Class 6

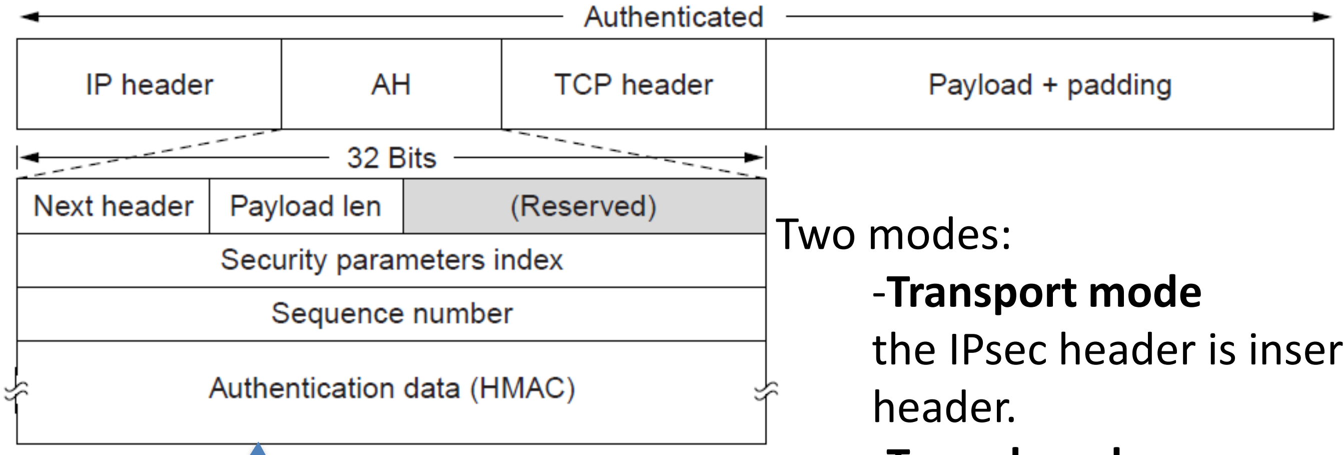
Communication Security

- IPsec
- Firewalls
- Virtual private networks
- Wireless security

From, Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

IPsec (1)

SA (security association). An SA is a simplex connection between two end points and has a security identifier associated with it.



Authenticated

IP header	AH	TCP header	Payload + padding

32 Bits

Next header	Payload len	(Reserved)
Security parameters index		
Sequence number		
Authentication data (HMAC)		

Two modes:

-**Transport mode**

the IPsec header is inserted just after the IP header.

-**Tunnel mode**

The entire IP packet, header and all, is encapsulated in the body of a new IP packet with a completely new IP header.

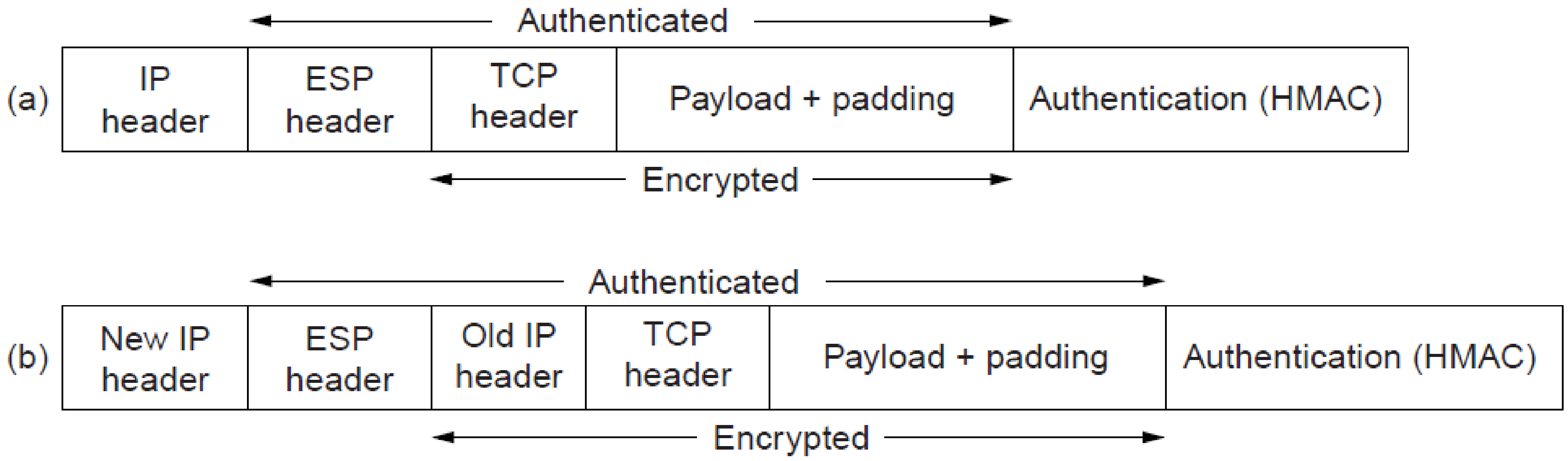
Authentication Header

Hashed Message Authentication Code

The IPsec authentication header in transport mode for IPv4.

IPsec (2)

