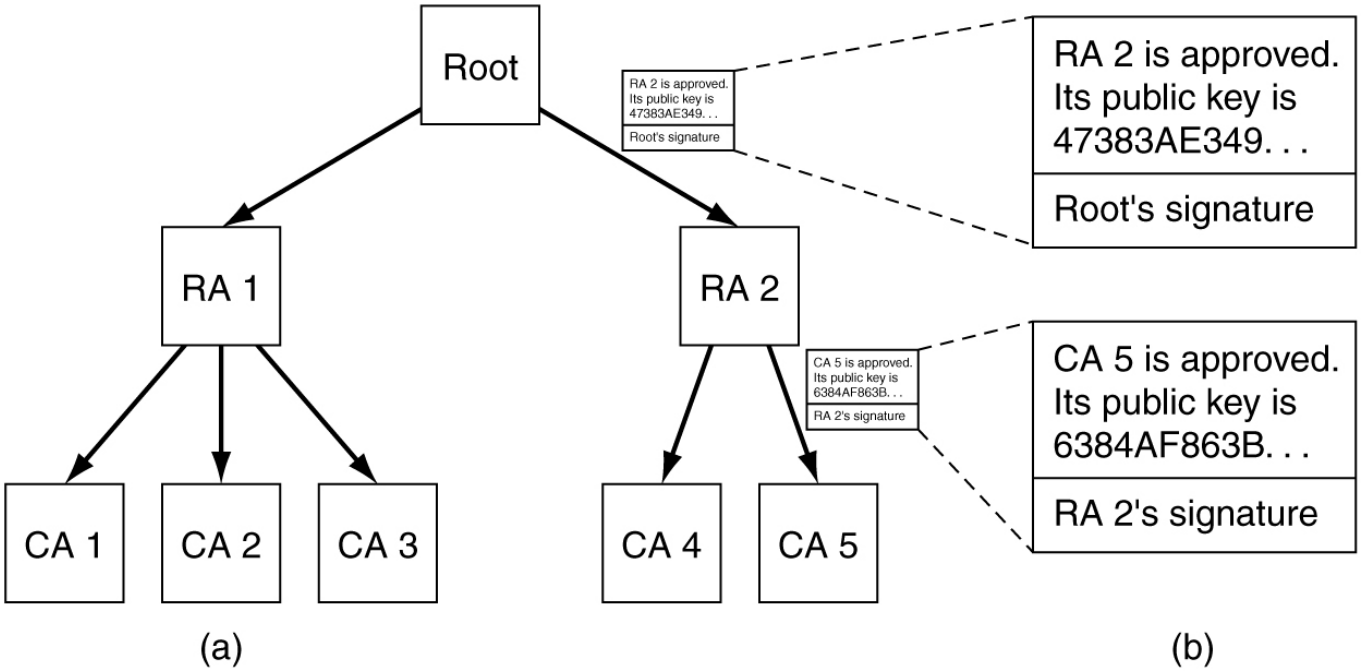
- Câmpurile de bază dintr-un certificat X.509:

Câmp	**Semnificaţie**
Versiune	Ce versiune de X.509 este utilizată
Număr de serie	Împreună cu numele CA identifică în mod unic certificatul
Algoritm de semnare	Algoritmul folosit la semnarea certificatului
Emitent	Numele X.500 al CA-ului
Perioada de validitate	Dată prin momentele de început şi sfârşit
Numele subiectului	Entitatea care este certificată
Cheia publică	Cheia publică a subiectului şi ID-ul algoritmului folosit
ID emitent	Un ID opţional identificând în mod unic emitentul certificatului
ID subiect	Un ID opţional identificând în mod unic subiectul certificatului
Extinderi	Au fost definite mai multe extinderi
Semnătura	Semnătura certificatului (semnat cu cheia privată a CA)

Public Key Infrastructure

- PKI
  - Set de componente (hardware şi software) care lucrează împreună pentru utilizarea sigură a tehnologiei de chei publice.
- CA
  - Autoritate de încredere care certifică faptul că cheia publică inclusă aparţine persoanei cu numele ataşat.
  - CA: administraţie centrală care eliberează certificate:
    - Organizaţie sau companie: pentru angajaţi.
    - Universitate: pentru studenţi.
    - CA publice (VeriSign): pentru clienţi.

Public Key Infrastructure



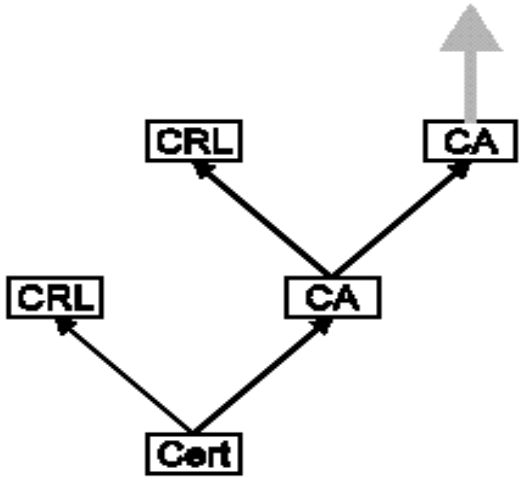
- (a) PKI ierarhic. (b) Un lanţ de incredere (certification path).
  - RA – Regional Authority
  - CA – Certificate Authority

Revocarea certificatelor

- Un certificat trebuie revocat când:
  - Cheia primară (secretă) este compromisă;
  - Cheia primară este pierdută;
  - O persoană pleacă din companie.
- Revocarea trebuie cunoscută de toţi utilizatorii:
  - Se folosesc liste de revocare (Certificate Revocation List CRL);
  - Greu de implementat şi folosit.

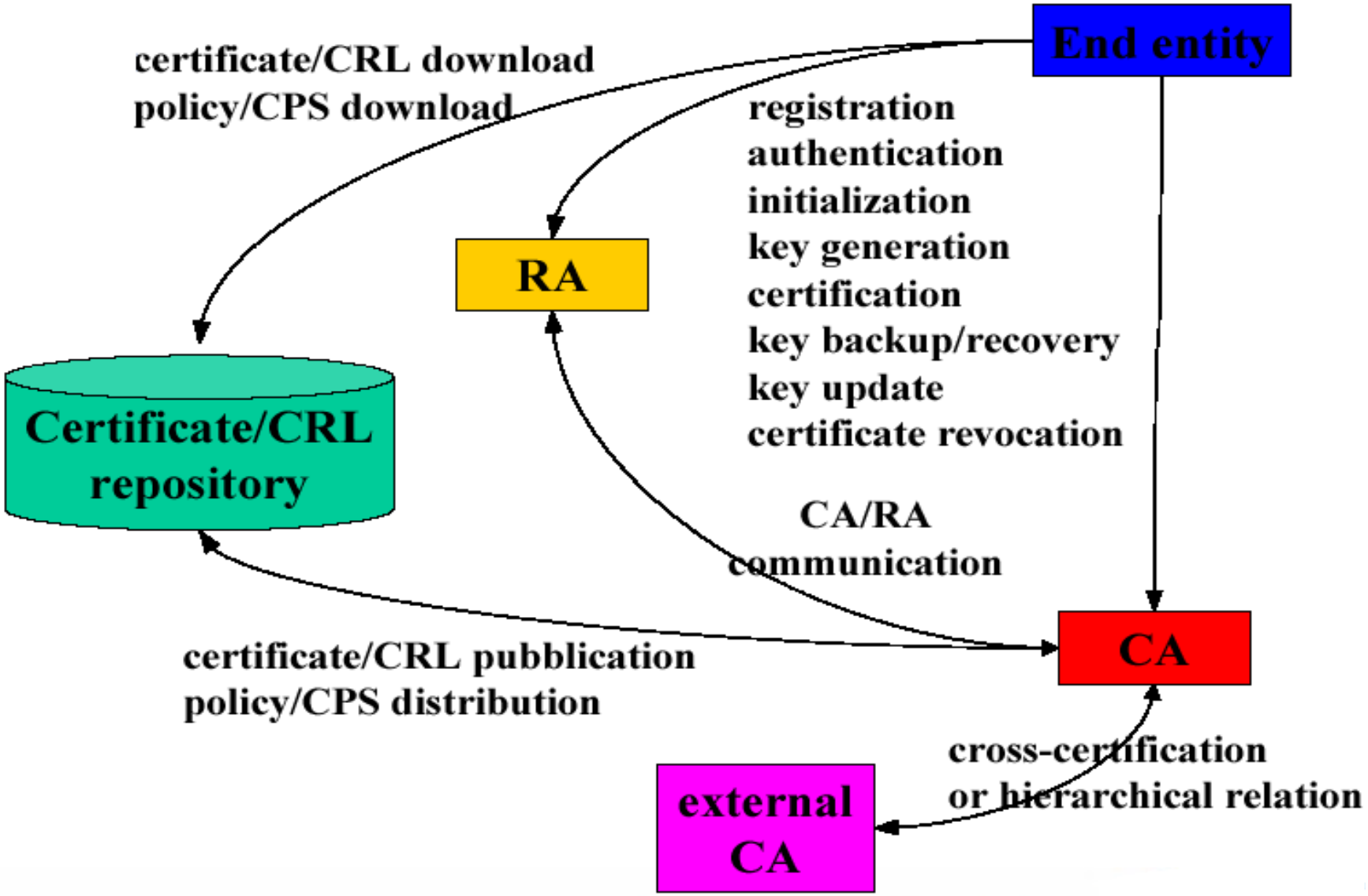
Verificarea revocării certificatelor

Checking works in reverse order to normal lookup



Check certificate
Check certificates CRL
repeat
    Check CA's certificate
    Check CA's CRL
until root reached

Componente PKI



Standarde având ca suport PKI

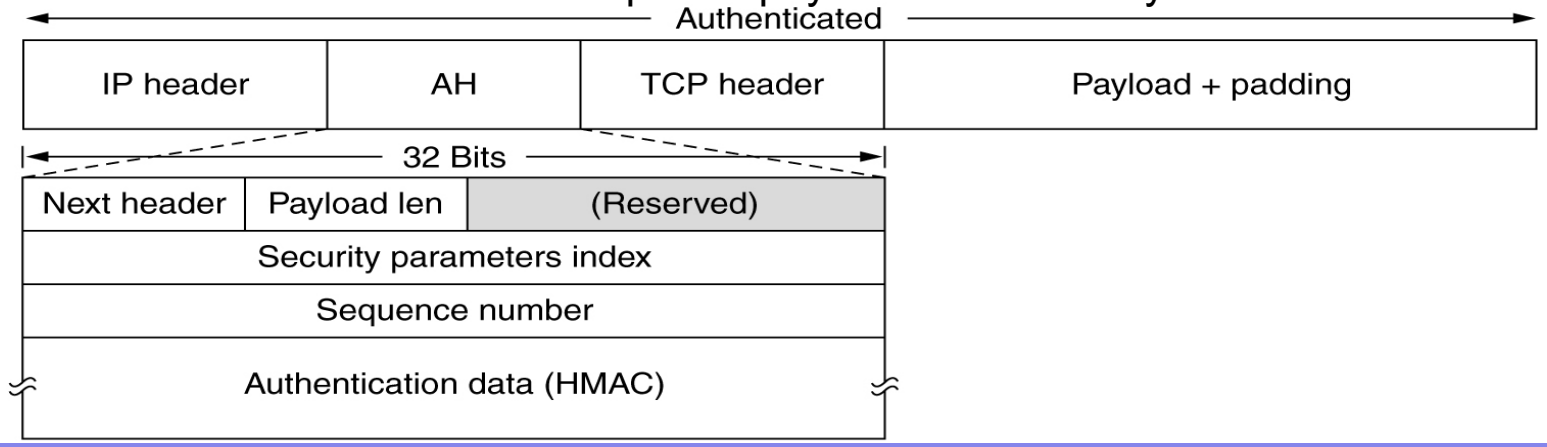
- S/MIME:
  - Standard IEFT pentru mesagerie sigură;
  - PKI pentru mesaje şi ataşamente.
- SSL/TLS:
  - Acces sigur la servere Web.
- SET:
  - Secure Electronic Transactions.
- IPSec
  - În VPN pentru criptare şi autentificare.

