計算機ネットワーク

開講クォーター: 1-2Q

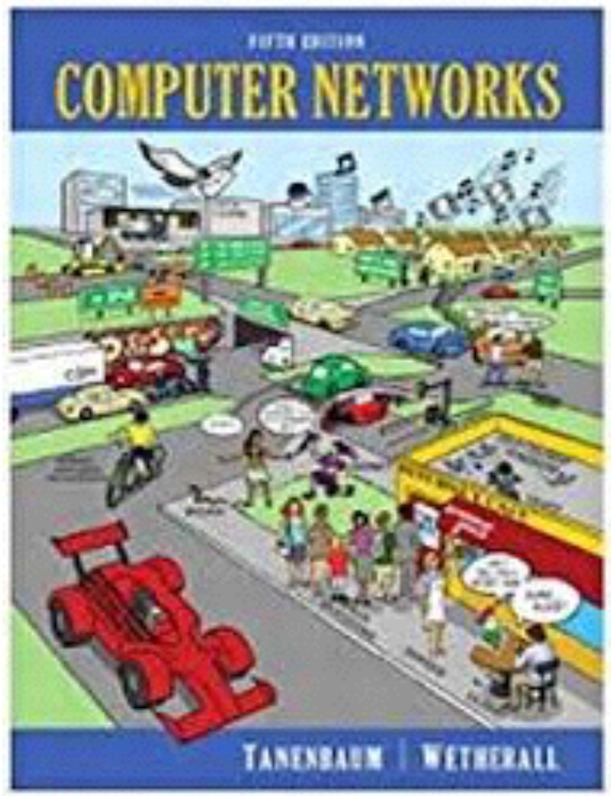
曜日・時限: 火7-8限

講義室: 1Q @ W834, 2Q @ W931

横田理央

rioyokota@gsic.titech.ac.jp

参考書



教科書

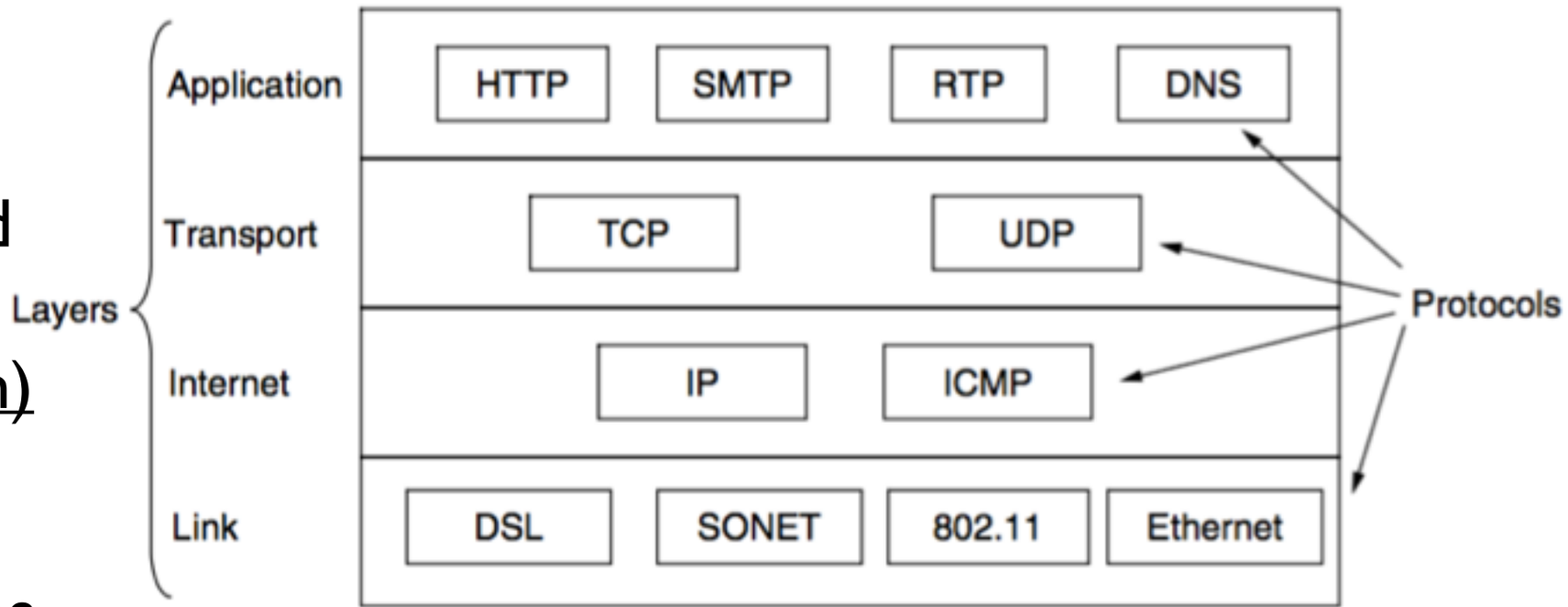
講義日程（2Q）

		授業計画		課題
06/14	第９回	ネットワーク層１ ルーティング・輻輳制御	５章	ルーティングの種類を理解し 輻輳制御手法を説明できる
06/21	第１０回	ネットワーク層２ インターネットとサービス品質	５章	インターネットの制御プロトコルを理解し ネットワーク間の接続について説明できる
06/28	第１１回	トランスポート層１ トランスポート・プロトコルの要素	６章	誤り制御とフロー制御を理解し 輻輳制御について説明できる
07/05	第１２回	トランスポート層２ UDP と TCP	６章	TCP の信頼性を理解し TCP のコネクション管理を説明できる
07/12	第１３回	アプリケーション層 DNS, 電子メール, www	７章	DNS, 電子メール, www のしくみを理解し ストリーミング，P2P について説明できる
07/26	第１４回	ネットワークセキュリティ１ 対称鍵暗号，公開鍵暗号	８章	暗号アルゴリズムを理解し SHA-1,2 と RSA について説明できる
08/02	第１５回	ネットワークセキュリティ２ デジタル署名，認証プロトコル	８章	電子メール,Web のセキュリティ の脅威について把握できる

Communication Security

<u>IPSec (IP Security)</u>
In the network layer,
but connection oriented

<u>SA (Security Association)</u>
A simplex connection
between two endpoints
and has a security identifier
associated with it



Multiple services: Not everyone wants to have all the services all the time

Multiple algorithms: An algorithm that is now thought to be secure may be broken in the future

Multiple granularity: To make it possible to protect a single TCP connection, all traffic between a pair of hosts, or all traffic between a pair of routers

IPSec

IPSec has two parts

1. The first part describes two new headers that can be added to packets to carry the security identifier, integrity control data, and other information.
2. The other part, ISAKMP (Internet Security Association and Key Management Protocol), deals with establishing keys.