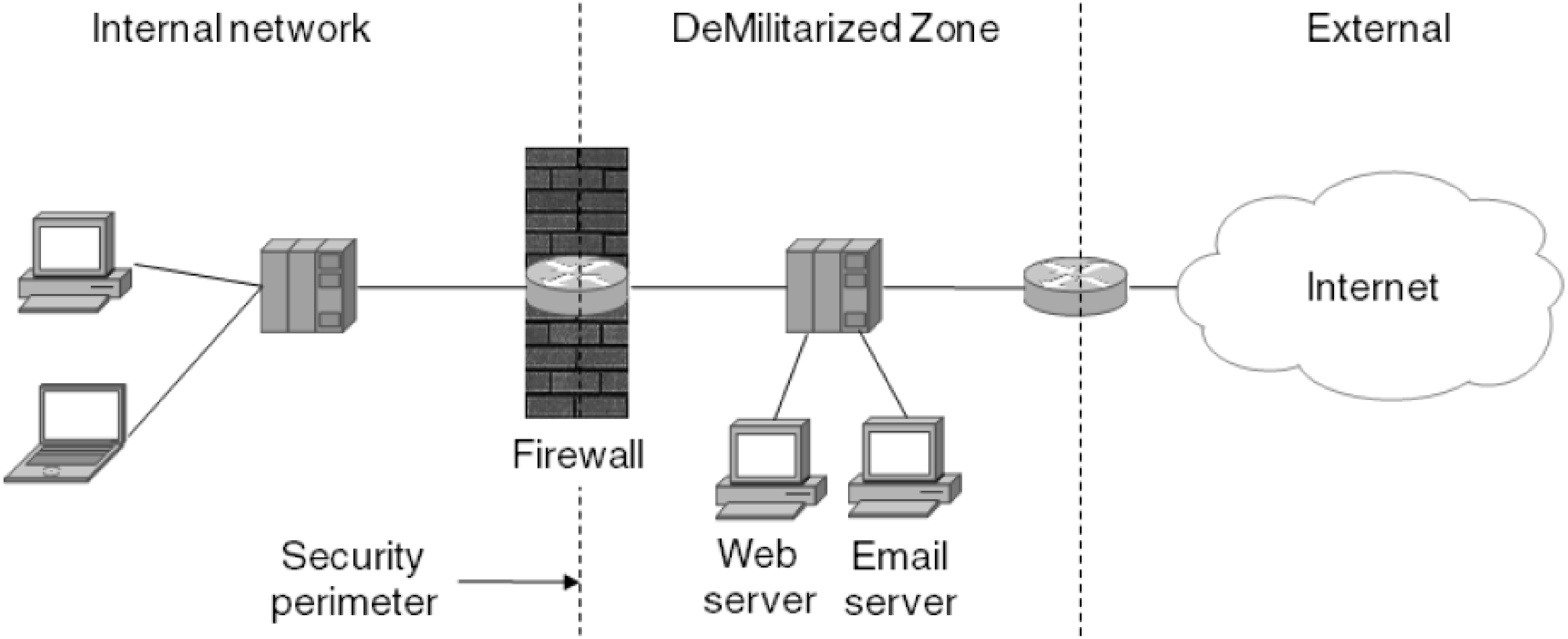
Encapsulating Security Payload



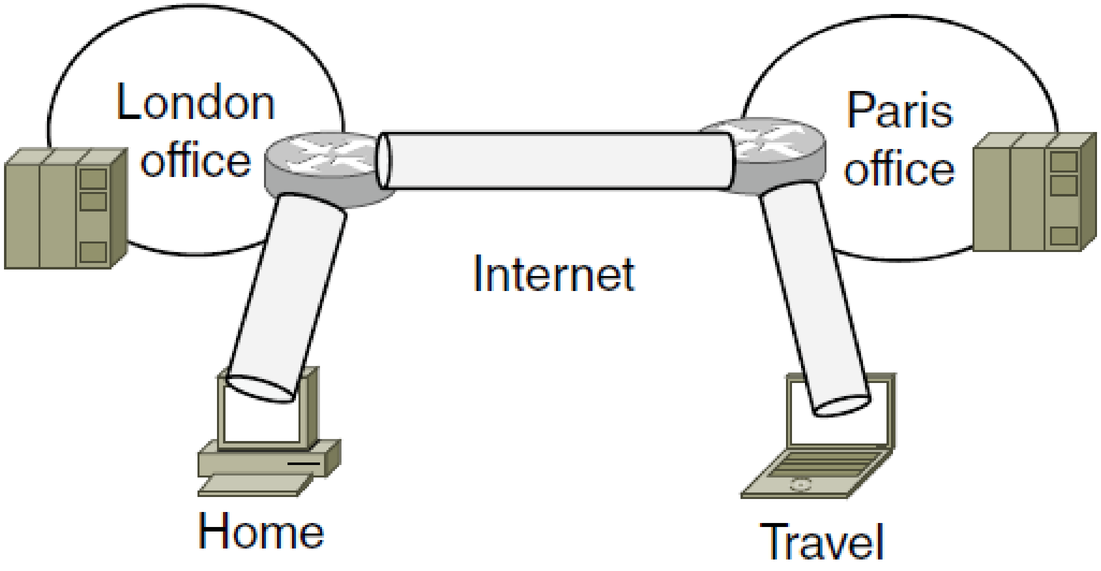
ESP header consists of two 32-bit words

(a) ESP in transport mode. (b) ESP in tunnel mode.

IPsec (3)

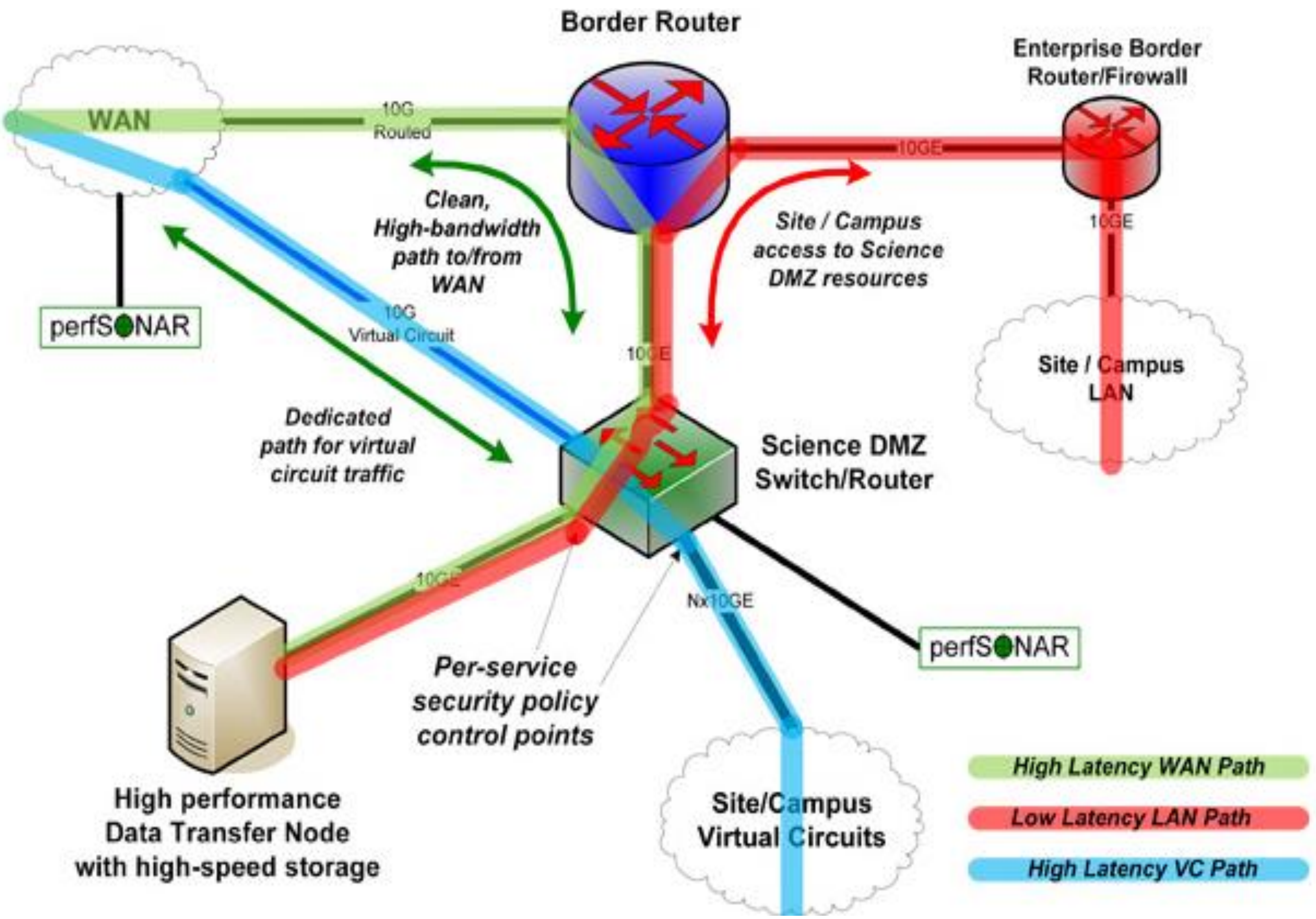

Internal network
DeMilitarized Zone
External
Internet
Firewall
Web server
Email server
Security perimeter

Virtual Private Networks (1)