Securitatea comunicaţiei

- IPsec
- Ziduri de protecţie (Firewalls)
- Virtual Private Networks (VPN).

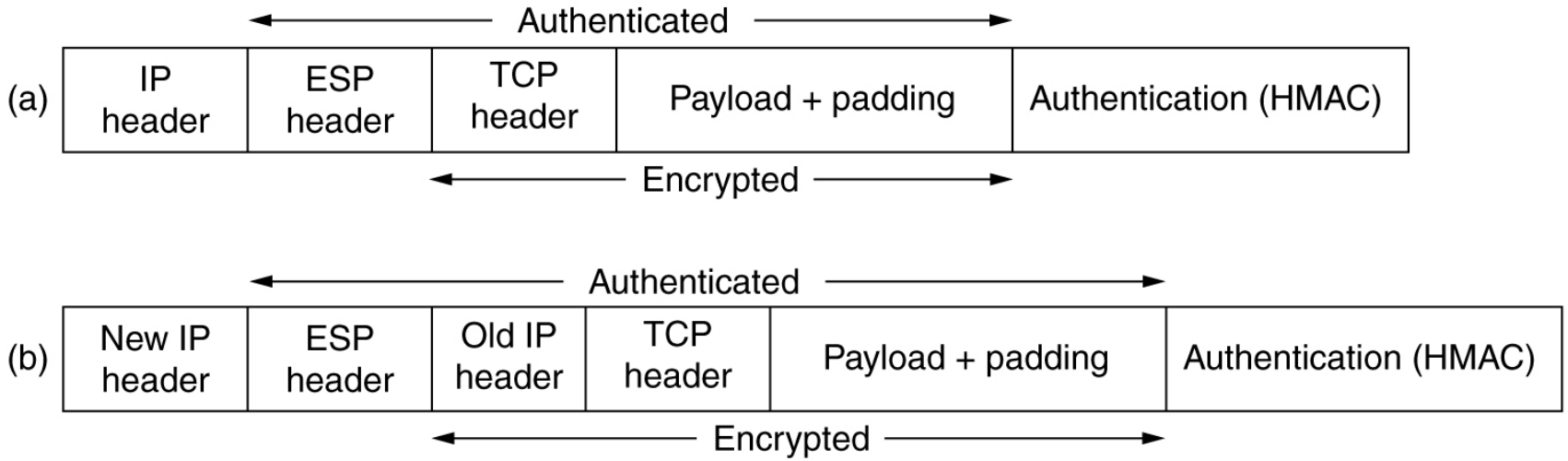
IPsec

- Are două părţi:
  - Descriere antet (discutat aici)
  - Generare chei
- IPsec folosit in modurile transport şi tunel.
  - Authentication header în mod transport pentru IPv4.
    - Security parameter index: indică înregistrarea care conţine shared key.
    - Sequence number: detectează atacuri prin replică.
    - HMAC: Hashed Message Authentication Code.
      - Foloseşte shared key.
      - Calculează rezumatul pentru payload + shared key.



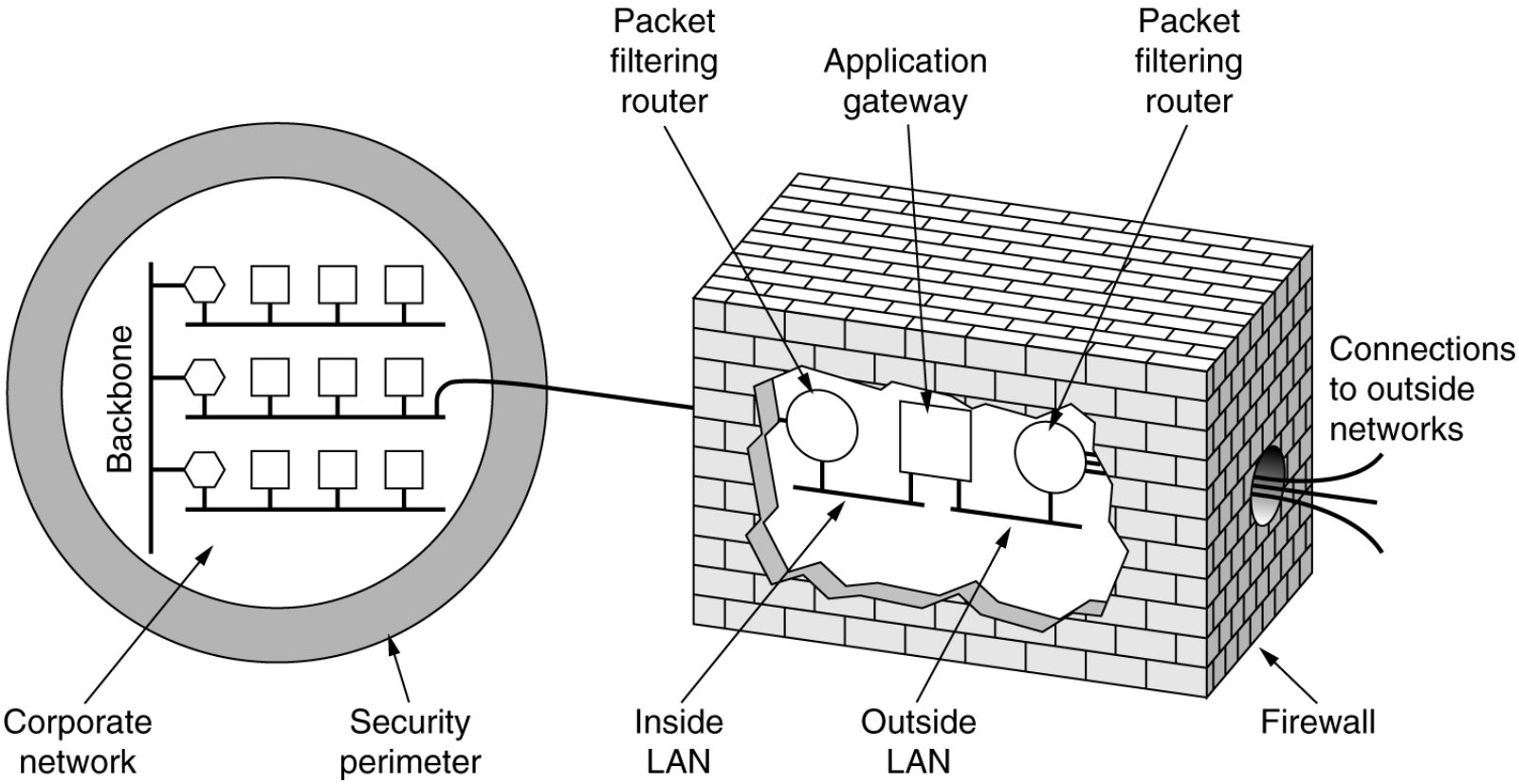
IPsec

- ESP: Encapsulating Security Payload
  - Security parameters index
  - Sequence number
  - Initialization vector (pentru criptare date)
  - HMAC – Hashed Message Authentication Cod
- (a) ESP în mod transport, (b) ESP în mod tunel:



Firewalls

- Firewall: două rutere de filtrare a pachetelor şi o poartă de nivel aplicaţie:

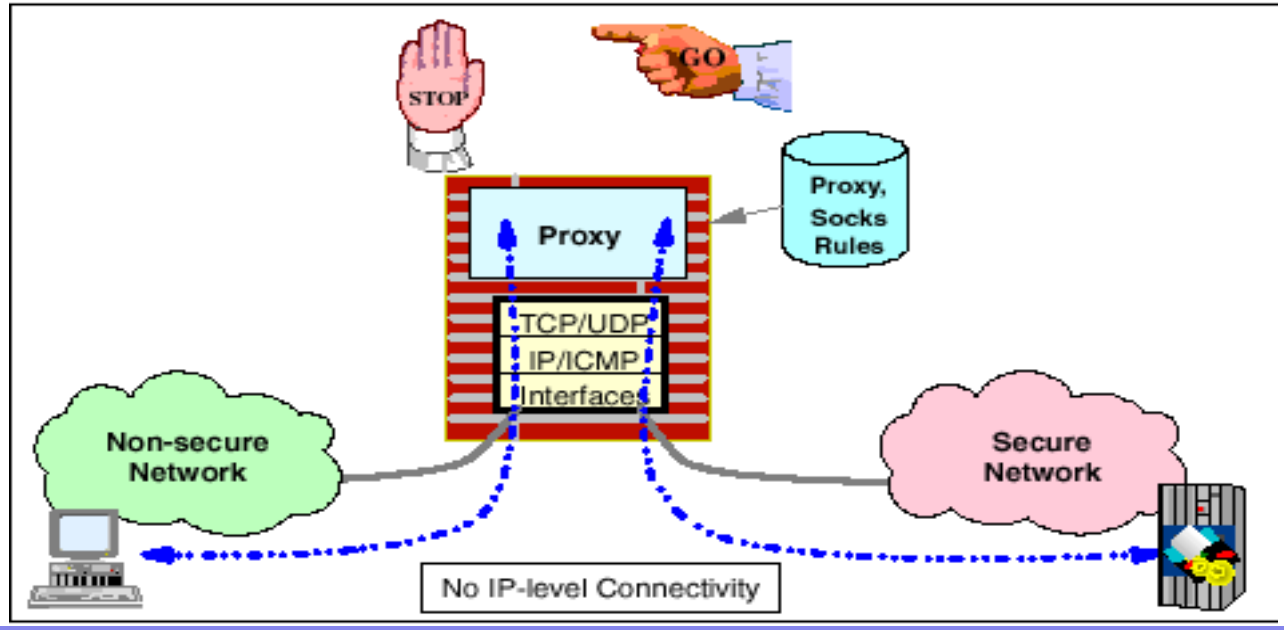


Filtrarea tradiţională de pachete

- Foloseşte reguli la nivel reţea.
- Filtrare după:
  - Adrese origine şi destinaţie.
  - Protocol (TCP sau UDP).
  - Numere port.
- Nepotrivit pentru medii care cer analiza mai detaliată pentru protocoale de nivel superior (adică proxy servers).