IPSec has two modes

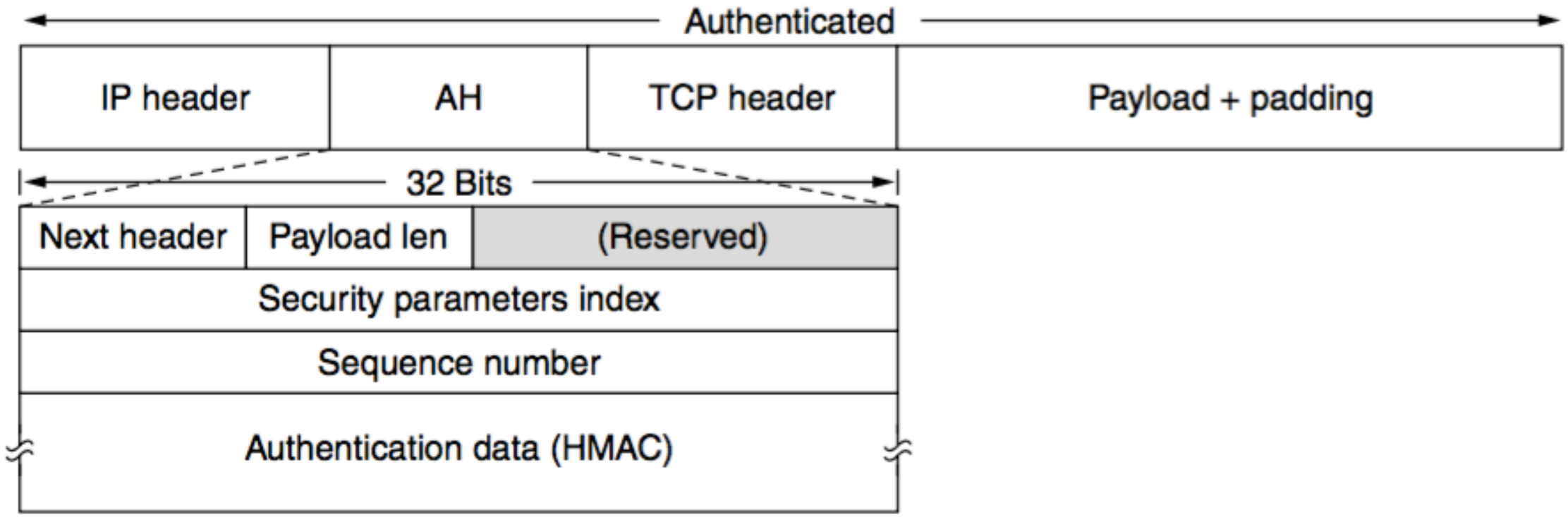
1. Transport mode: The IPsec header is inserted just after the IP header
2. Tunnel mode: The entire IP packet, header and all, is encapsulated in the body of a new IP packet with a completely new IP header

Benefits of Tunnel mode

1. Aggregate connections to prevent traffic analysis
2. VPN (Virtual Private Network)

IPSec

AH (Authentication Header)



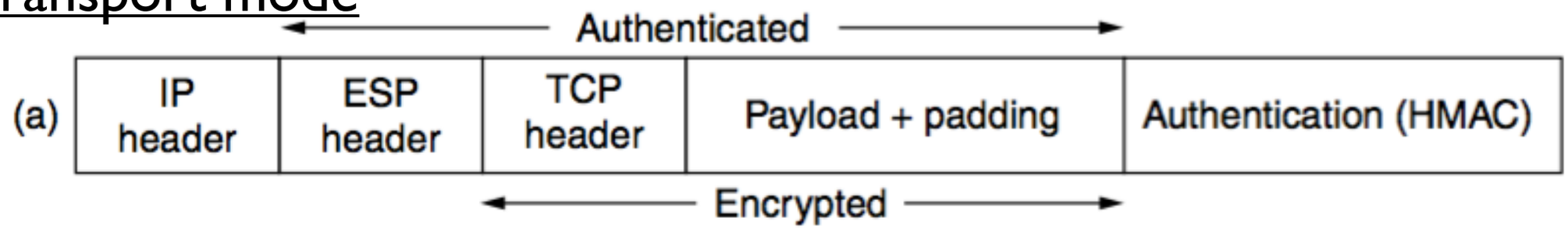
Next header: Used to store the value that the IP Protocol field had before it was replaced
Payload length: The number of 32-bit words in the AH header minus 2
Security parameters index: Contains the shared key used on this connection
Sequence number: Every packet gets a unique number, even retransmissions
(detect replay attacks)
Authentication data: Contains the payload's digital signature

Public keys are too slow, so HMAC (Hashed Message Authentication Code) is used
HMAC compute the hash over the packet plus the shared key, and is much faster than first running SHA-1 and then running RSA on the result.

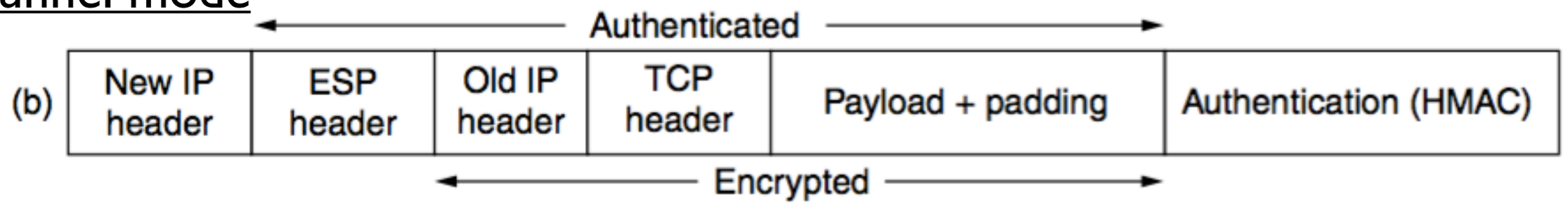
IPSec

ESP (Encapsulating Security Payload)

Transport mode



Tunnel mode



ESP header: Consists of Security parameters index, Sequence number, Initialization vector.
HMAC comes after the payload:
Can be calculated as the bits are going out over the network interface and appended to the end.

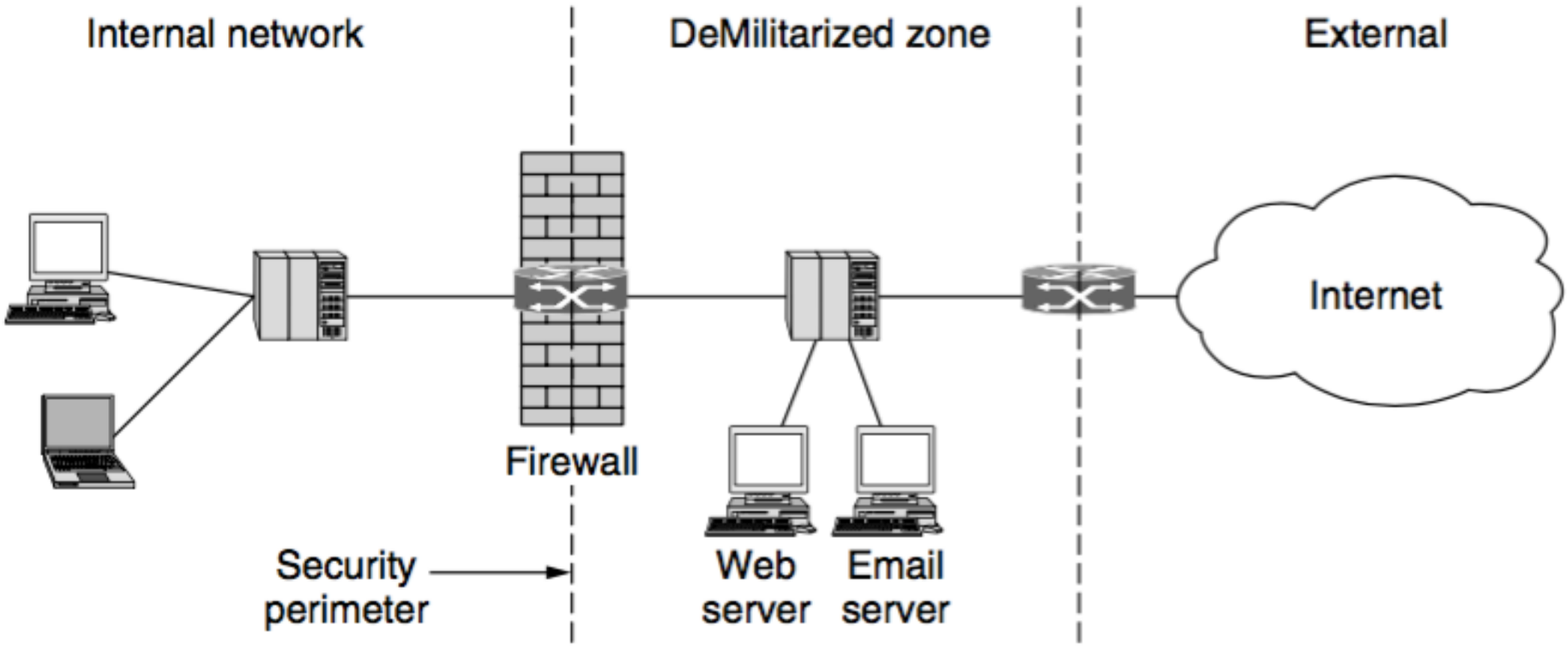
Given that ESP can do everything AH can do and more and is more efficient,
AH is likely to be phased out in the future.