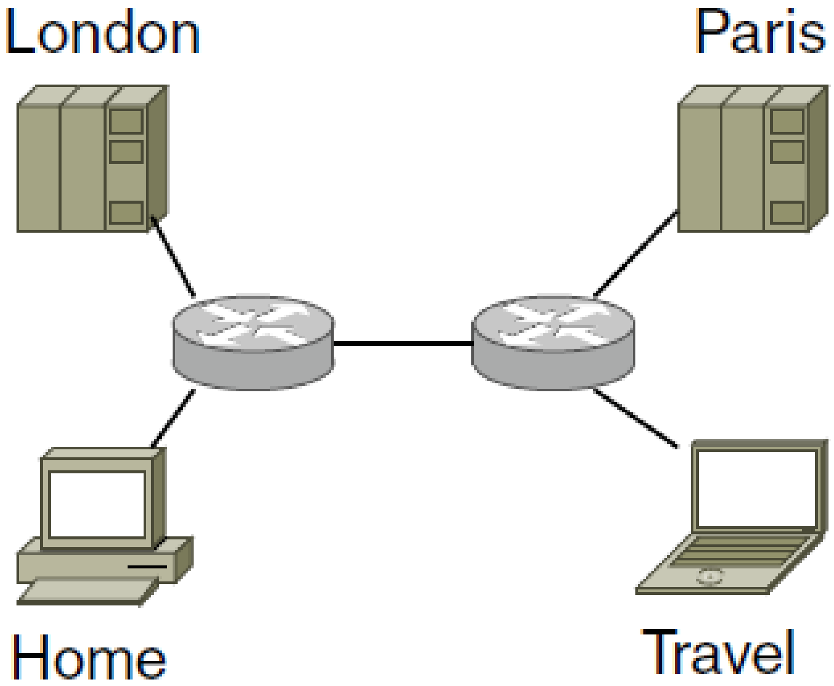


A virtual private network

From ESnet, Energy Science Network

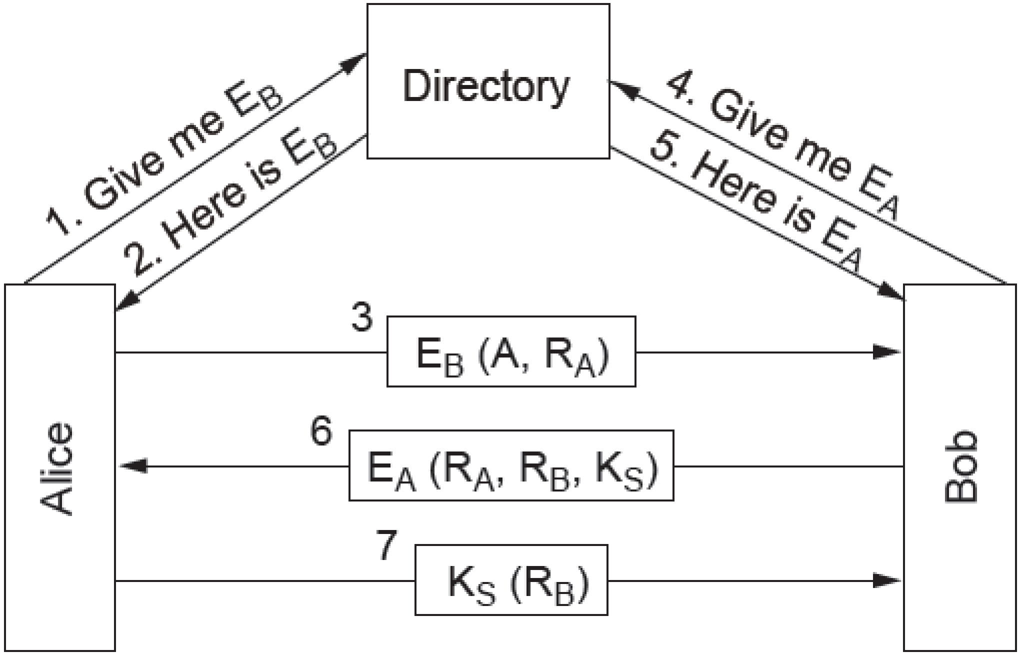

Border Router
Enterprise Border Router/Firewall
WAN
10G Routed
10GE
Clean, High-bandwidth path to/from WAN
Site / Campus access to Science DMZ resources
10GE
perfSONAR
10G Virtual Circuit
10GE
Site / Campus LAN
Dedicated path for virtual circuit traffic
Science DMZ Switch/Router
10GE
Nx10GE
perfSONAR
Per-service security policy control points
High performance Data Transfer Node with high-speed storage
Site/Campus Virtual Circuits
High Latency WAN Path
Low Latency LAN Path
High Latency VC Path

Virtual Private Networks (2)



Topology as seen from the inside

Public-Key Cryptography

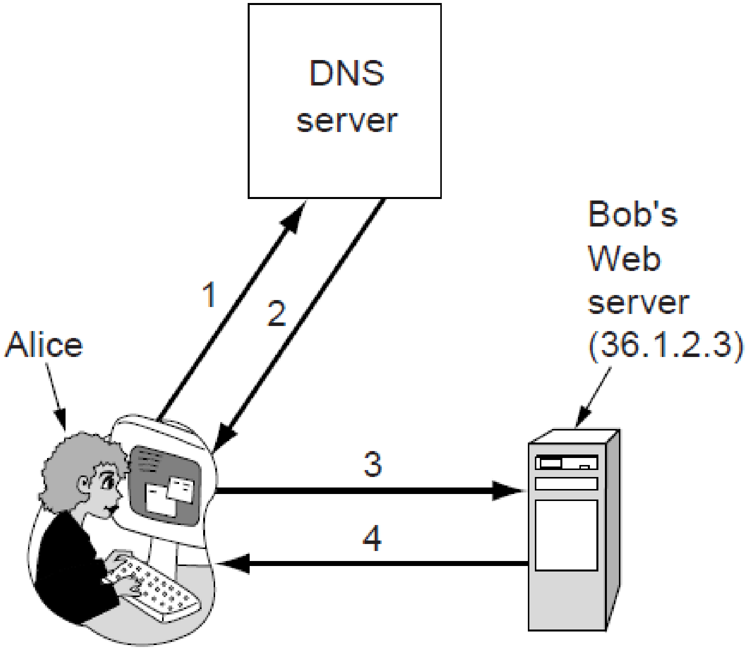


Mutual authentication using public-key cryptography

Web Security

- Threats
- Secure naming
- SSL—the Secure Sockets Layer
- Mobile code security

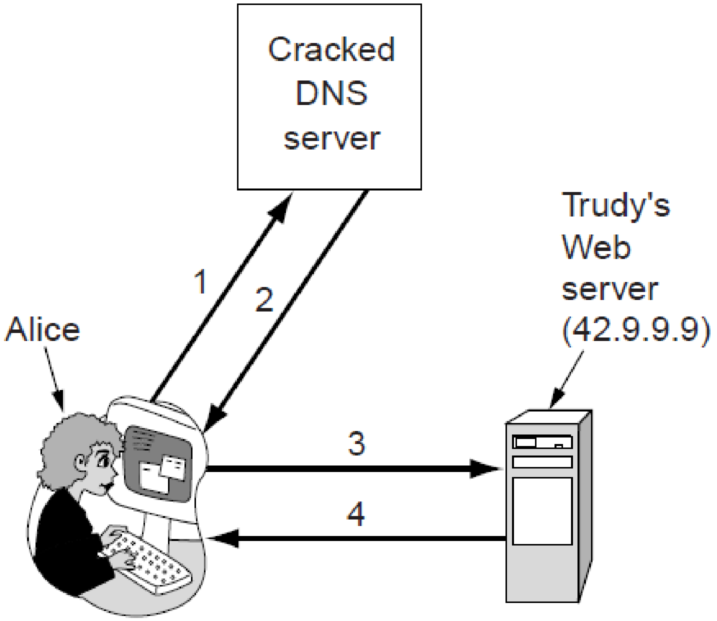
Secure Naming (1)