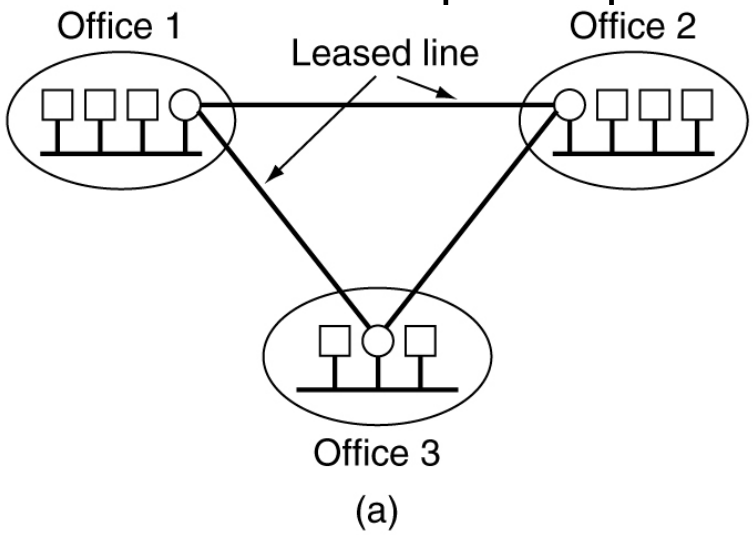
Nivel aplicaţie – gateway

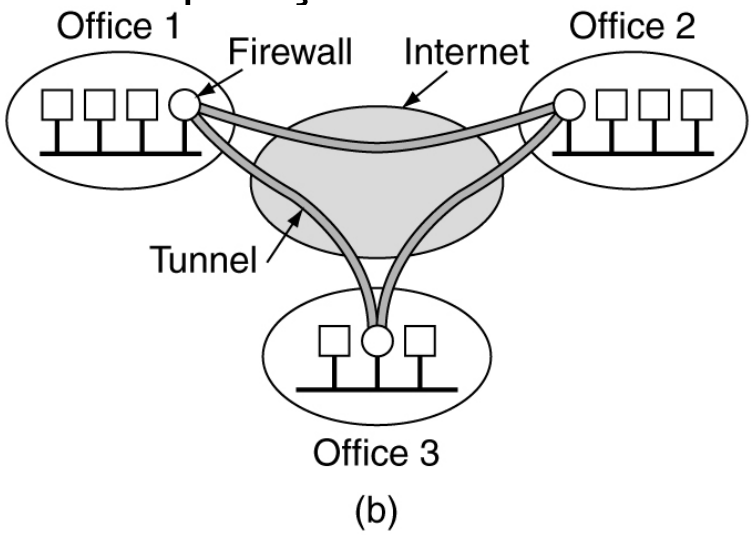
- Proxy de aplicaţie rulând pe firewall:
  - Pasează cererile către serviciile din reţeaua privată şi răspunsurile către clienţii din reţeaua publică:
    - Proxy SMTP poate accepta mail din Internet fără a devoala adresele interne de mail.
  - Autentifică credenţialele utilizator înainte de a permite accesul la reţeaua internă.
  - Foloseşte mecanisme de auditare şi logging (jurnalizare).



Virtual Private Networks

- Reţea privată:
  - (a) Cu linii închiriate.
  - (b) VPN.
- VPN se construiesc peste Internet:
  - Fiecare oficiu are un firewall, se crează tunele între firewalls.
  - IPsec folosit pentru tunneling (ESP în mod tunel).
  - În Internet pachetele apar ca şi cele obişnuite.
  - VPN este transparent pentru software de aplicaţii.



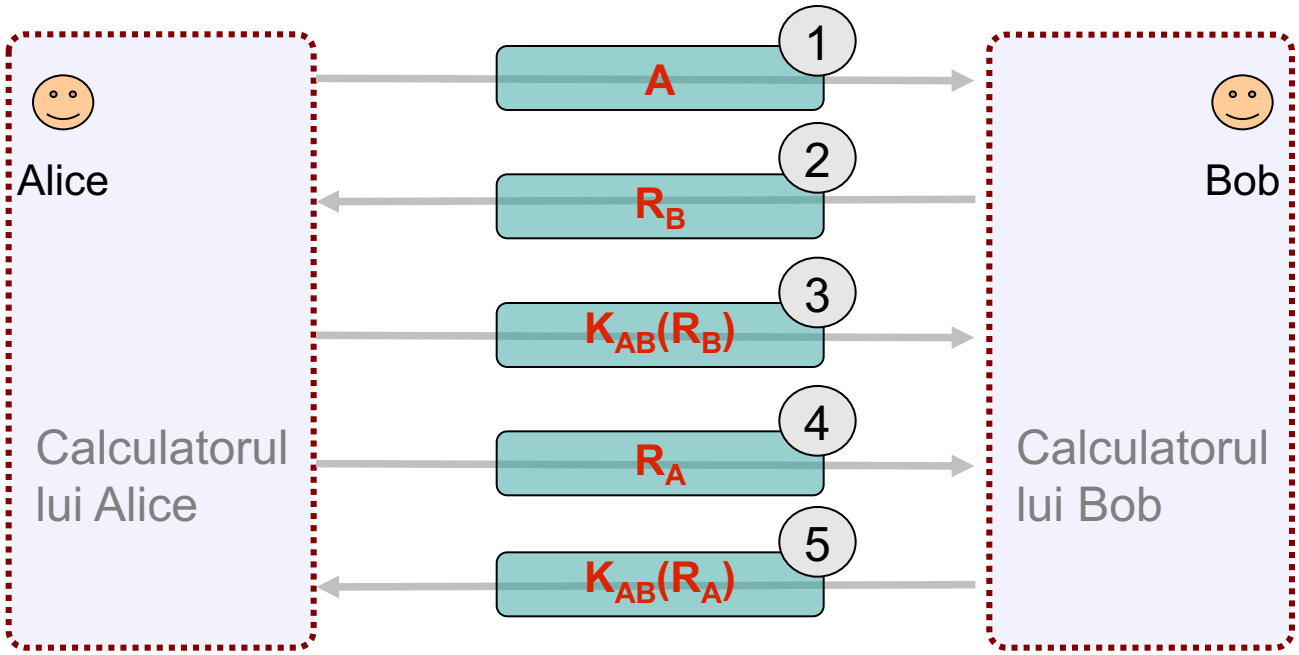


Protocoale de autentificare

- Folosesc:
  - Cheie secretă partajată.
  - Stabilirea unei chei partajate: Diffie-Hellman.
- KDC – Key Distribution Center.
- Kerberos.
- Public-Key Cryptography.

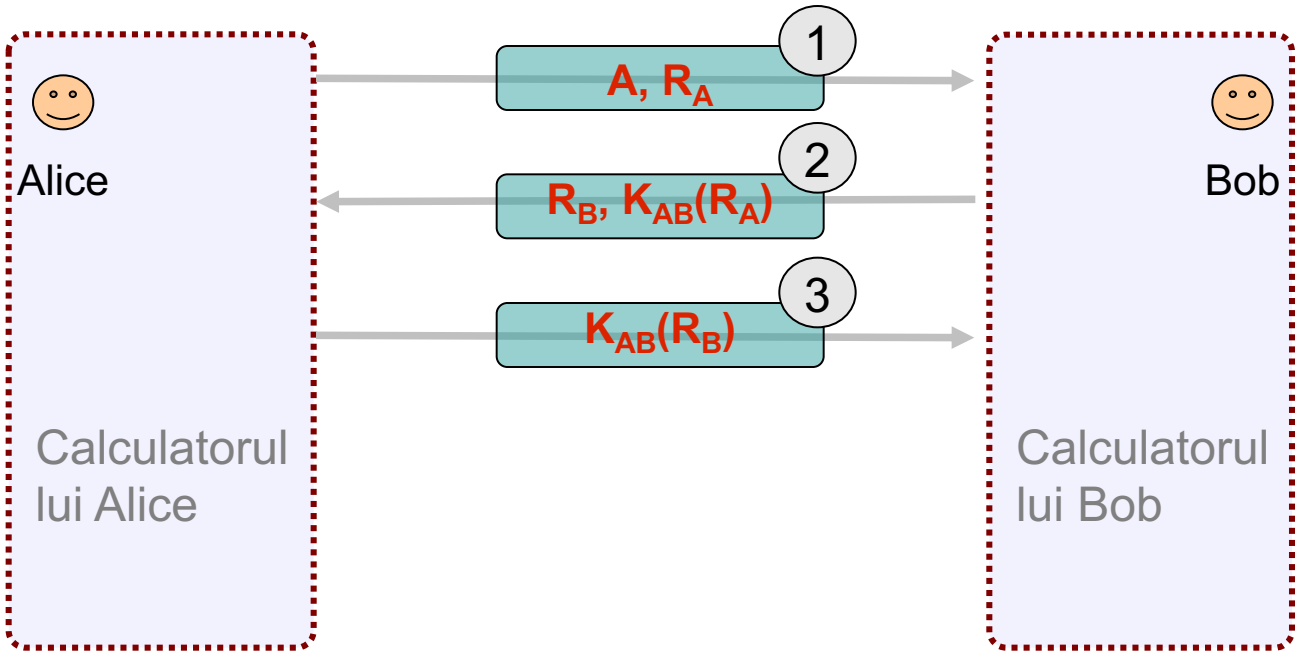
Autentificare cu cheie secretă partajată

- Autentificare reciprocă cu un protocol challenge-response:



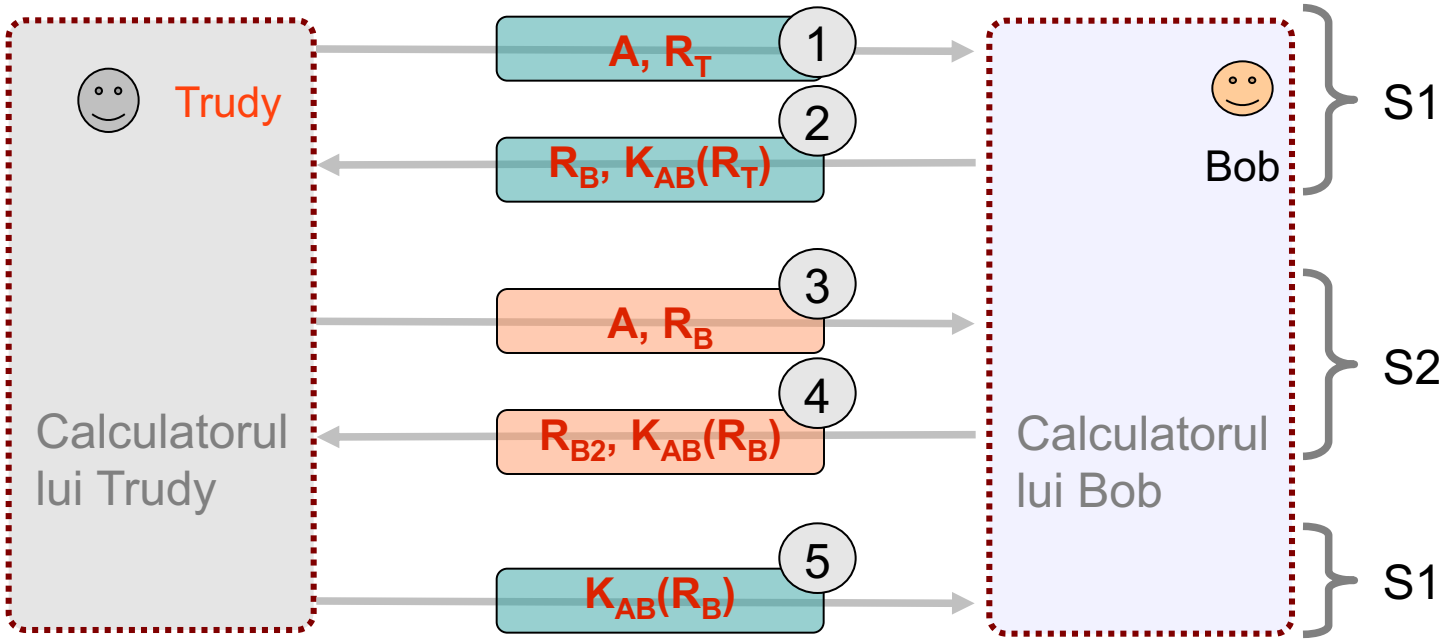
Autentificare cu cheie secretă partajată

- Reducere număr de paşi folosiţi:
  - Trimiterea mai multor informaţii la un pas:



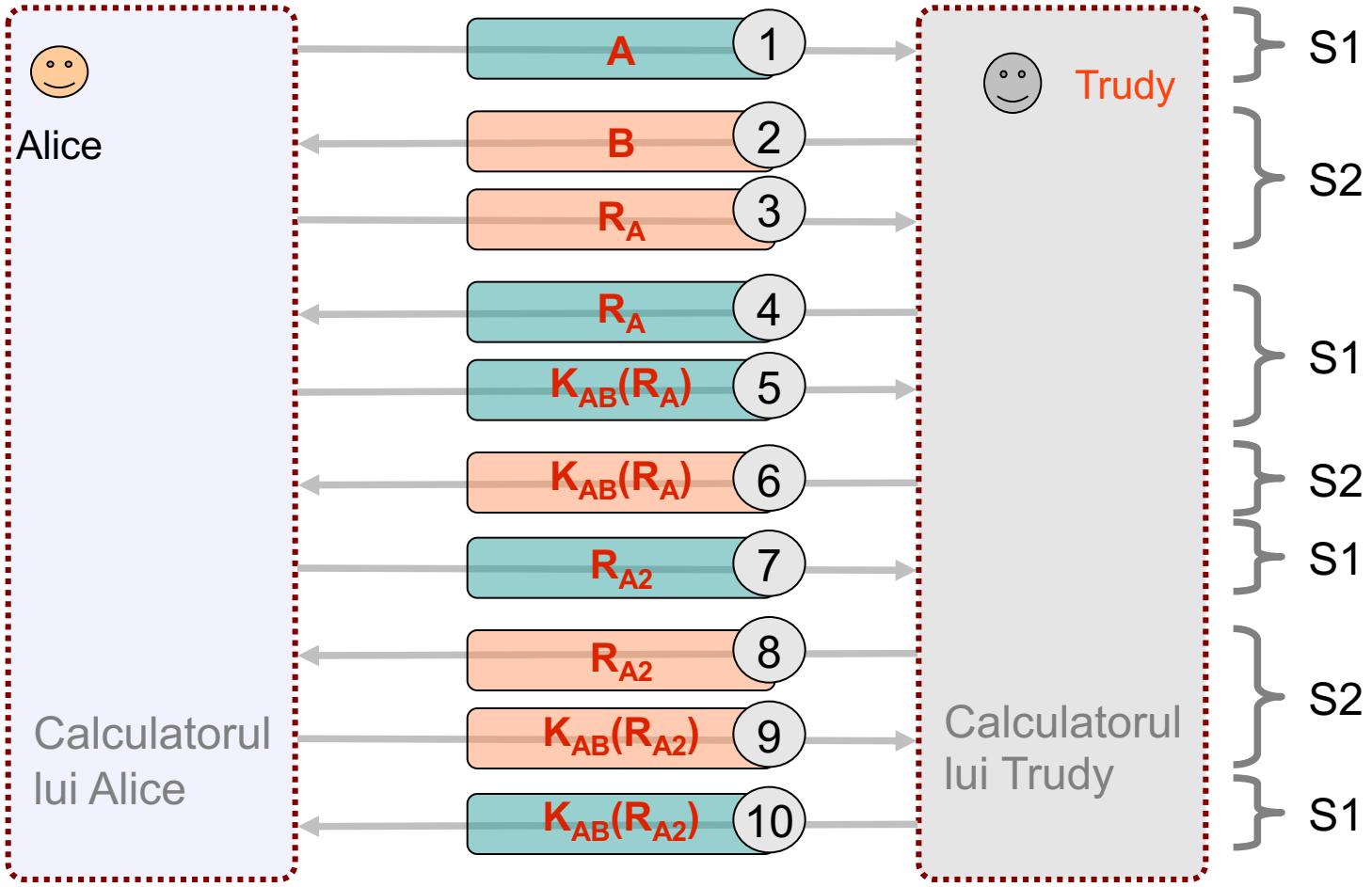
Autentificare cu cheie secretă partajată

- Atacul prin reflexie:
  - Trudy deschide 2 sesiuni şi foloseşte informaţia dintr-una în cealaltă:

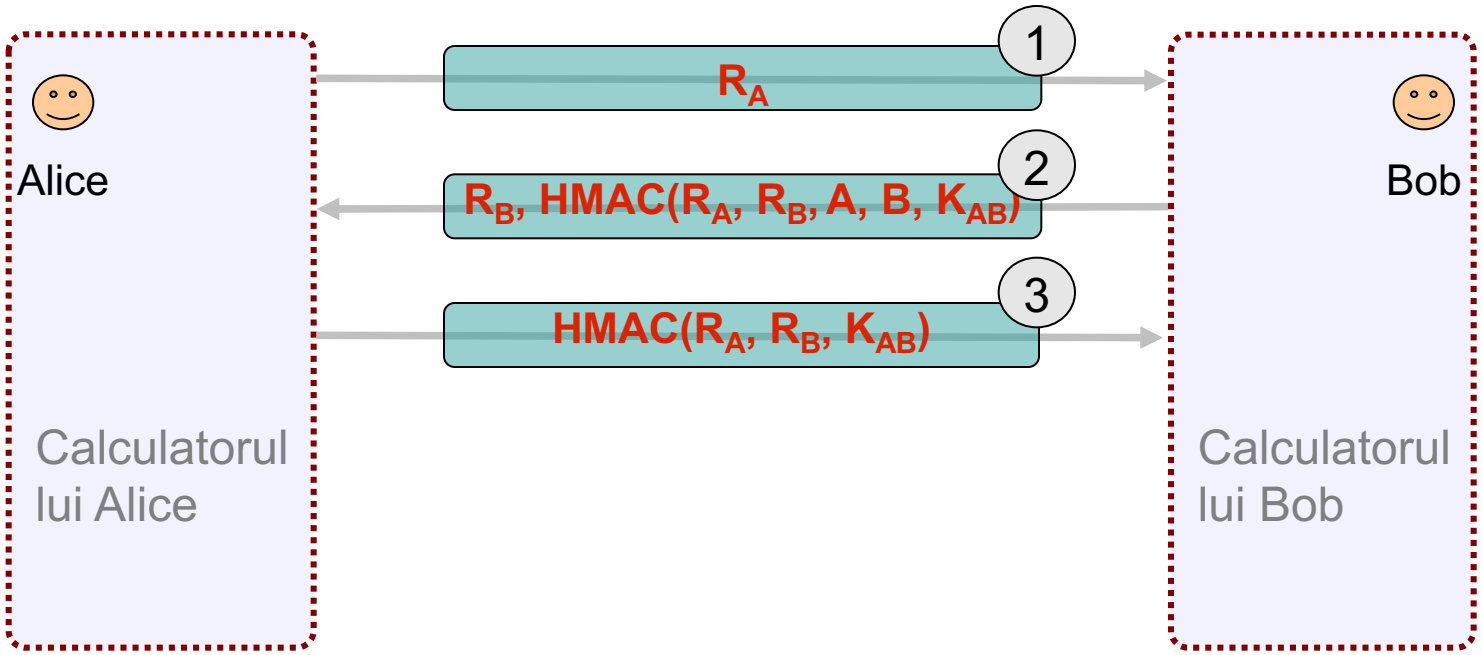


Autentificare cu cheie secretă partajată

- Atacul prin reflexie pe protocolul iniţial:

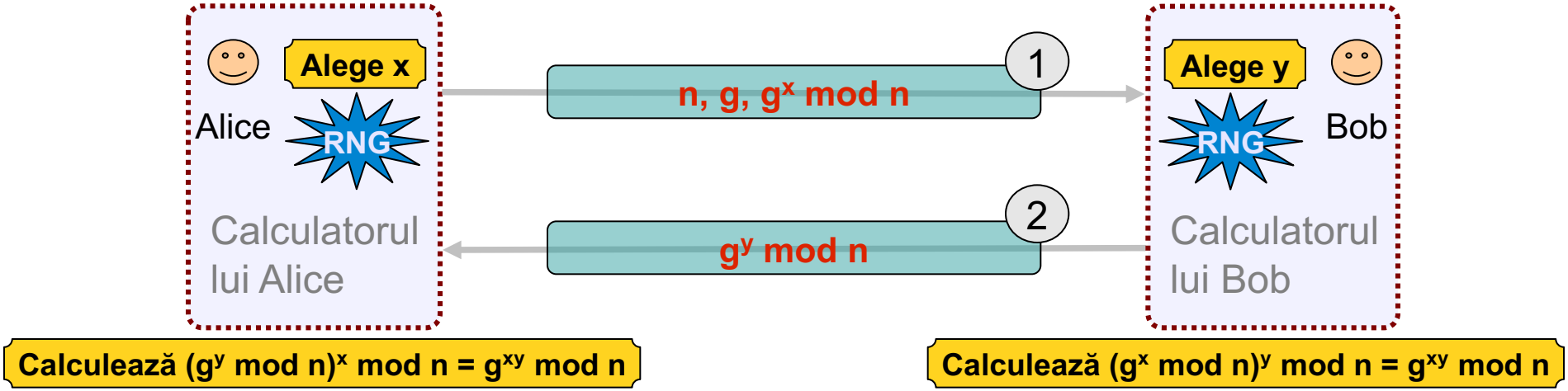


Autentificarea cu HMAC

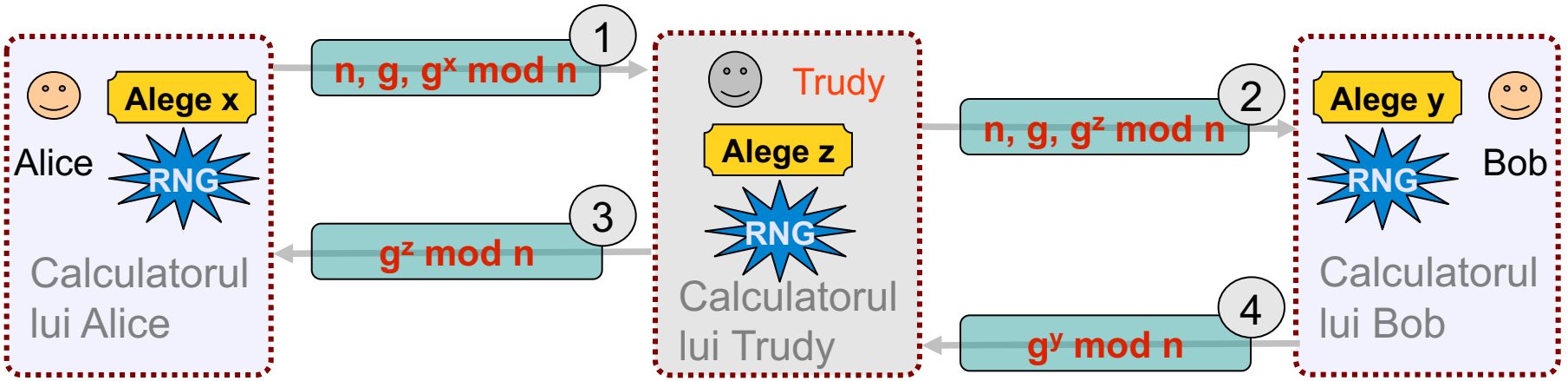


Stabilire cheie partajată: Diffie-Hellman

- Condiţii:
  - n, g – numere mari, x nu poate fi calculat din $g^x \bmod n$
  - n prim
  - (n-1)/2 prim
  - g îndeplineşte condiţii speciale