Firewalls

Packet filtering
Inspects each and every incoming and outgoing packet

IP/Port filtering
Inspects IP addresses combined with TCP ports

DMZ (DeMilitarized Zone)
Part of the internal network that lies outside of the security perimeter

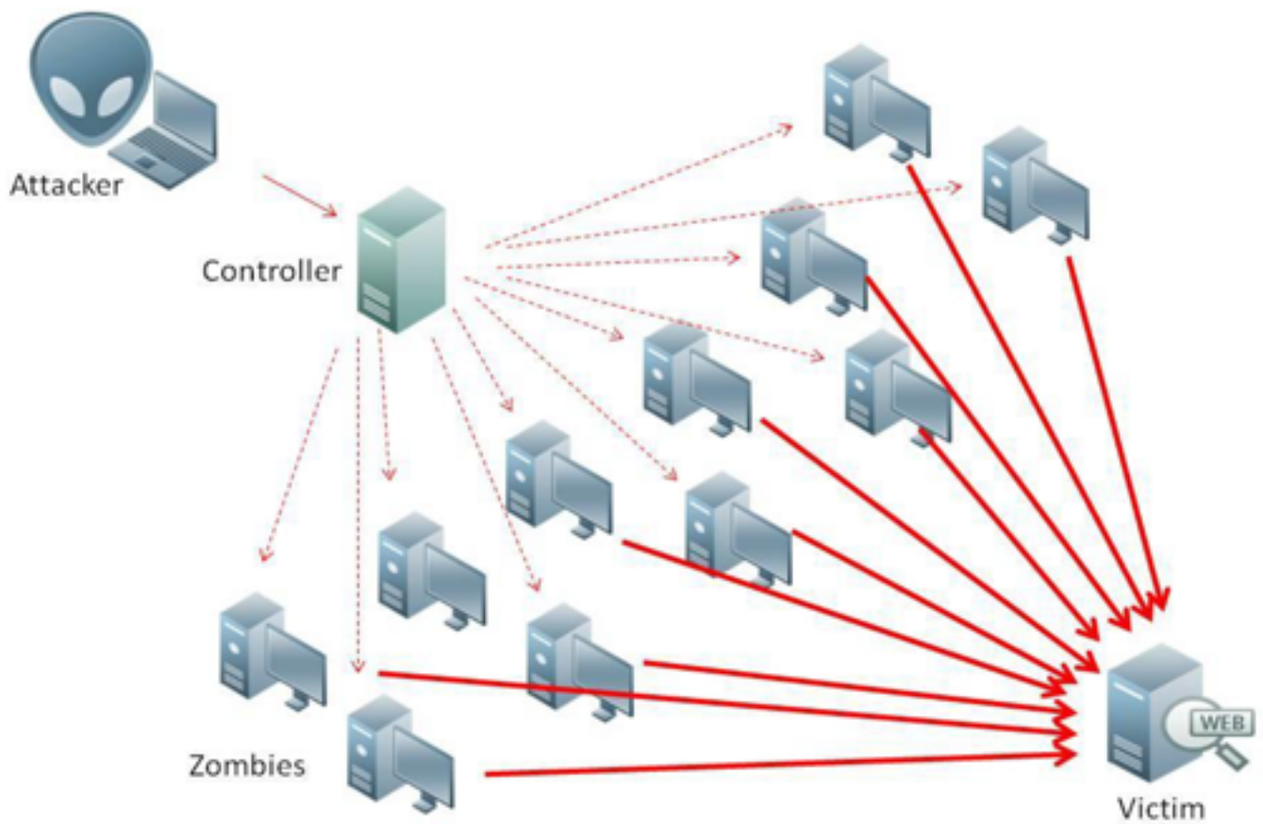


Firewalls

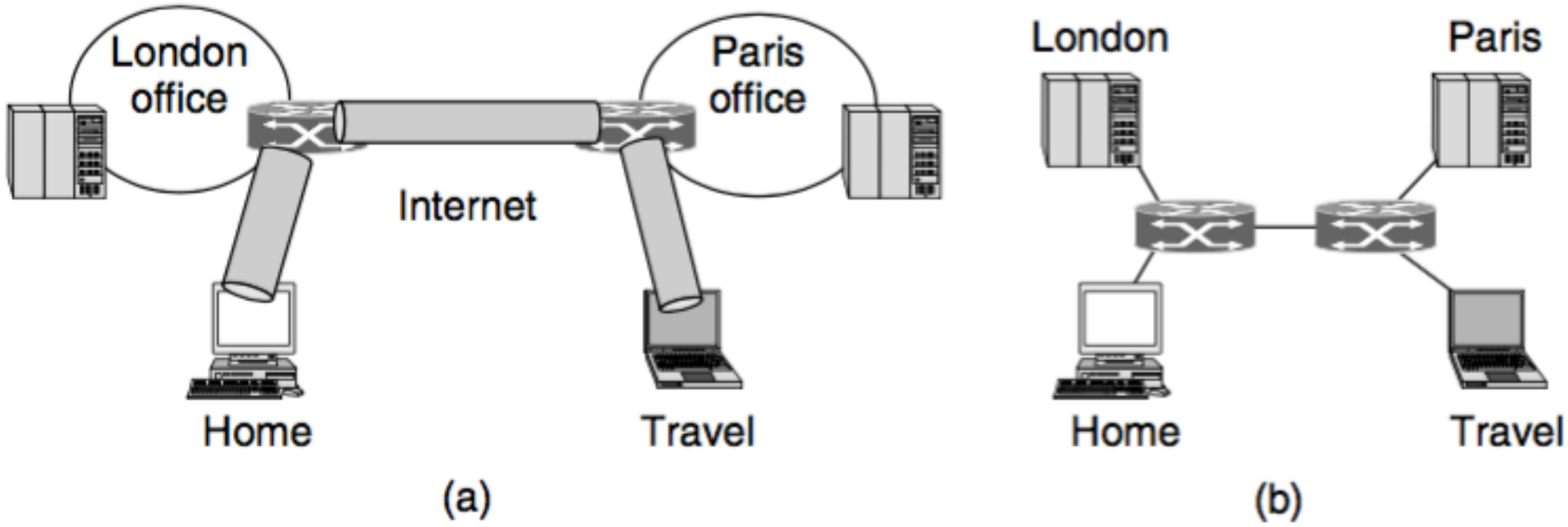
Stateful firewalls
Map packets to connections and use TCP/IP header fields to keep track of connections

Application-level gateways
Looking beyond the TCP header, to see what the application is doing
(block peer-to-peer file sharing)

Attacks that firewalls cannot prevent
DoS (Denial of Service)
DDoS (Distributed Denial of Service)



Virtual Private Networks



Each pair of firewalls has to negotiate the parameters of its SA.