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

Normal situation

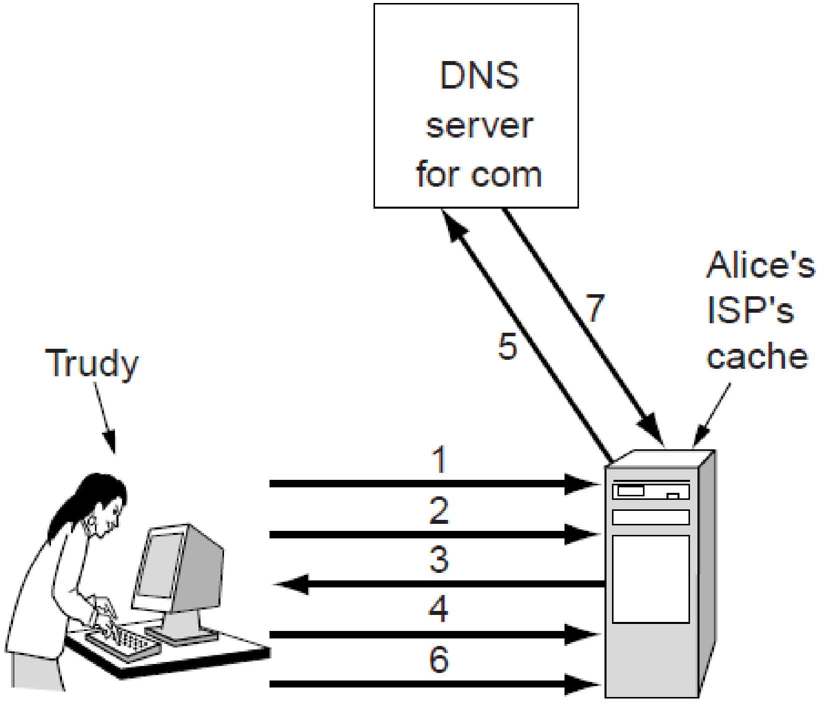
Secure Naming (2)



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

An attack based on breaking into DNS and modifying Bob’ s record.

Secure Naming (3)



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)

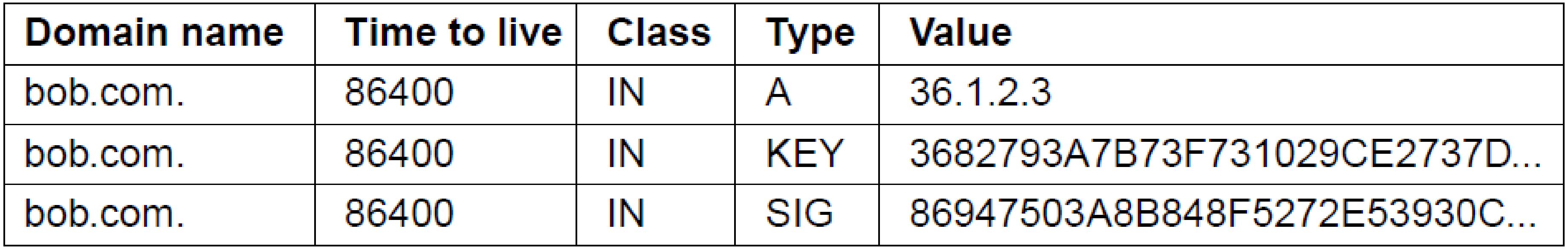
How Trudy spoofs Alice’s ISP.

Secure Naming (4)

DNSsec fundamental services:

- Proof of where the data originated.
- Public key distribution.
- Transaction and request authentication.

Secure Naming (5)



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...

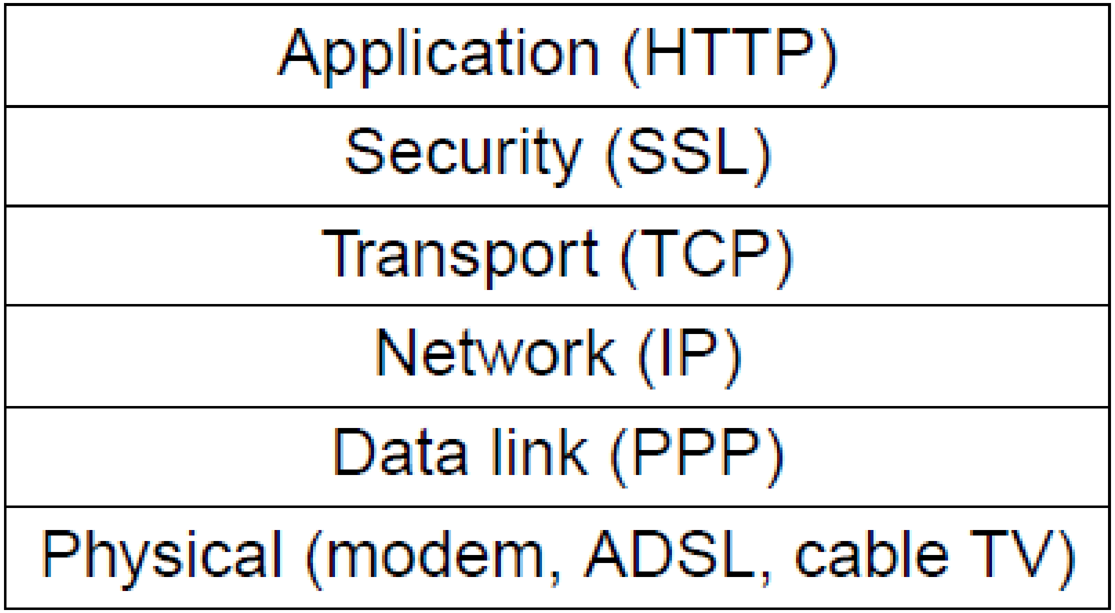
An example RRSet for *bob.com.* The KEY record is Bob’ s public key. The *SIG* record is the top-level *com* server’ s signed hash of the *A* and *KEY* records to verify their authenticity.

SSL—The Secure Sockets Layer (1)

Secure connection includes …

- Parameter negotiation between client and server.
- Authentication of the server by client.
- Secret communication.
- Data integrity protection.

SSL—The Secure Sockets Layer (2)



Application (HTTP)

Security (SSL)

Transport (TCP)