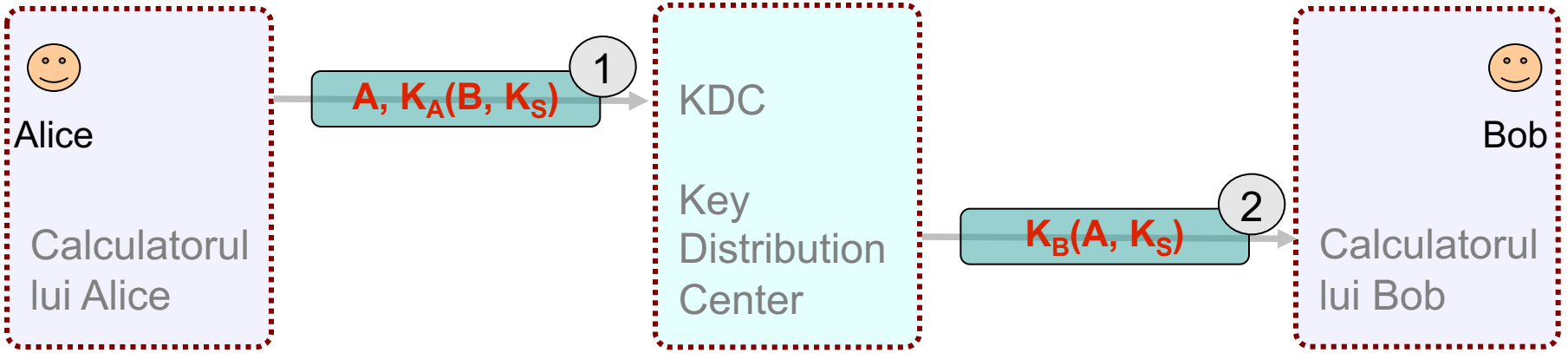


Atacul man-in-the-middle



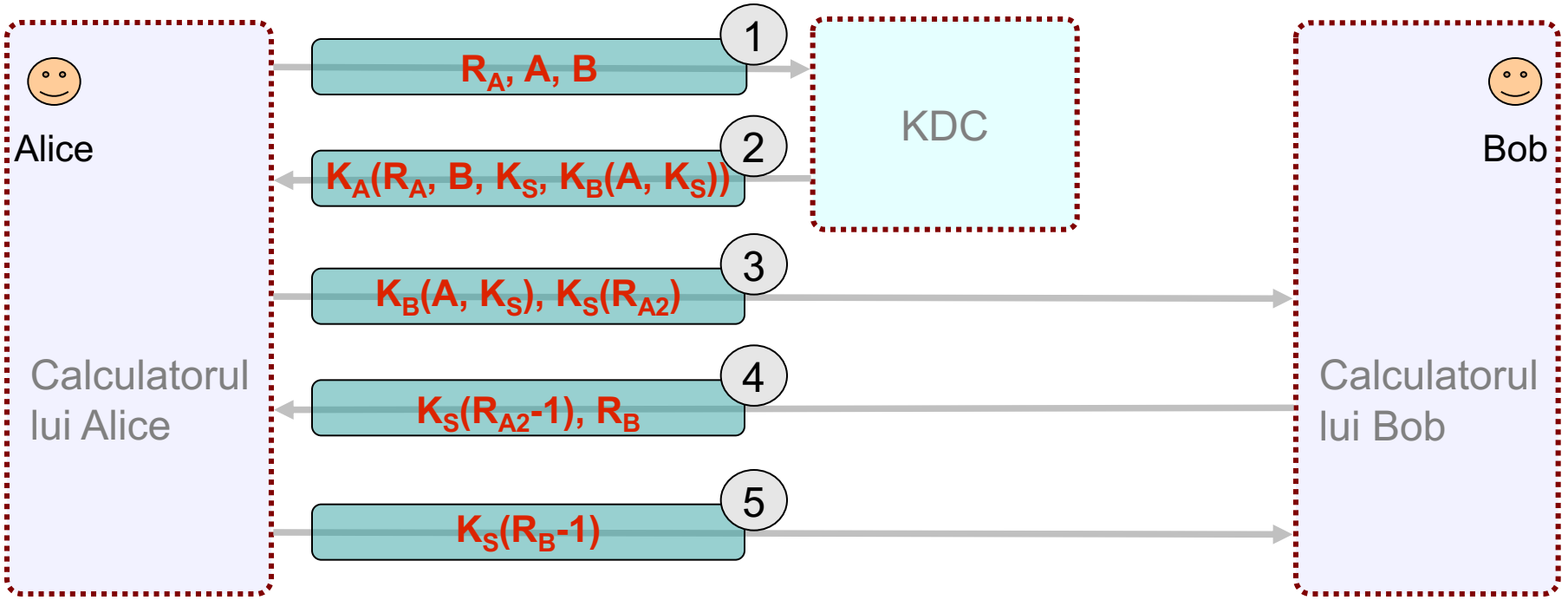
Autentificarea folosind Key Distribution Center

- Prima încercare:
  - Vulnerabil la replay attack – Trudy retransmite mesajul 2 (cu mesajul asociat).



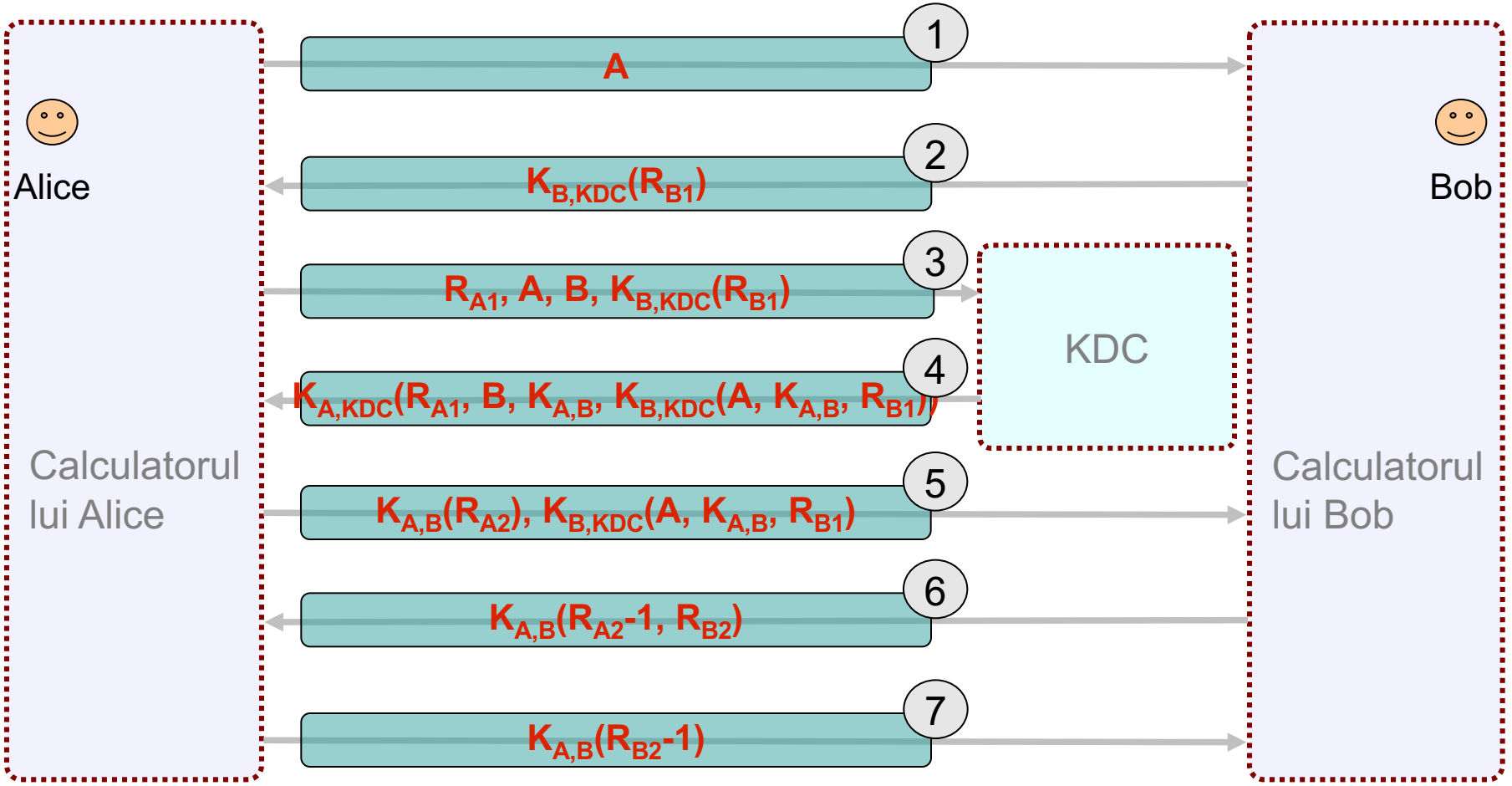
Autentificarea folosind Key Distribution Center

- Protocolul Needham-Schroeder:
  - Vulnerabilitate: dacă Trudy obţine o cheie de sesiune veche Ks, în text clar, ea poate rejuca mesajele începand cu pasul 3.



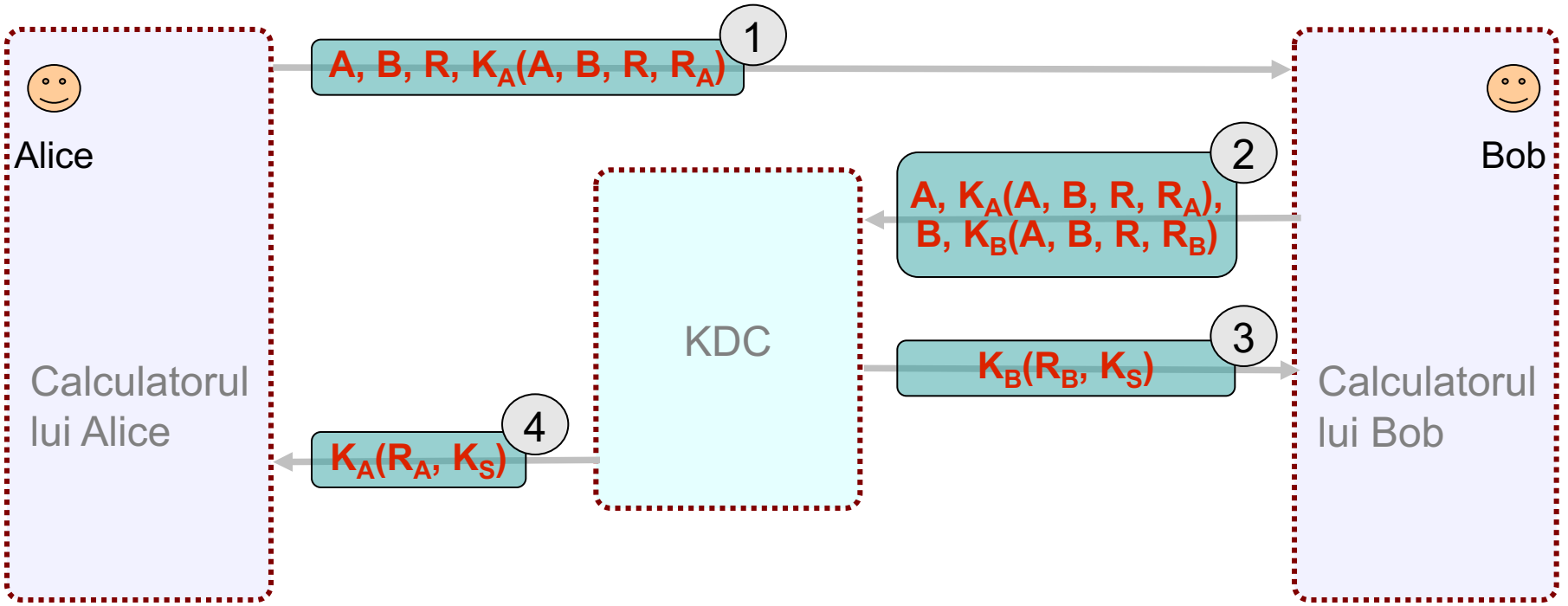
Autentificarea folosind Key Distribution Center

- Protecţia împotriva reutilizării malitioase a unei chei de sesiune generate anterior, în protocolul Needham-Schroeder:



Autentificarea folosind Key Distribution Center

- Protocolul Otway-Rees (simplificat):