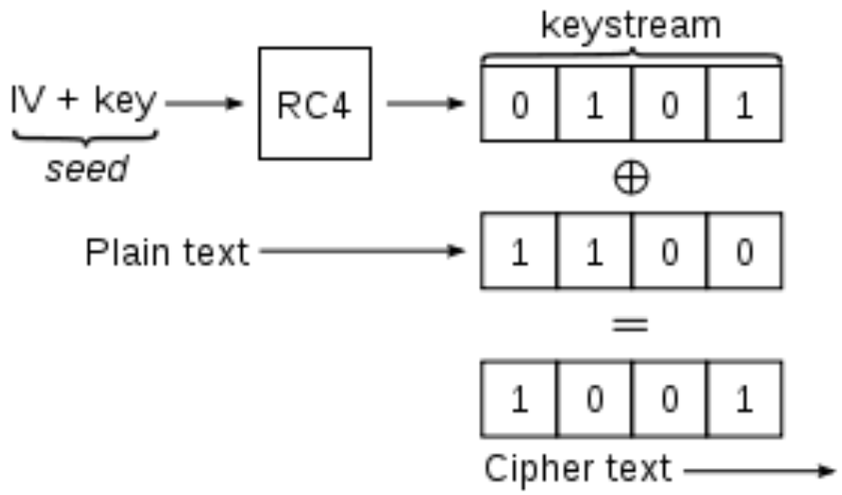
If IPsec is used for the tunneling, it is possible to aggregate all traffic.

Using MPLS (Multiprotocol Label Switching), VPN traffic can be set up across the ISP network.

Wireless Security

<u>WEP (Wired Equivalent Privacy)</u>

1. The pre-shared WEP key is also used for encrypting the data frames using RC4.
2. The key is concatenated with a 24-bit initialization vector (IV).
3. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

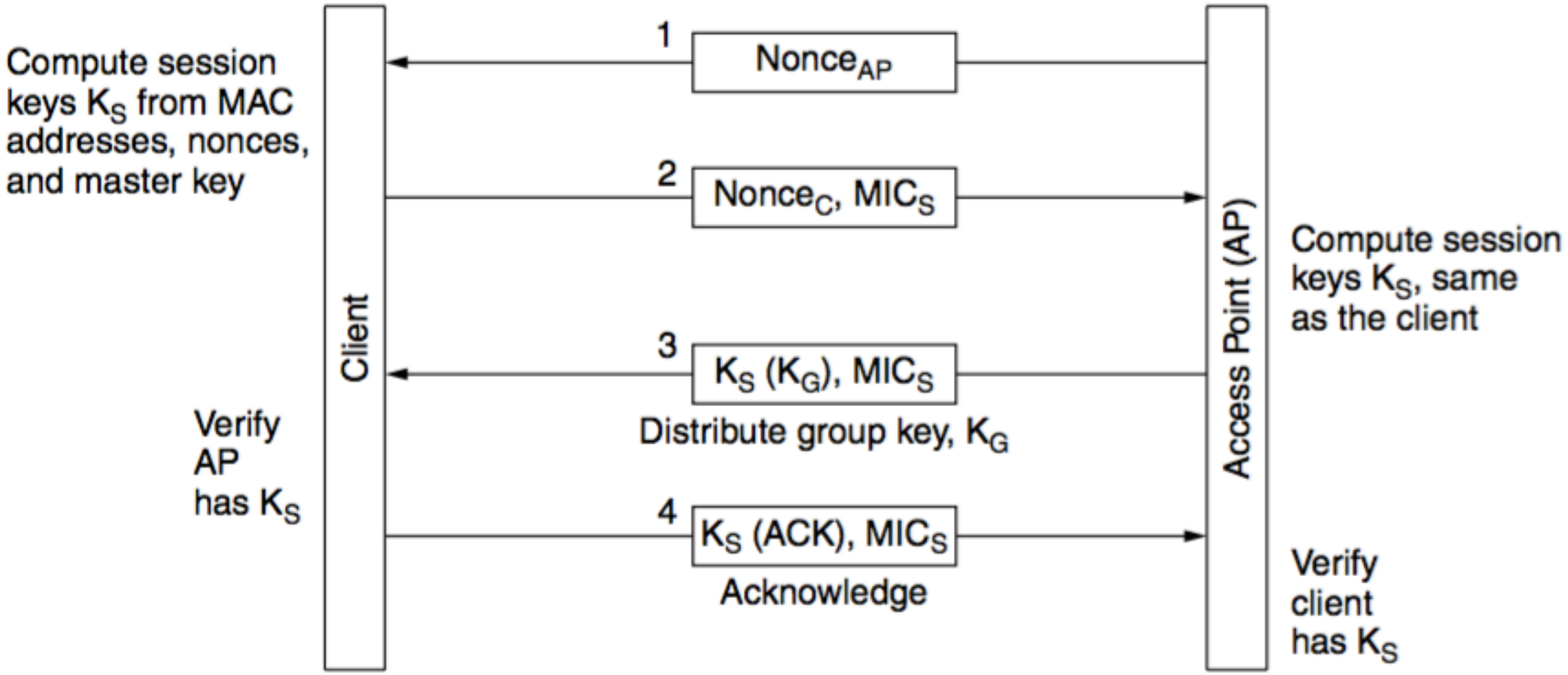


2001 Fluhrer *et al.* published a passive attack that can recover the RC4 key after eavesdropping on the network.

<u>WPA (Wi-Fi Protected Access)</u>

1. At the start of the handshake, the client has either the shared network password or its password for the authentication server
2. This password is used to derive a master key
3. The master key is not used directly to encrypt packets
4. A session key is computed with the four-packet handshake

802.11i Key Setup Handshake



Nonce

Random numbers used just once in security protocols

The message from the client is protected with an integrity check called a MIC (Message Integrity Check)

The client uses the nonces, its MAC address and that of the AP, and the master key to compute a session key, K_S

Bluetooth Security

Physical layer

Frequency hopping provides a little bit of security

Data-link layer

The slave and master each check to see if the other one knows the passkey
Then they select a random 128-bit session key, some of whose bits may be public

Network layer

Encryption uses a stream cipher called E_0
Integrity control uses SAFER+

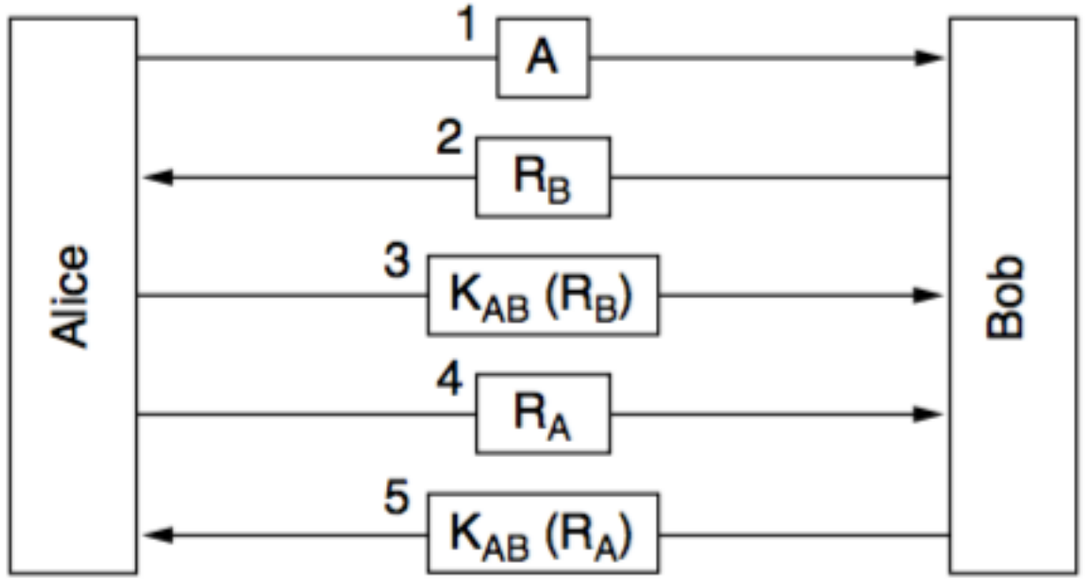
Application layer

In the event of a breach of link-level security, some security may remain, especially for applications that require a PIN code