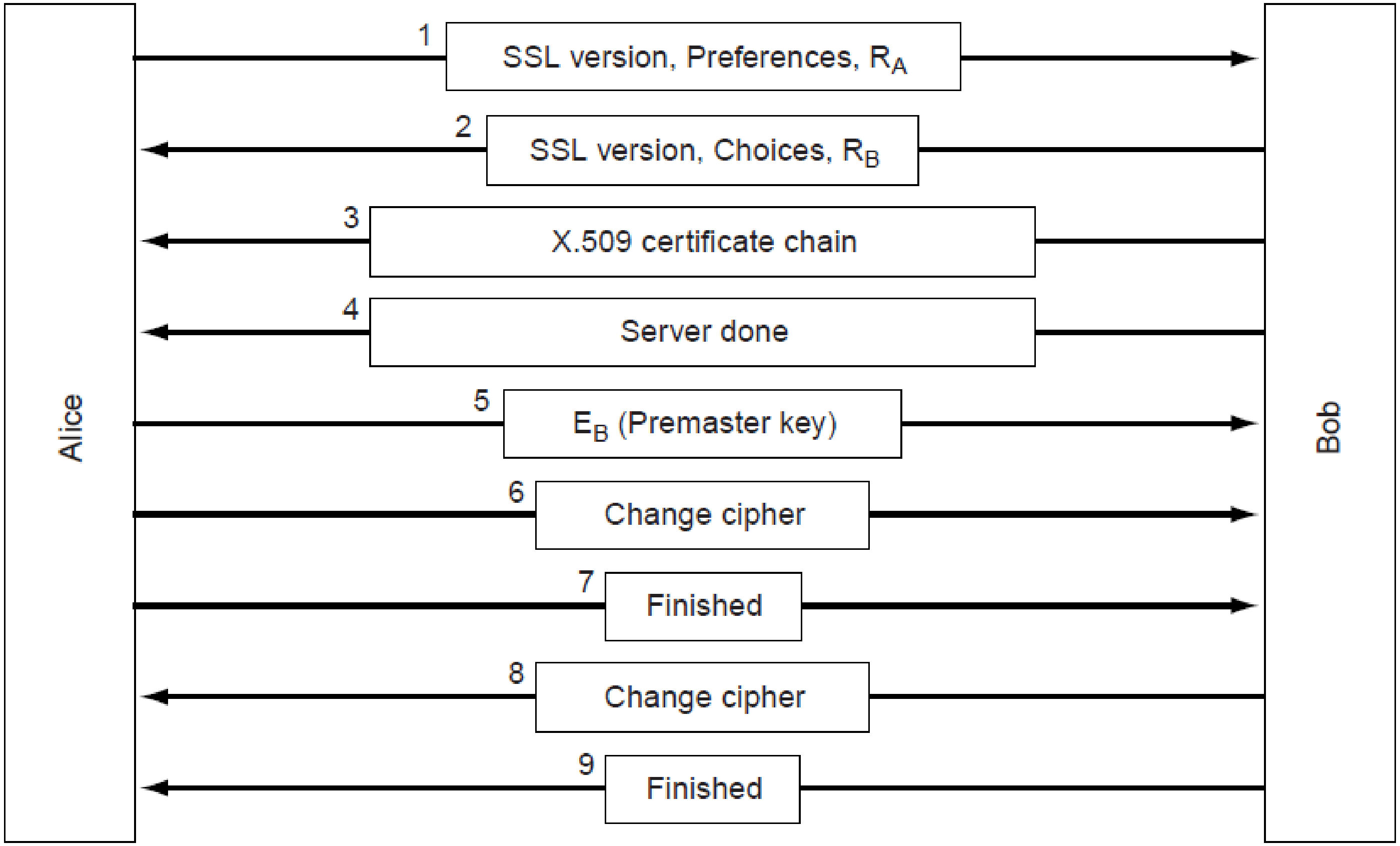
Network (IP)

Data link (PPP)

Physical (modem, ADSL, cable TV)

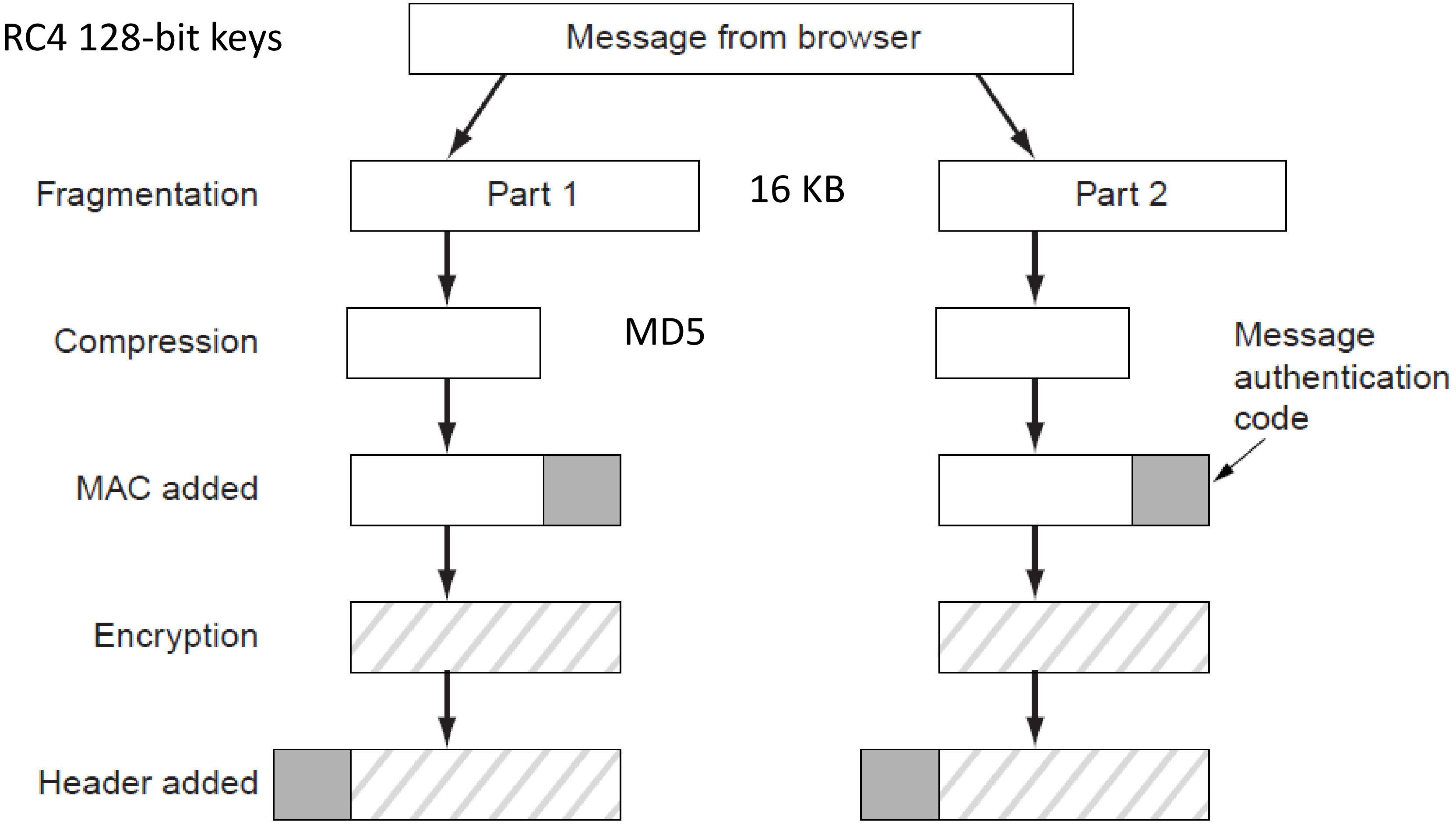
Layers (and protocols) for a home
user browsing with SSL.

SSL—The Secure Sockets Layer (3)



A simplified version of the SSL connection establishment subprotocol.