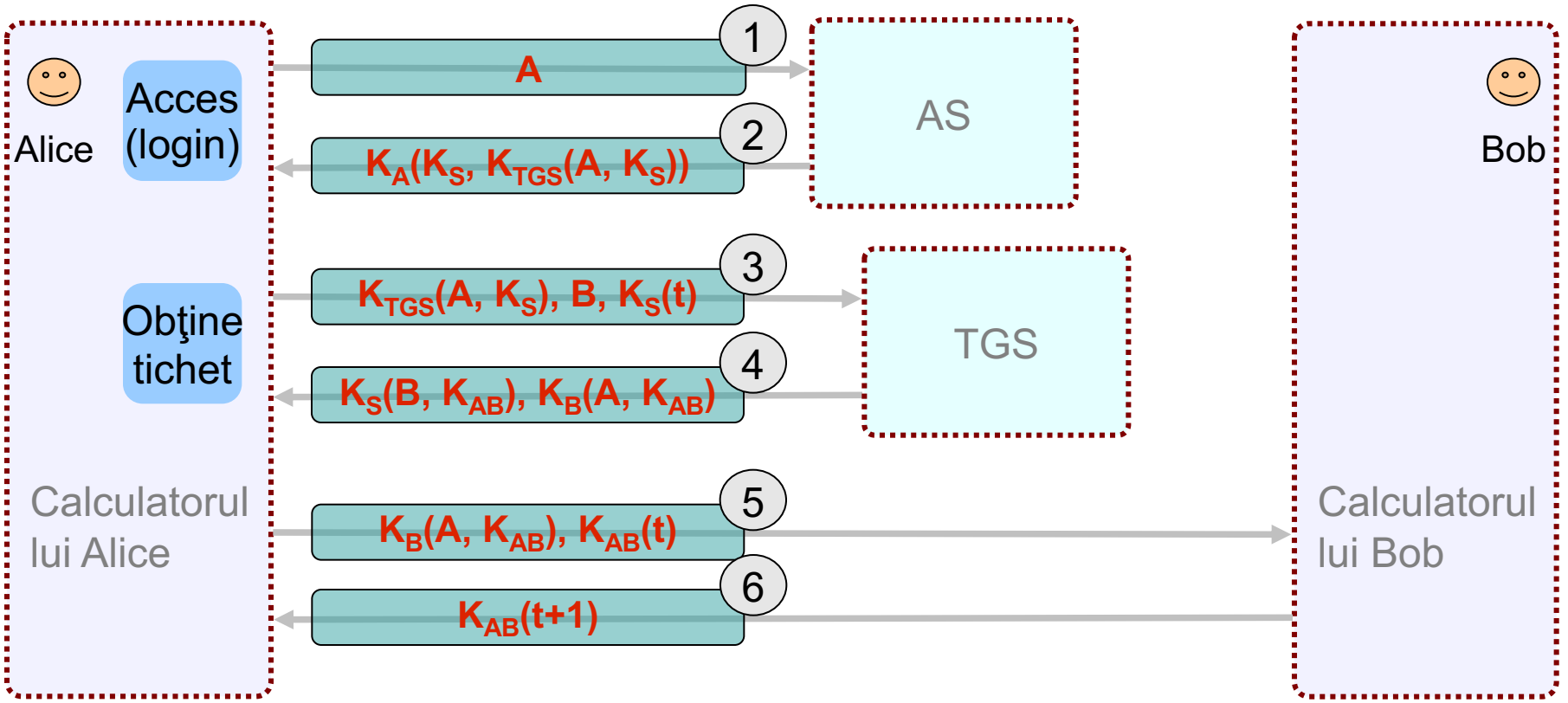


Kerberos

- Protocol autentificare.
- Dezvoltat în proiectul Athena la Massachusetts Institute of Technology.
- Sistem de securitate care oferă:
  - Autentificare;
  - Autorizare;
  - Confidenţialitatea mesajelor.

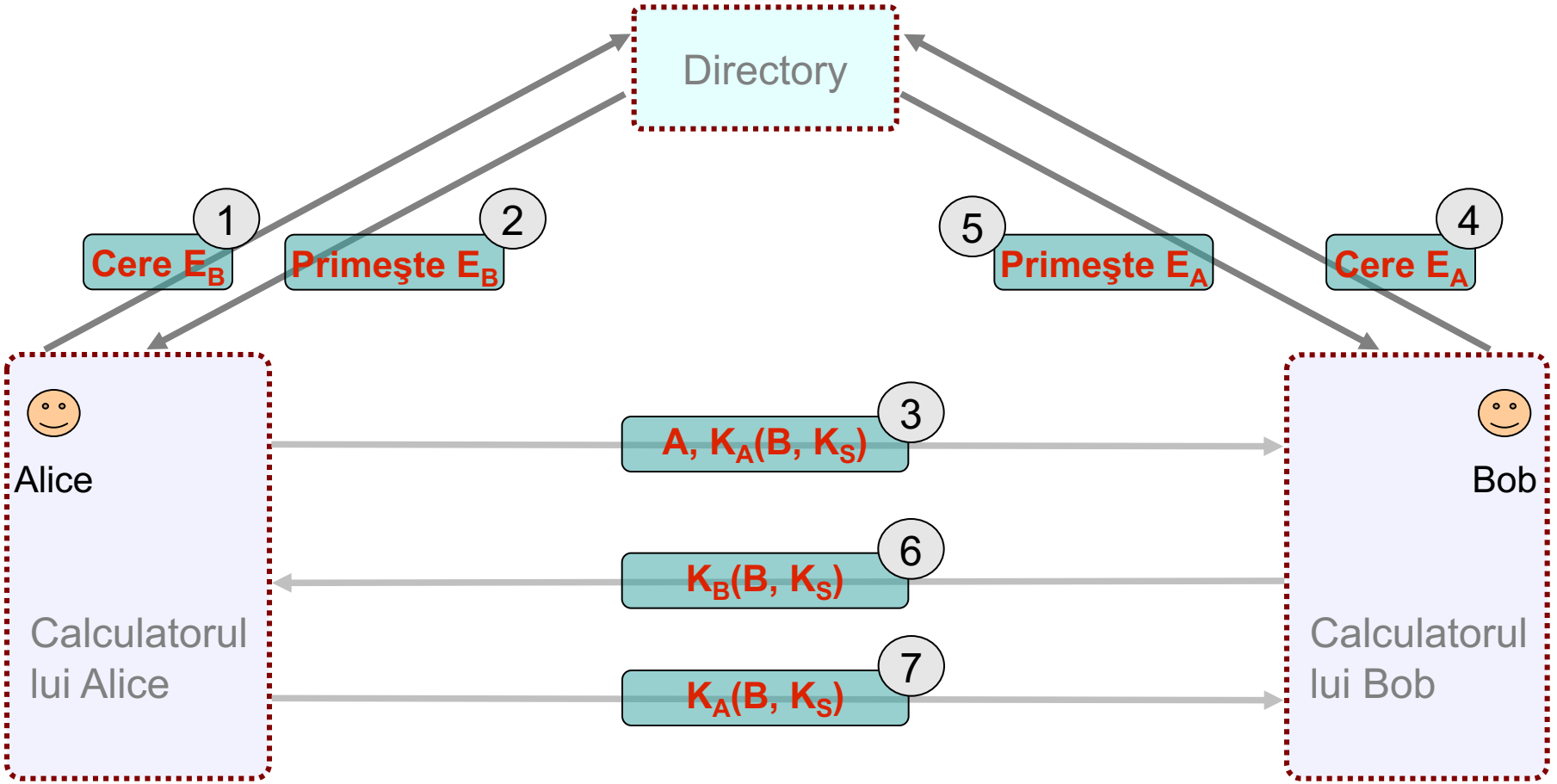
Autentificarea folosind Kerberos

- Operatii Kerberos V4:
  - AS: Authentication Server
  - A: login name (Alice), parola folosită pentru a decripta mesajul 2
  - TGS: Ticket Granting Server



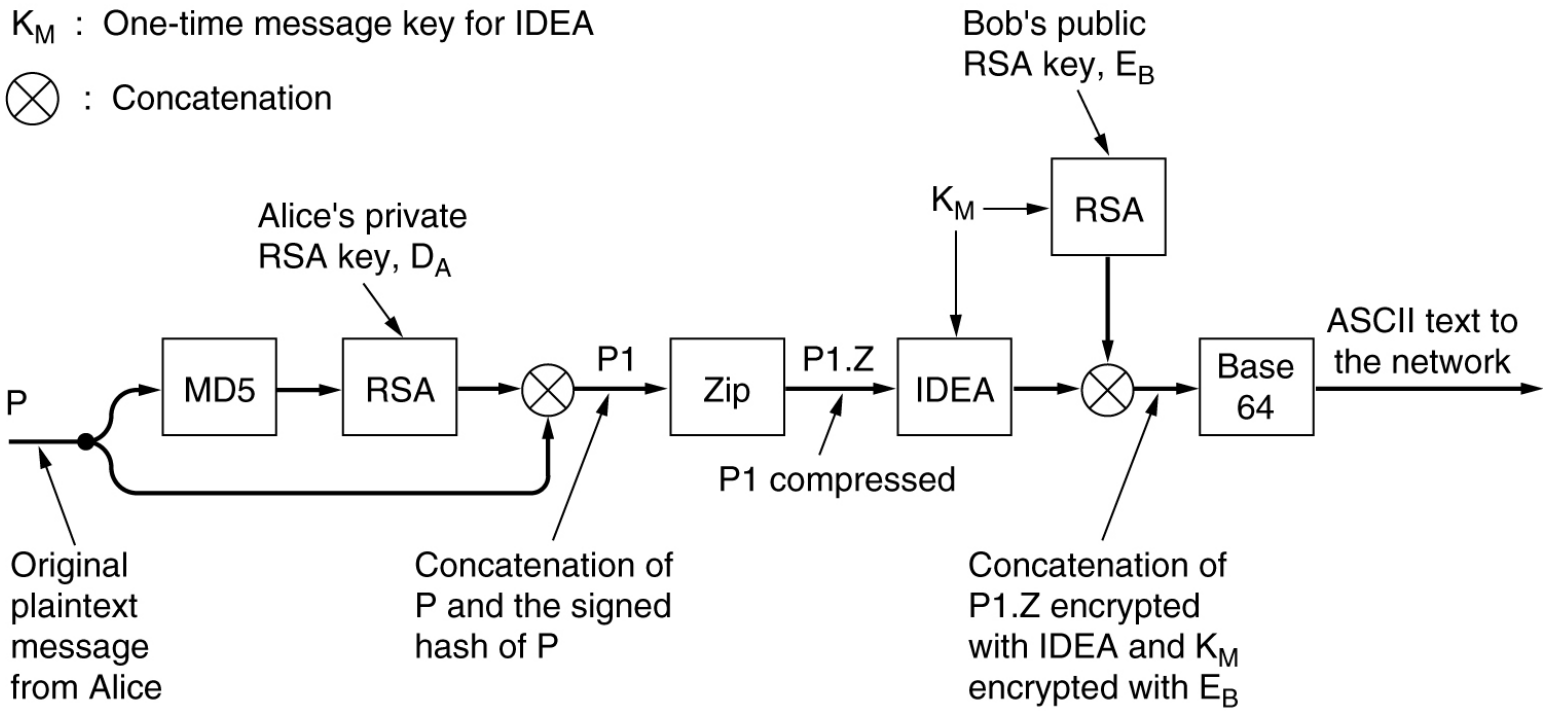
Authentificarea cu Public-Key Cryptography

- Autentificare mutuală folosind public-key cryptography:



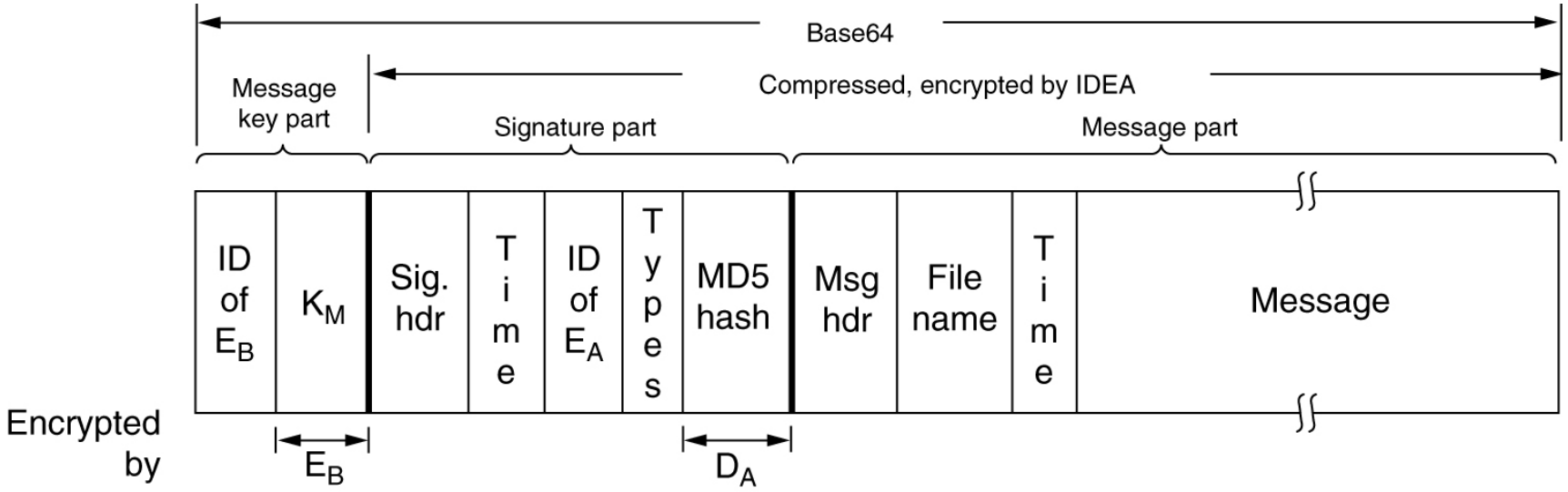
Securitatea E-Mail (PGP: Pretty Good Privacy)

- Autor: Phil Zimmermann.
  - Criptează date folosind IDEA (International Data Encryption Algorithm)
  - K_M cheie de sesiune 128 biţi produsă dintr-un text introdus de Alice
- PGP în operare pentru a trimite un mesaj:



PGP – Pretty Good Privacy

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

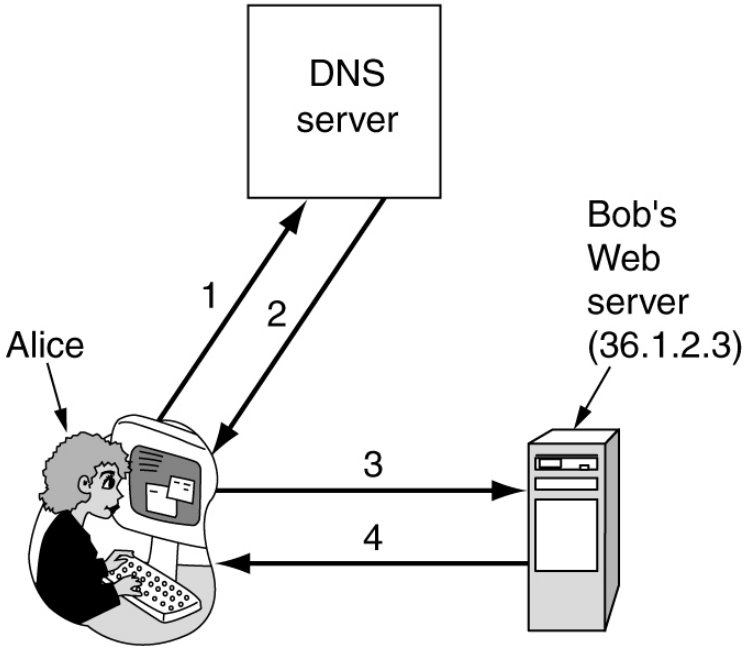


Securitatea Web

- Atacuri:
  - Înlocuire Home page.
  - Denial-of-service.
  - Citire mail-uri.
  - Furt numere credit card.
- Soluţii:
  - Secure Naming.
  - SSL – Secure Sockets Layer.

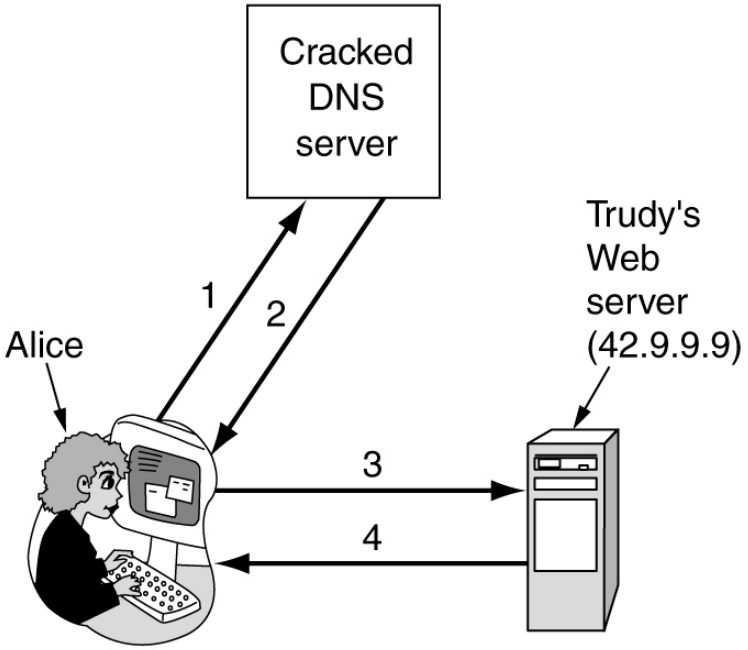
Secure Naming

- (a) Situaţie normală
- (b) Un atac bazat pe modificarea înregistrarii lui Bob în DNS.



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)

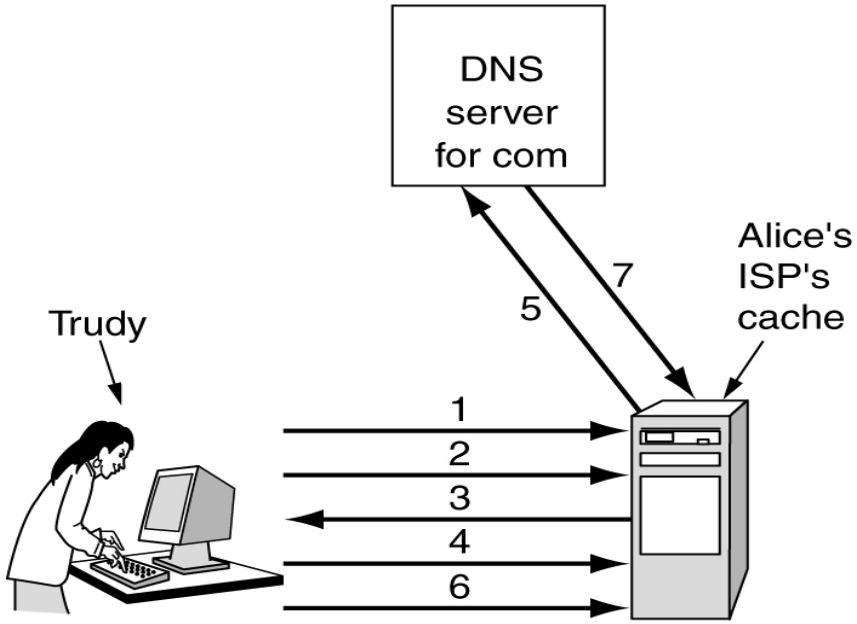


1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page

(b)

Secure Naming (2)

- Trudy păcăleşte ISP-ul lui Alice:
  - DNS foloseste sequence numbers (pentru a mapa cererile şi răspunsurile)
  - Trudy înregistrează un domeniu trudy-the-intruder.com (IP 42.9.9.9)
  - Instaleaza un server dns.trudy-the-intruder.com (aceeaşi IP)
  - Cere adresa foobar.trudy-the-intruder.com pentru a forţa dns.trudy-the-intruder.com în cache ISP-ului lui Alice (pas 1)



1. Look up foobar.trudy-the-intruder.com (to force it into the ISP's cache)
2. Look up www.trudy-the-intruder.com (to get the ISP's next sequence number)
3. Request for www.trudy-the-intruder.com (Carrying the ISP's next sequence number, n)
4. Quick like a bunny, look up bob.com (to force the ISP to query the com server in step 5)
5. Legitimate query for bob.com with seq = n+1
6. Trudy's forged answer: Bob is 42.9.9.9, seq = n+1
7. Real answer (rejected, too late)

Secure DNS

- Fiecare zona DNS are o pereche de chei publică/privată.
- Informaţiile trimise sunt semnate cu cheia privată.
- DNS records sunt grupate în RRSs (Resource Record Sets).
- În DNS se adaugă noi tipuri de înregistrări:
  - KEY: cheia publică a unei zone, utilizator, host, etc.
  - SIG: hash semnat (criptat) pentru înregistrări A şi KEY pentru verificare autenticitate.
- Clienţii primesc un RRS semnat:
  - Aplică cheia publică a zonei pentru a decripta hash-ul.
  - Calculează hash-ul separat.
  - Compară cele două valori (calculată şi decriptată).
- Un exemplu de RRS pentru bob.com.

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...

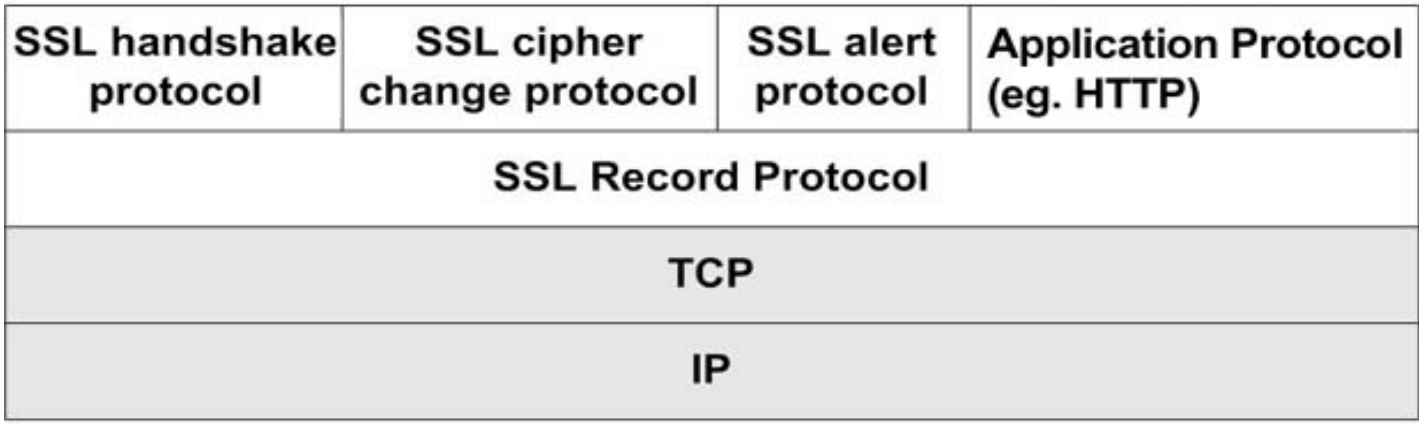
SSL: Secure Sockets Layer

- Niveluri (şi protocoale) pentru un utilizator casnic navigând pe web cu SSL.
- SSLv1 – 1994
- SSLv2 – 1995
- SSLv3.0 – 1996
- TLS 1.0 (SSL 3.1) – 1999 (TLS = **Transport Layer Security**)
- TLS 1.1 (SSL 3.2) - 2001
- TLS 1.2 (SSL 3.3) - 2008

Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

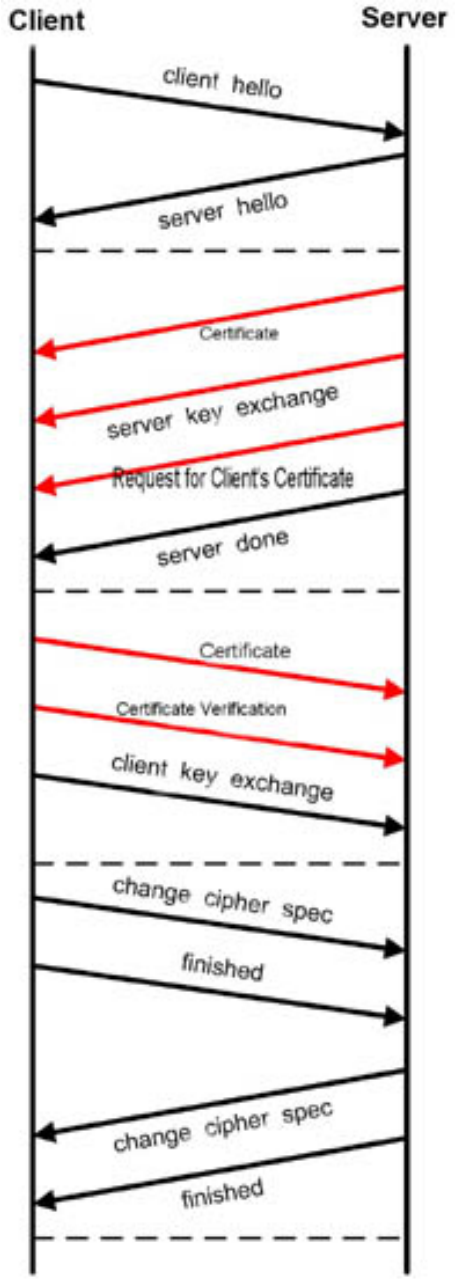
SSL

- 2 nivele:
  - Record
  - Secure Application
- Este folosit peste protocoale care folosesc TCP
  - HTTP, LDAP, POP3, FTP
- 2 roluri
  - Client
  - Server



Handshaking Messages

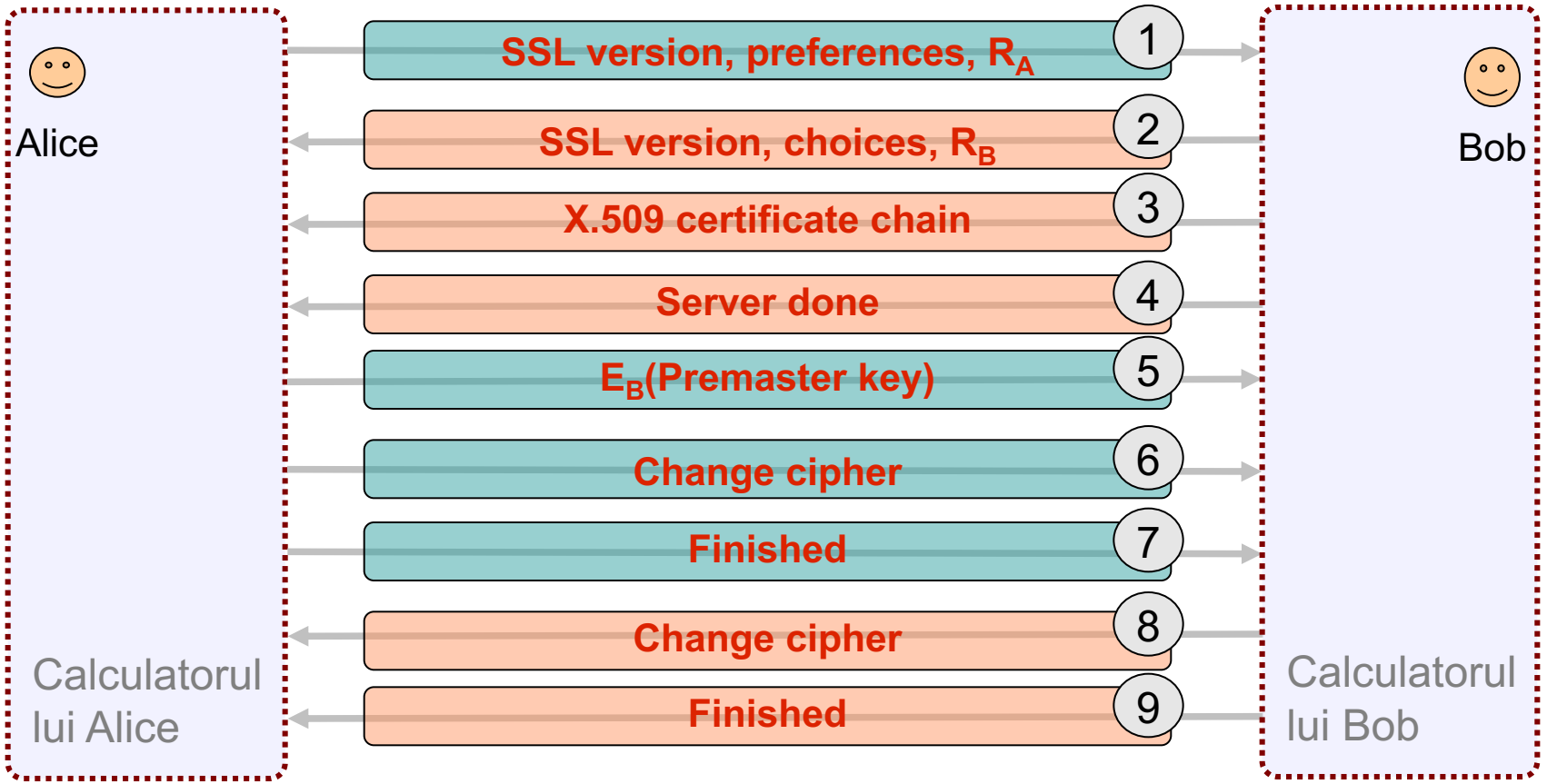
- ClientHello
- ServerHello
- *Certificate
- ServerKeyExchange
- *CertificateRequest
- ServerHelloDone
- *Certificate
- *CertificateVerify
- ClientKeyExchange
- ChangeCipherSpec
- Finished



*=optional

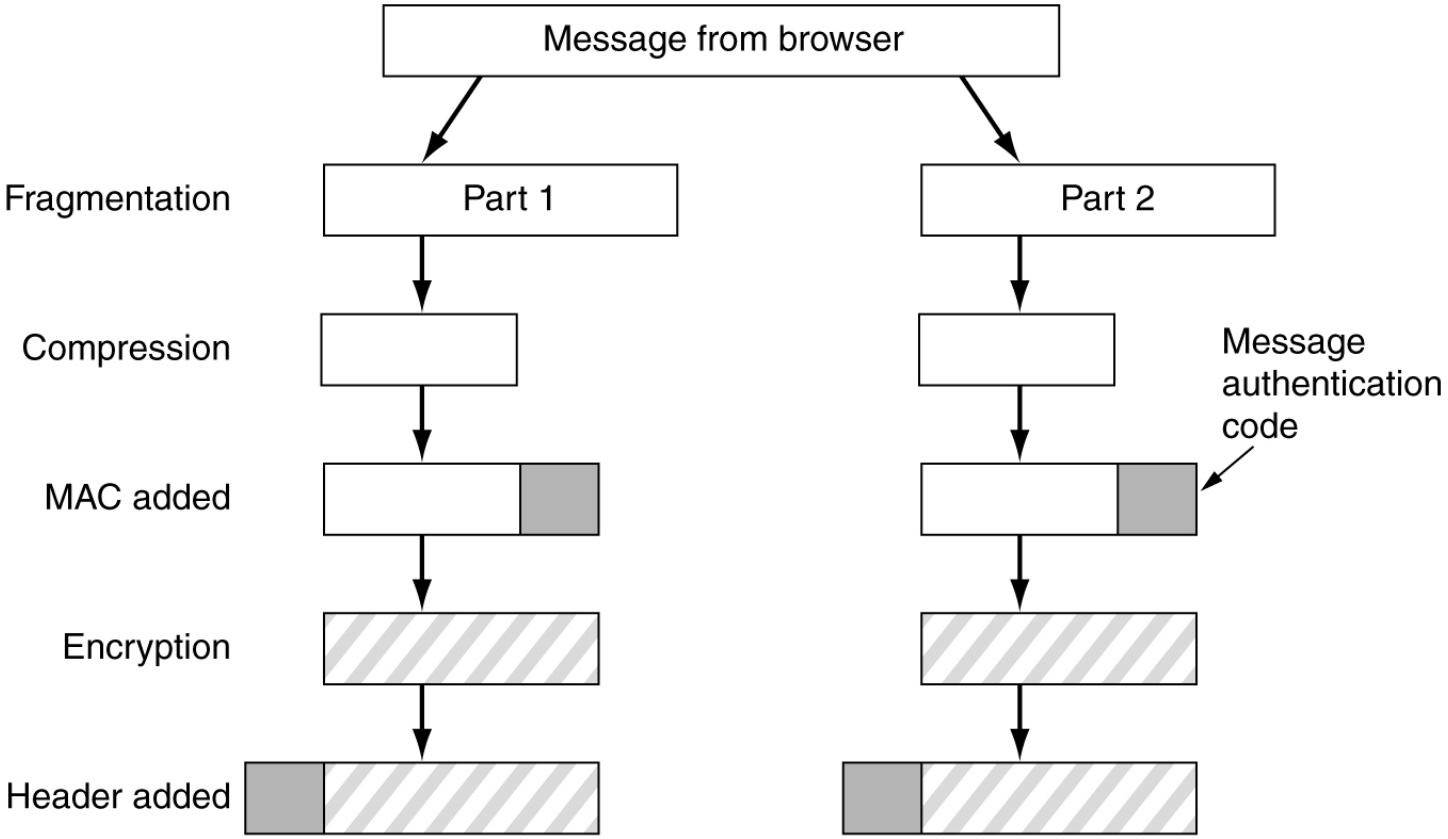
SSL

- Versiune simplificată a subprotocolului de stabilire a unei conexiuni:



SSL

- Transmiterea datelor folosind SSL:



SSL

- **Handshaking Protocol**
  - Stabilirea variabilelor de comunicare
- **ChangeCipherSpec Protocol**
  - Schimbari ce apar in variabilele de comunicare
- **Alert Protocol**
  - Mesaje importante pentru conexiunea SSL
- **Application Encryption Protocol**
  - Criptarea/Decriptarea datelor

- http://www.openssl.org/docs/ssl/ssl.html

Sumar

- Rezumatele mesajelor
  - Funcţii hash: MD5, SHA-1
- Semnături digitale
  - Cu chei secrete (simetrice)
  - Cu chei publice (asimetrice)
  - Verificare semnatură digitală
- Managementul cheilor publice
  - Certificate
  - X.509
  - PKI
- Standarde bazate pe PKI
  - S/MIME
  - SSL/TLS
  - SET
  - IPSec
- Securitatea comunicaţiei
  - IPSec
  - Ziduri de protecţie (Firewalls)
  - Virtual Private Networks
- Protocoale de autentificare
  - Cu cheie secretă partajată
  - Cu HMAC
  - Cu Key Distribution Center
  - Folosind Kerberos
  - Cu Public-Key Cryptography
- Securitatea E-Mail (PGP)
- Securitatea Web
  - Secure Naming
  - SSL – Secure Sockets Layer