Authentication Protocols

Challenge-response protocols

One party sends a random number to the other, who then transforms it in a special way and returns the result

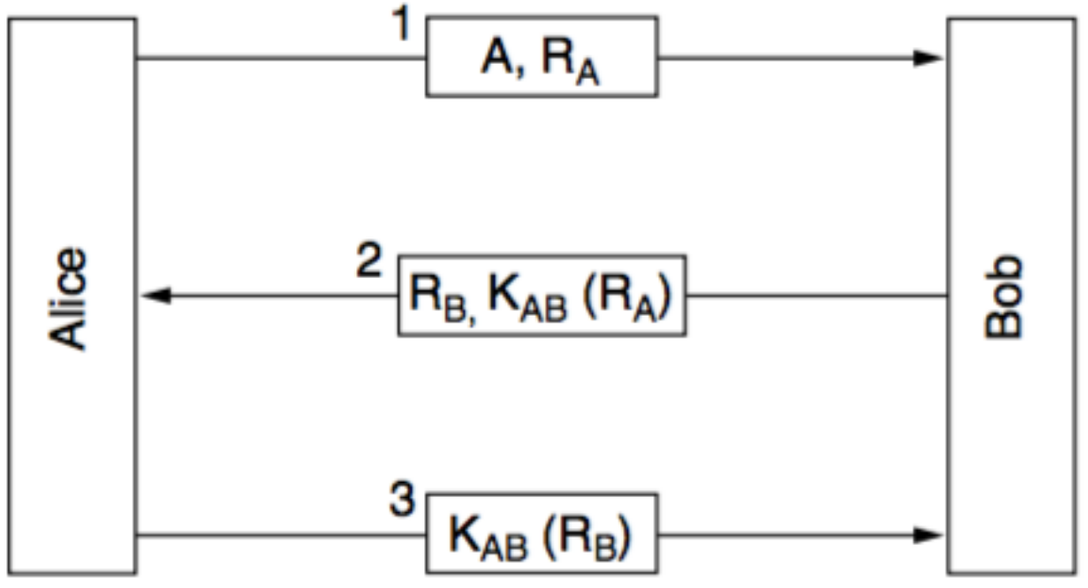


A, B are the identities of Alice and Bob.

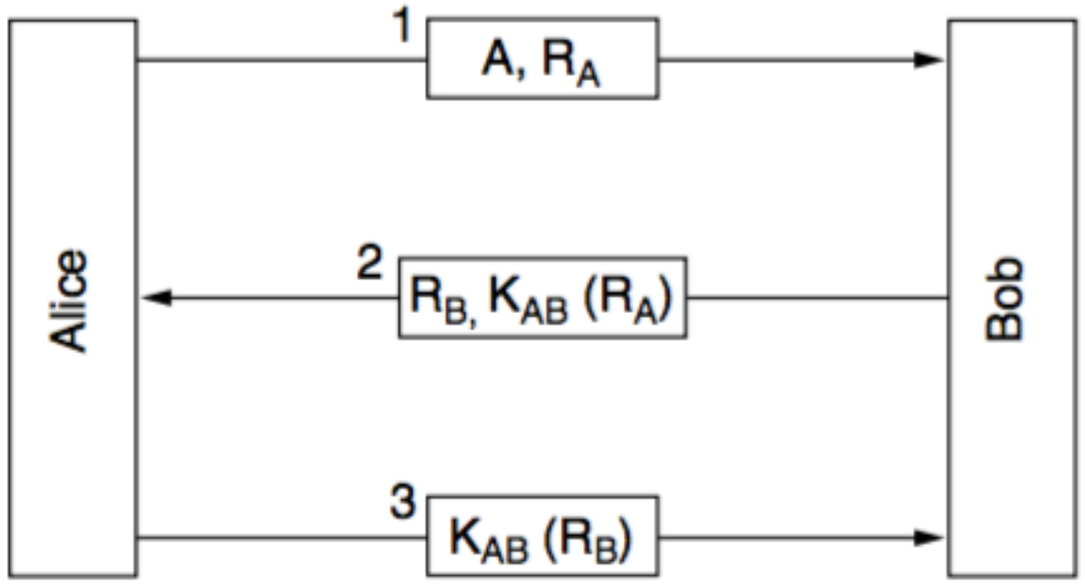
R_i's are the challenges, where i identifies the challenger.

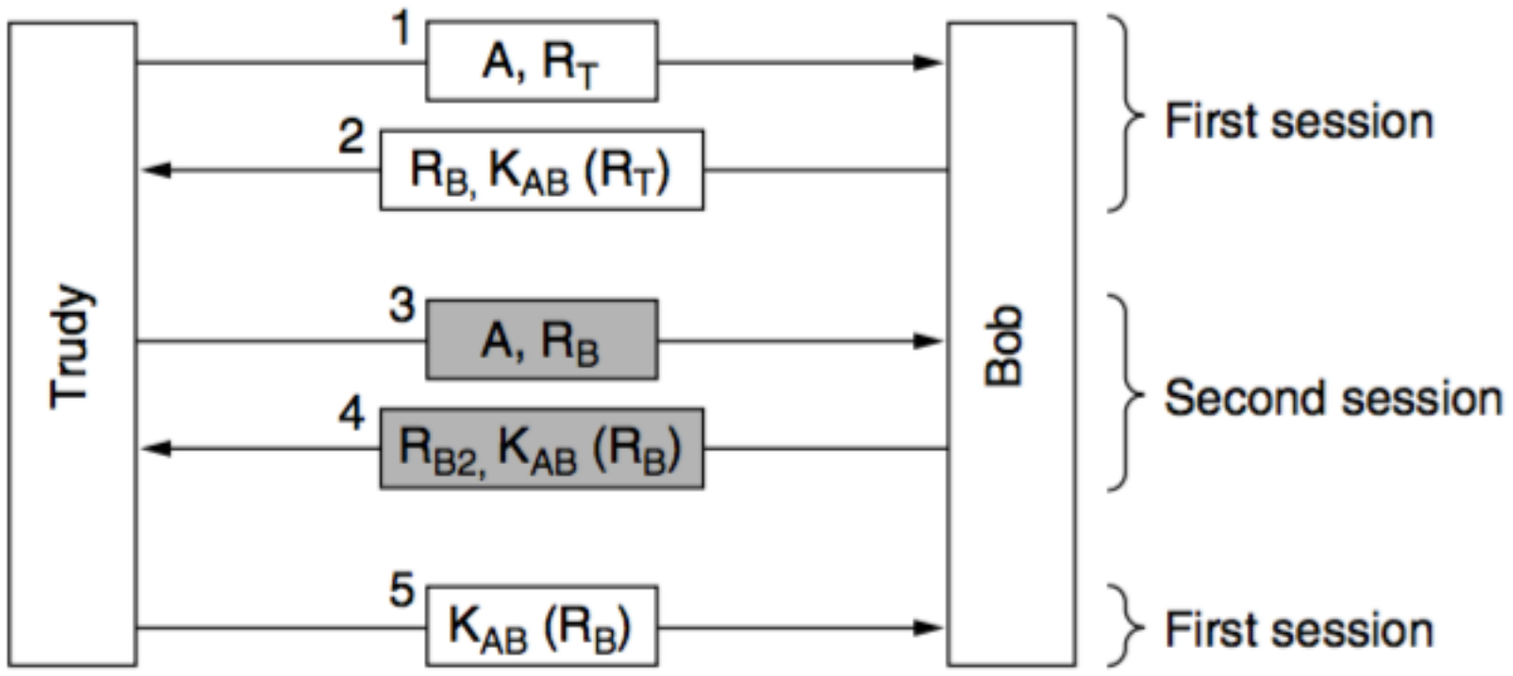
K_i's are keys, where i indicates the owner.