SSL—The Secure Sockets Layer (4)



RC4 128-bit keys

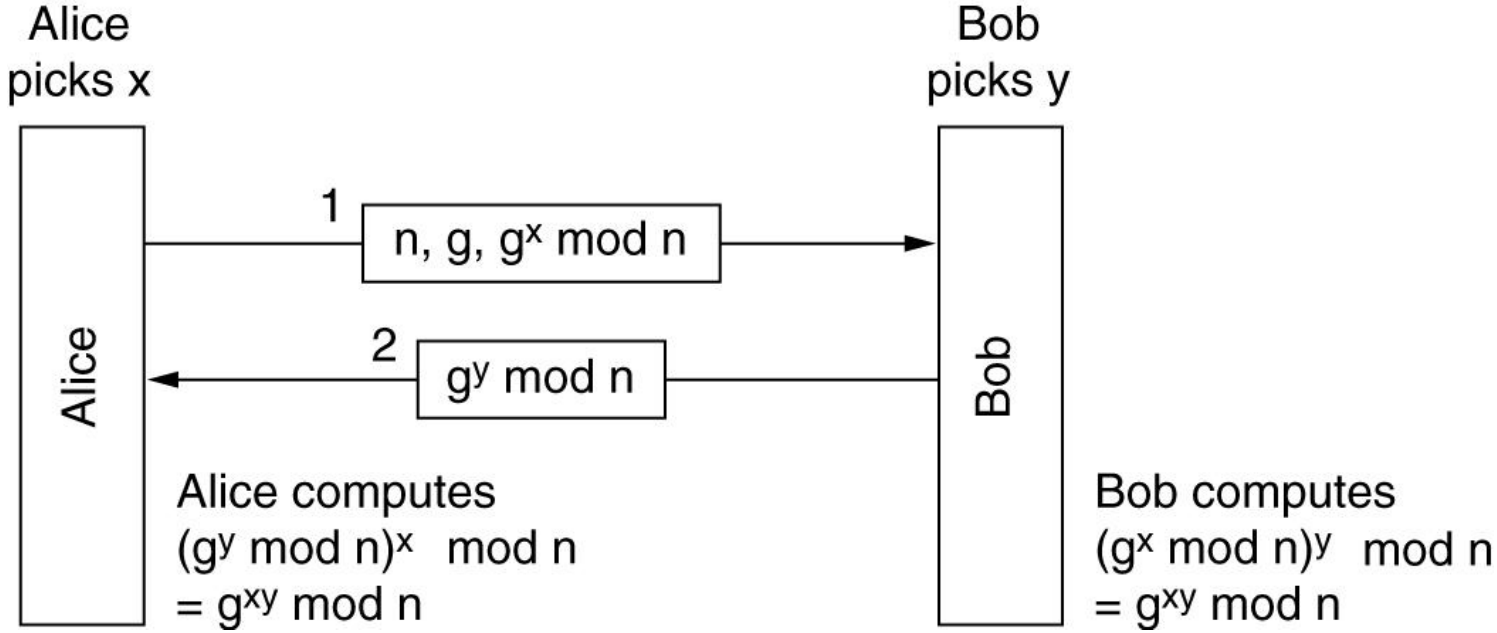
16 KB

MD5

Data transmission using SSL

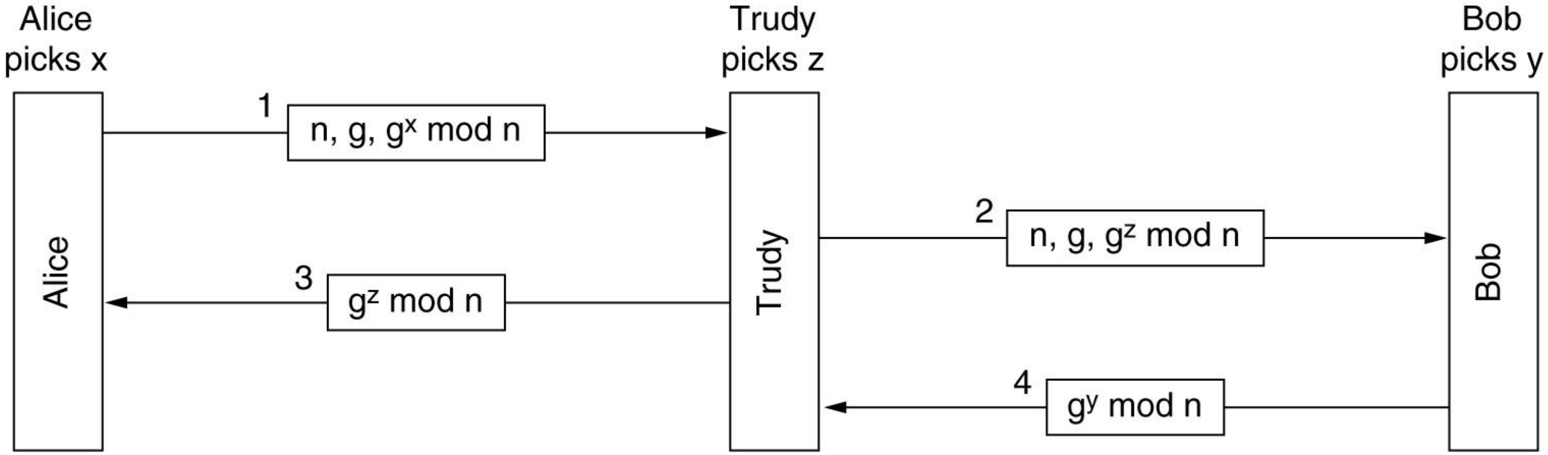
Establishing a Shared Key:
The Diffie-Hellman Key Exchange

- The Diffie-Hellman key exchange.



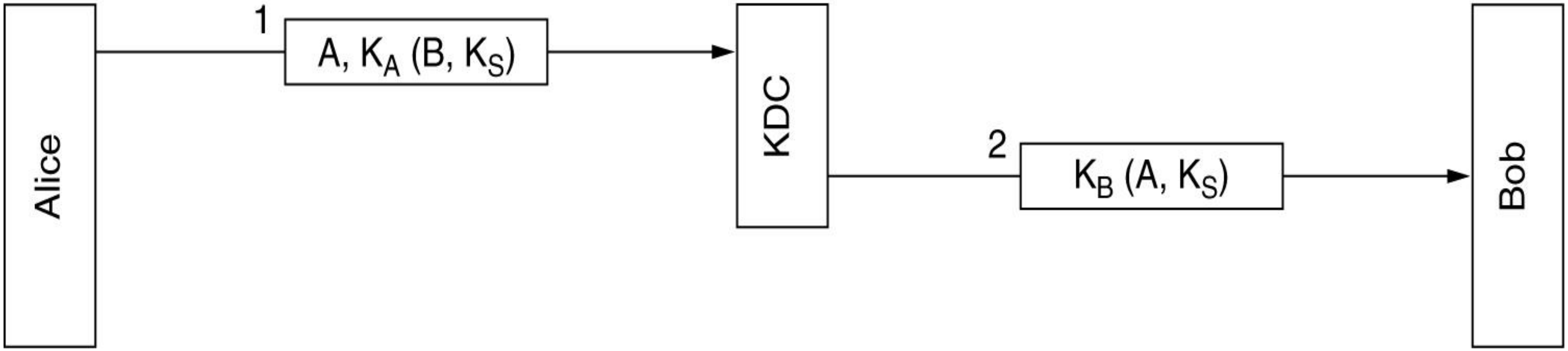
Establishing a Shared Key: The Diffie-Hellman Key Exchange

- The bucket brigade or man-in-the-middle attack.