K_S is the session key.



Reflection Attack



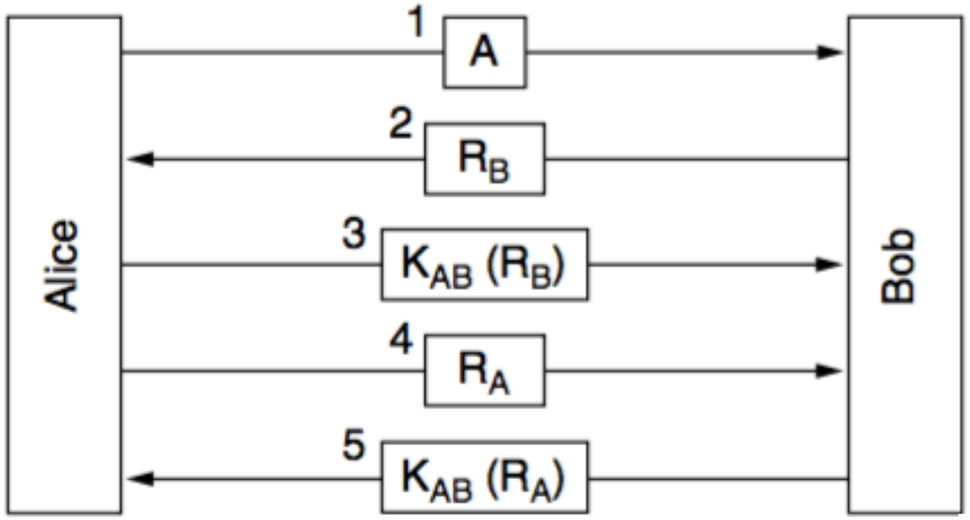


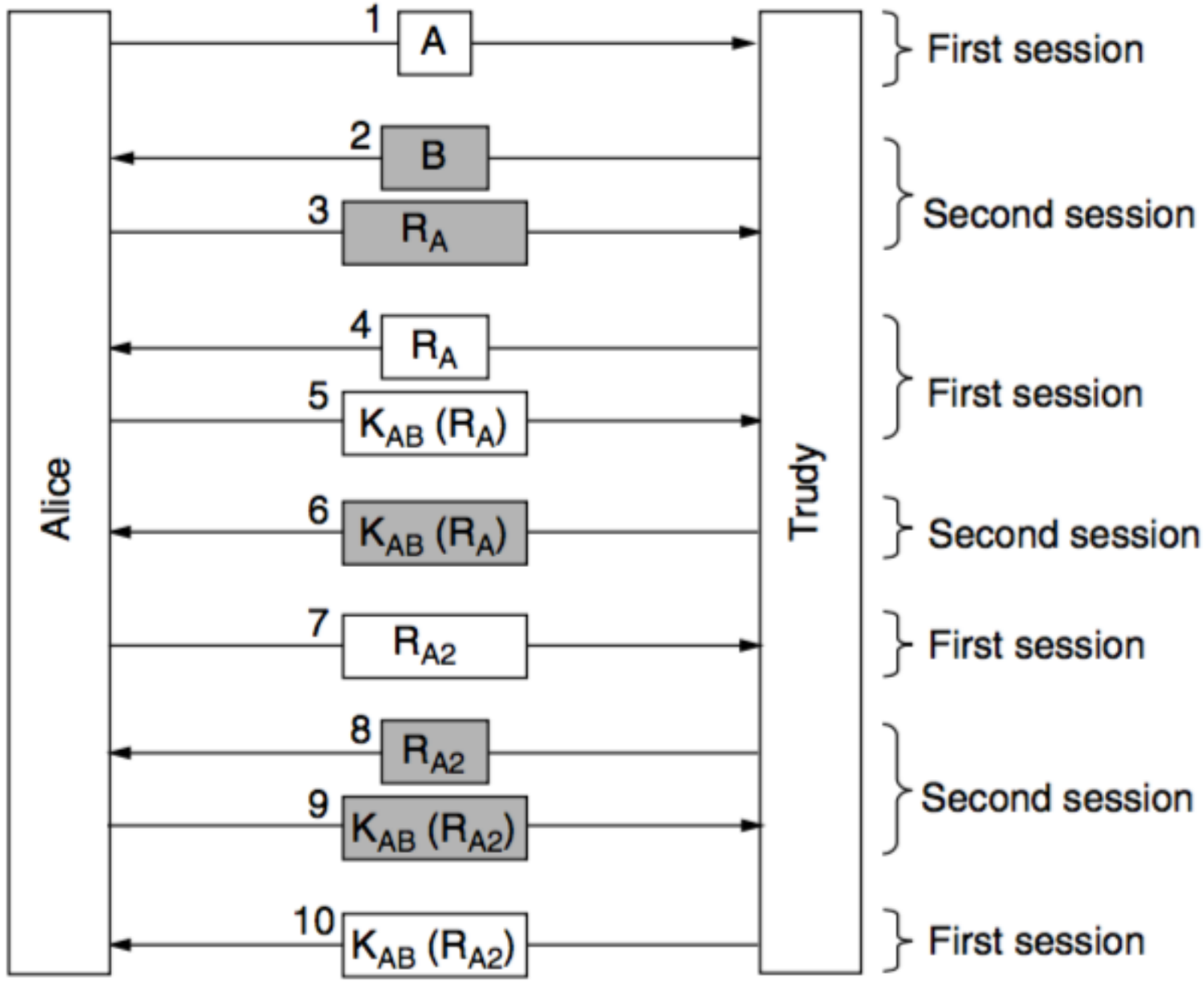
Authentication Protocols

Four general rules

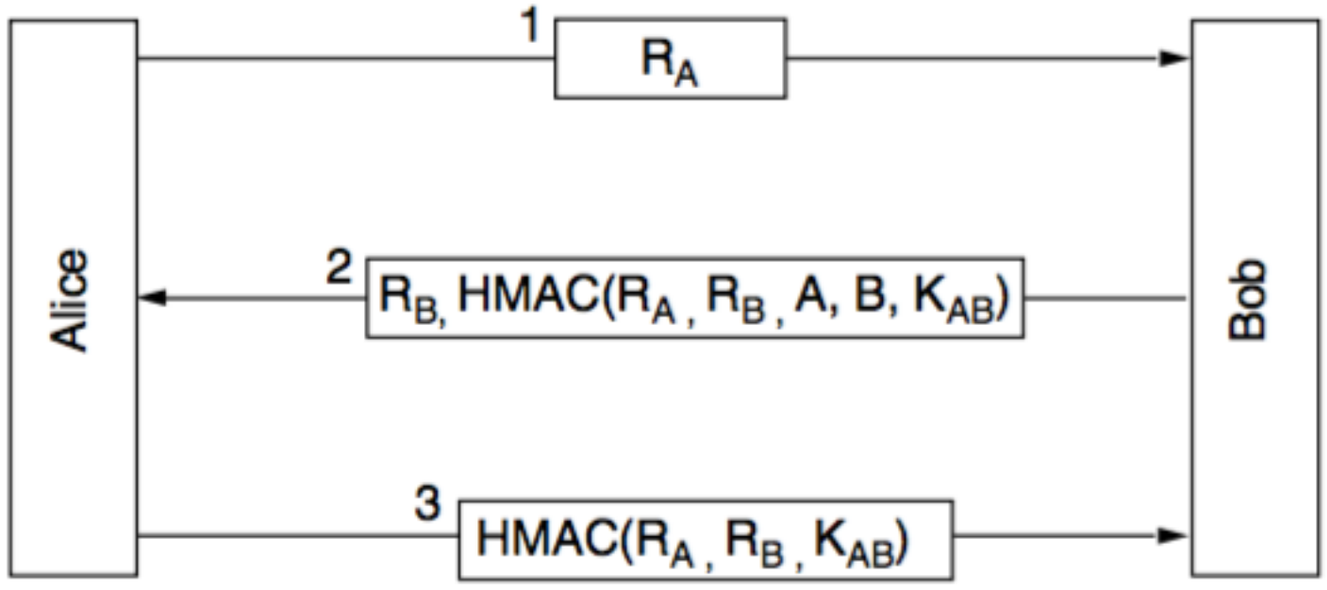
1. Have the initiator prove who she is before the responder has to. This avoids Bob giving away valuable information before Trudy has to give any evidence of who she is.
2. Have the initiator and responder use different keys for proof, even if this means having two shared keys, K_{AB} and K'_{AB}.
3. Have the initiator and responder draw their challenges from different sets. For example, the initiator must use even numbers and the responder must use odd numbers.