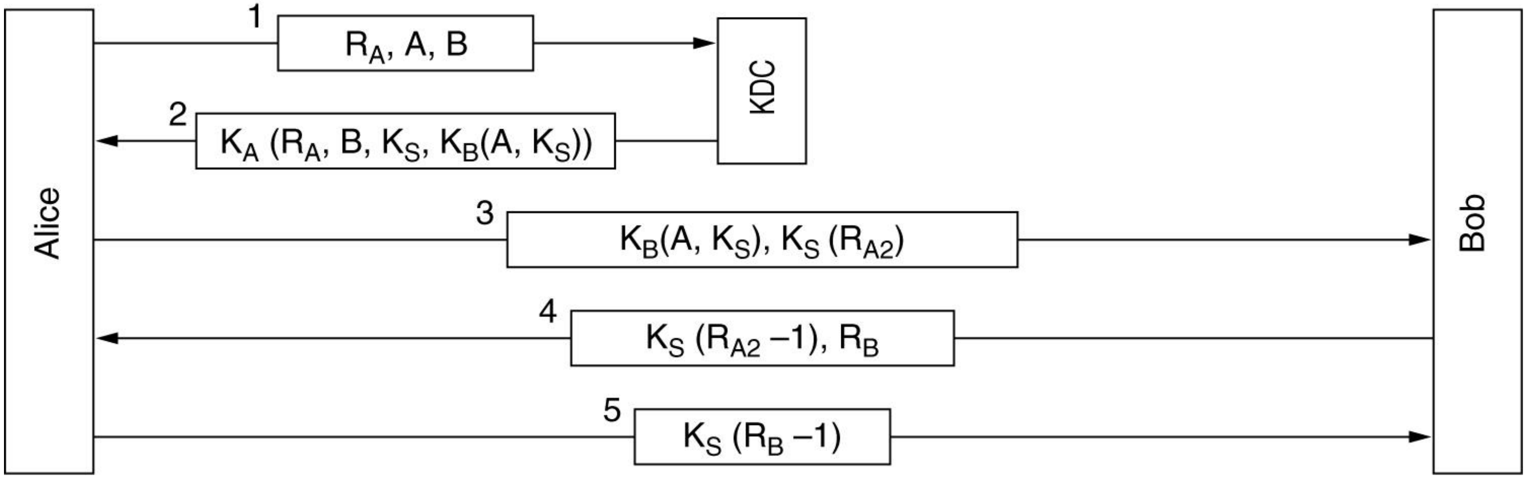
Authentication Using a Key Distribution Center

- A first attempt at an authentication protocol using a KDC.



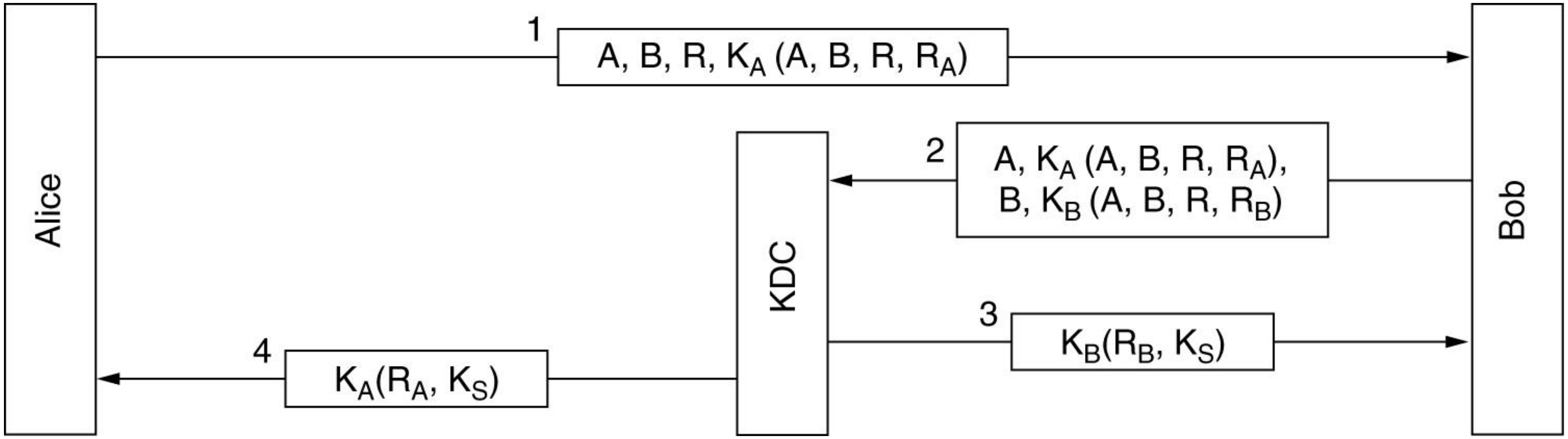
Authentication Using a Key Distribution Center (2)

- The Needham-Schroeder authentication protocol.


Alice
KDC
Bob
1
R_A, A, B
2
K_A (R_A, B, K_S, K_B(A, K_S))
3
K_B(A, K_S), K_S (R_{A2})
4
K_S (R_{A2} –1), R_B
5
K_S (R_B –1)

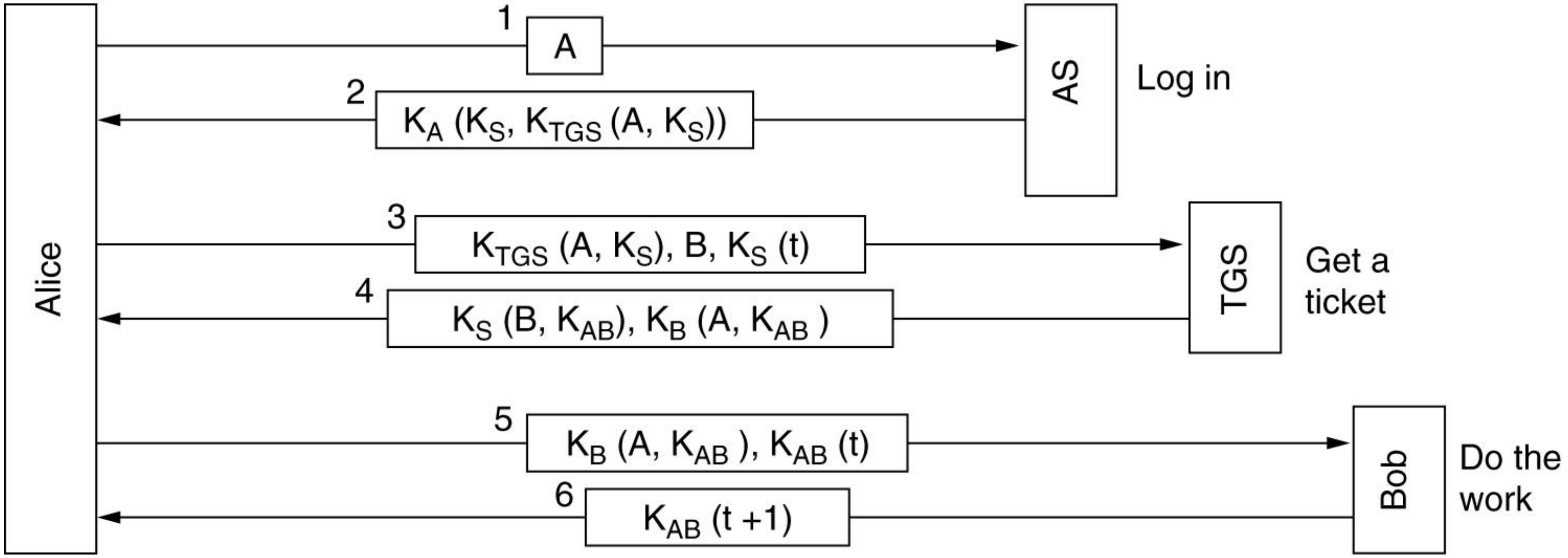
Authentication Using a Key Distribution Center (3)

- The Otway-Rees authentication protocol (slightly simplified).