4. Make the protocol resistant to attacks involving a second parallel session in which information obtained in one session is used in a different one.

Reflection Attack





Authentication Using HMACs



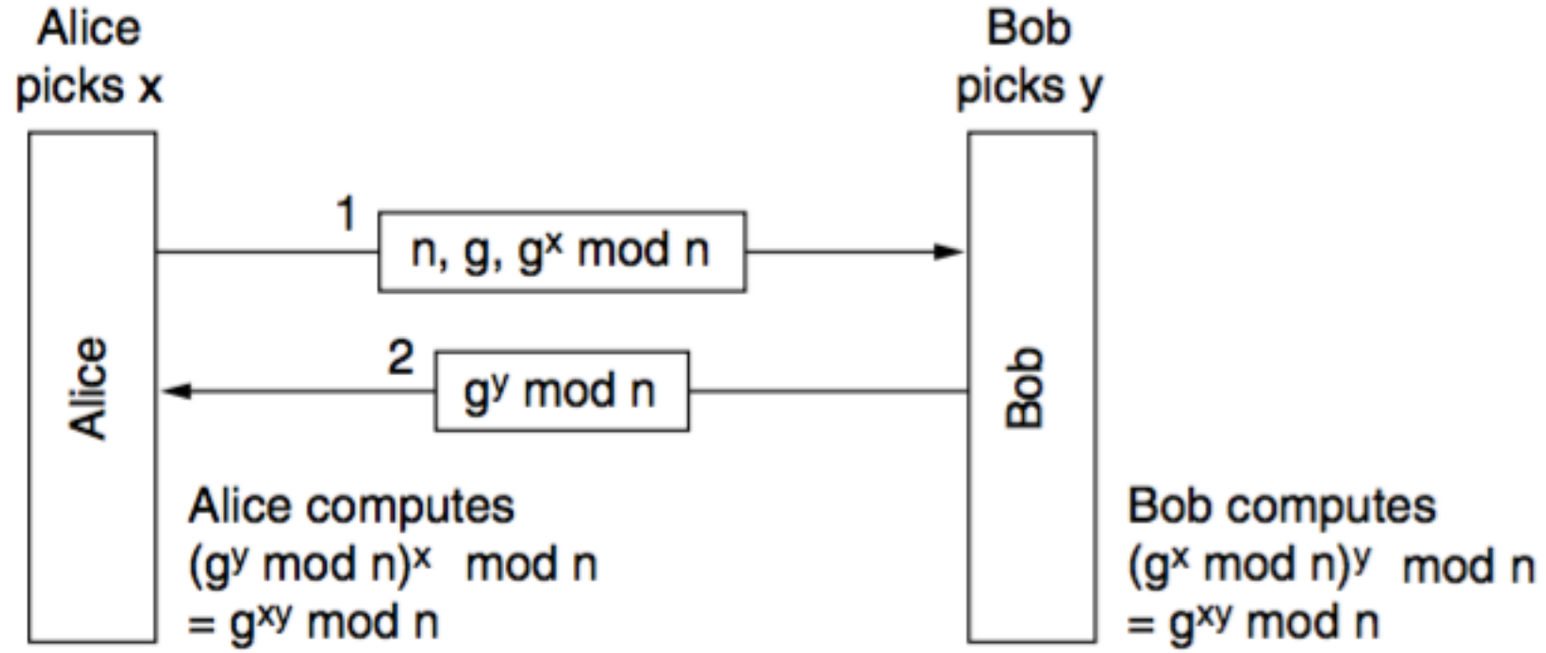
1. Alice starts out by sending Bob a nonce, R_A
2. Bob responds by selecting his own nonce, R_B, and sending it back along with an HMAC
3. Alice now has R_A, R_B, the two identities, and the secret key, K_{AB} so she can compute the HMAC herself
4. Alice responds to Bob with an HMAC containing just the two nonces.

Both HMACs include values chosen by the sending party, something that Trudy cannot control.