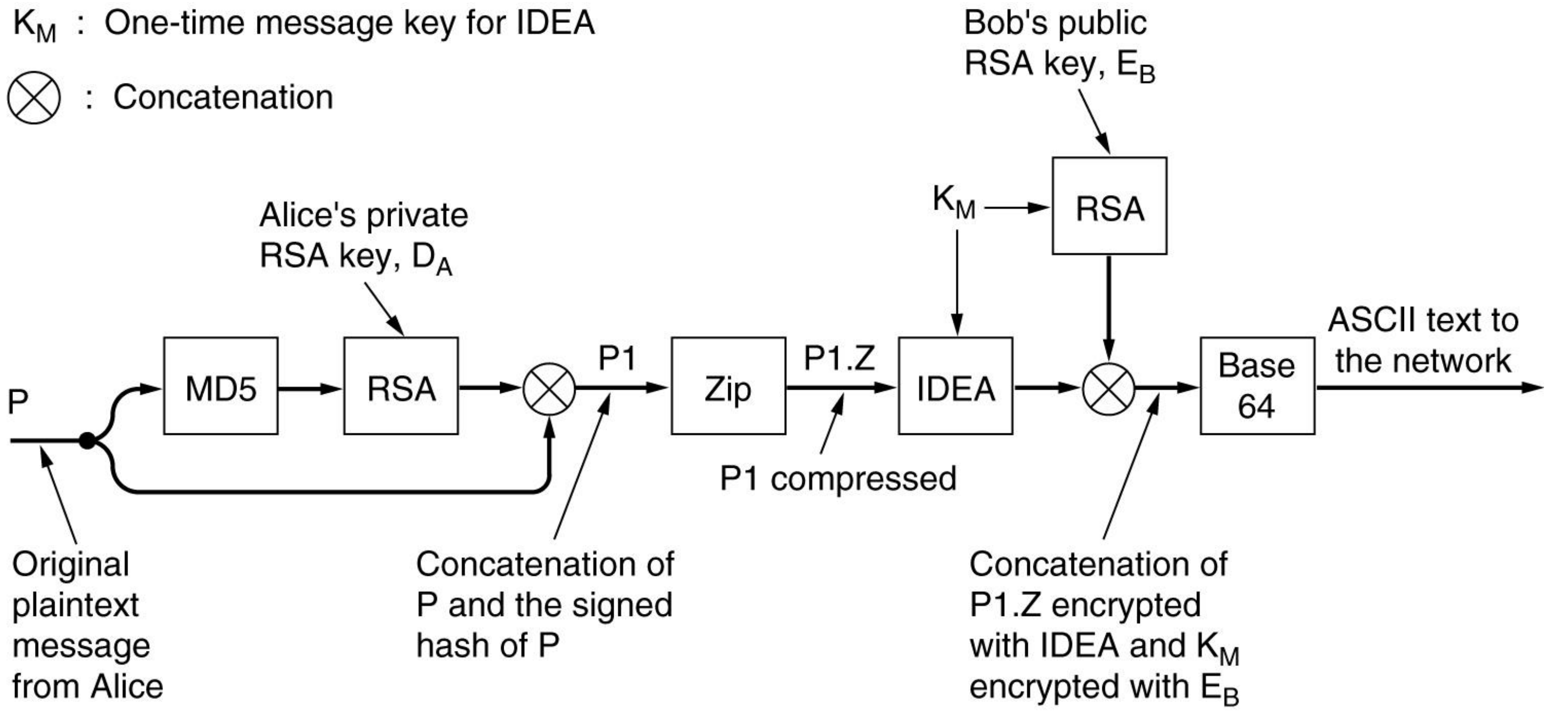
Authentication Using Kerberos

- The operation of Kerberos V4.


Alice
1
A
AS
Log in
2
$K_A (K_S, K_{TGS} (A, K_S))$
3
$K_{TGS} (A, K_S), B, K_S (t)$
TGS
Get a ticket
4
$K_S (B, K_{AB}), K_B (A, K_{AB})$
5
$K_B (A, K_{AB}), K_{AB} (t)$
Bob
Do the work
6
$K_{AB} (t +1)$

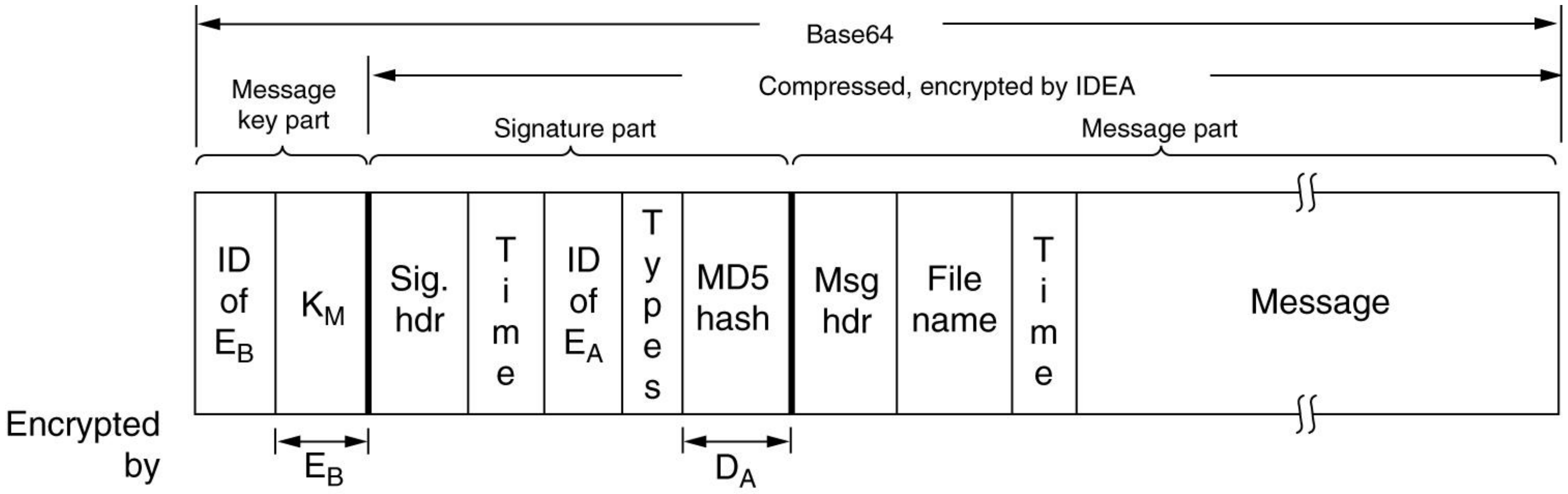
PGP – Pretty Good Privacy

- PGP in operation for sending a message.


K_M : One-time message key for IDEA
⊗ : Concatenation
Bob's public RSA key, E_B
K_M
RSA
Alice's private RSA key, D_A
ASCII text to the network
P
MD5
RSA
P1
Zip
P1.Z
IDEA
Base 64
P1 compressed
Original plaintext message from Alice
Concatenation of P and the signed hash of P
Concatenation of P1.Z encrypted with IDEA and K_M encrypted with E_B

PGP – Pretty Good Privacy (2)

- A PGP message.


Base64
Compressed, encrypted by IDEA
Message key part
Signature part
Message part
ID of E_B
K_M
Sig. hdr
Time
ID of E_A
Types
MD5 hash
Msg hdr
File name
Time
Message
Encrypted by
E_B
D_A