Establishing a Shared Key

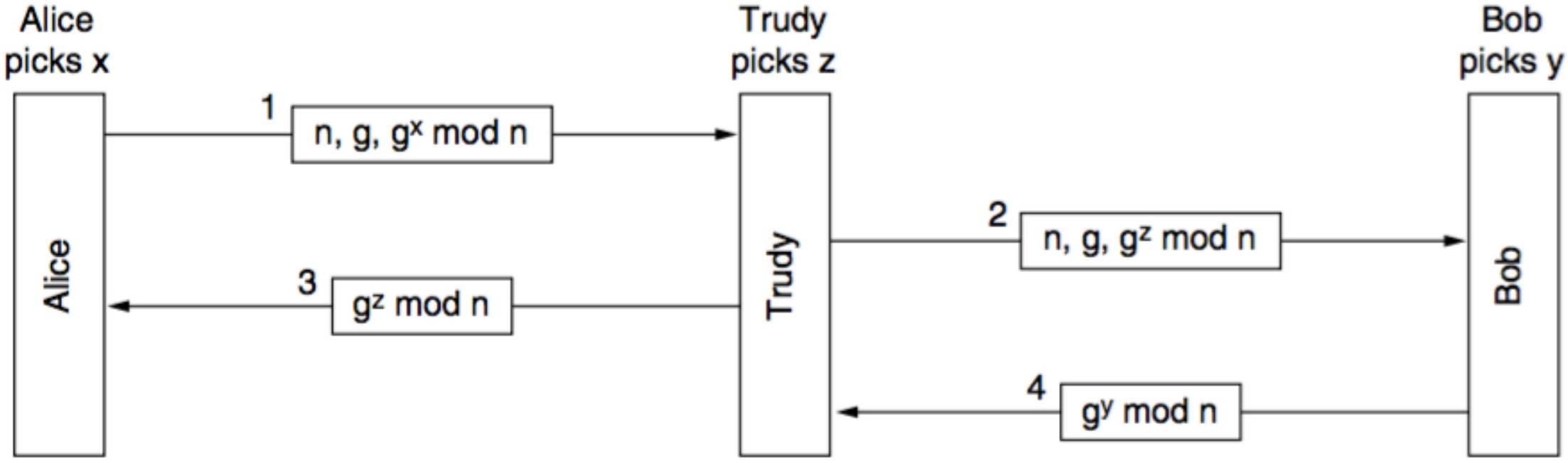
<u>The Diffie-Hellman Key Exchange</u>

n is a large prime number
g is a large number
x and y are 1024-bit numbers



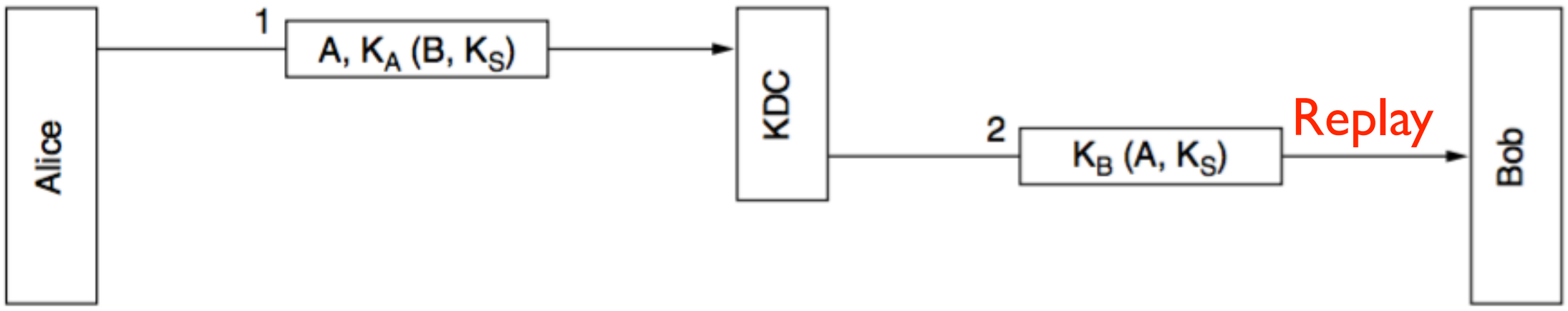
1. Alice initiates the key exchange protocol by sending Bob a message containing $(n, g, g^x \bmod n)$
2. Bob responds by sending Alice a message containing $g^y \bmod n$
3. Alice computes $(g^y \bmod n)^x \bmod n$
4. Bob computes $(g^x \bmod n)^y \bmod n$
5. Alice and Bob now share a secret key $g^{xy} \bmod n$

Man-in-the-Middle Attack



1. While Alice and Bob are choosing x and y, respectively, Trudy picks her own random number, z.
2. Trudy intercepts Alice's message and sends it to Bob, using her own z instead of x.
3. Trudy intercepts Bob's message and sends it to Alice, using her own z instead of y.
4. Alice computes the secret key as g^{xz} mod n, and so does Trudy
5. Bob computes g^{yz} mod n, and so does Trudy

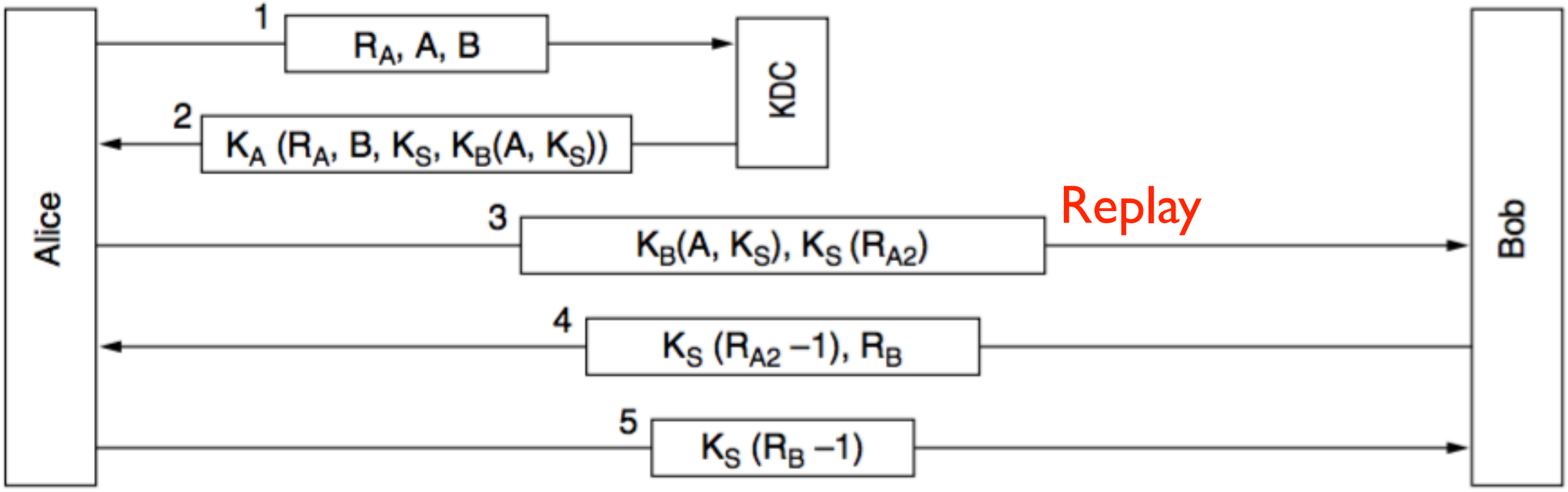
Authentication Using a Key Distribution Center



Replay attack

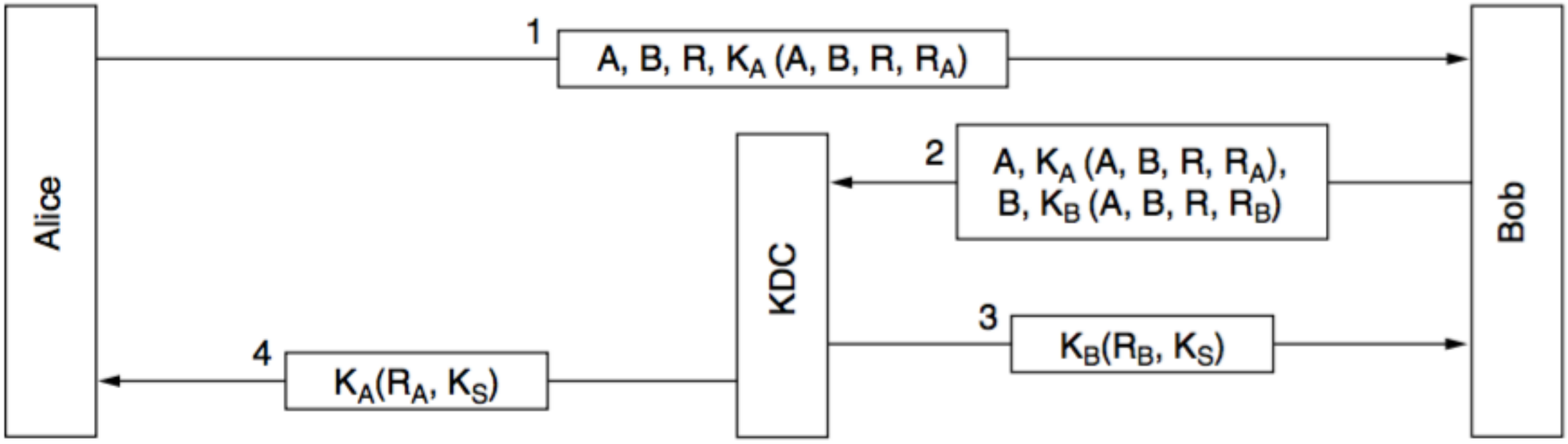
If message 2 was a bank transfer request

Needham-Schroeder protocol



Authentication Using a Key Distribution Center

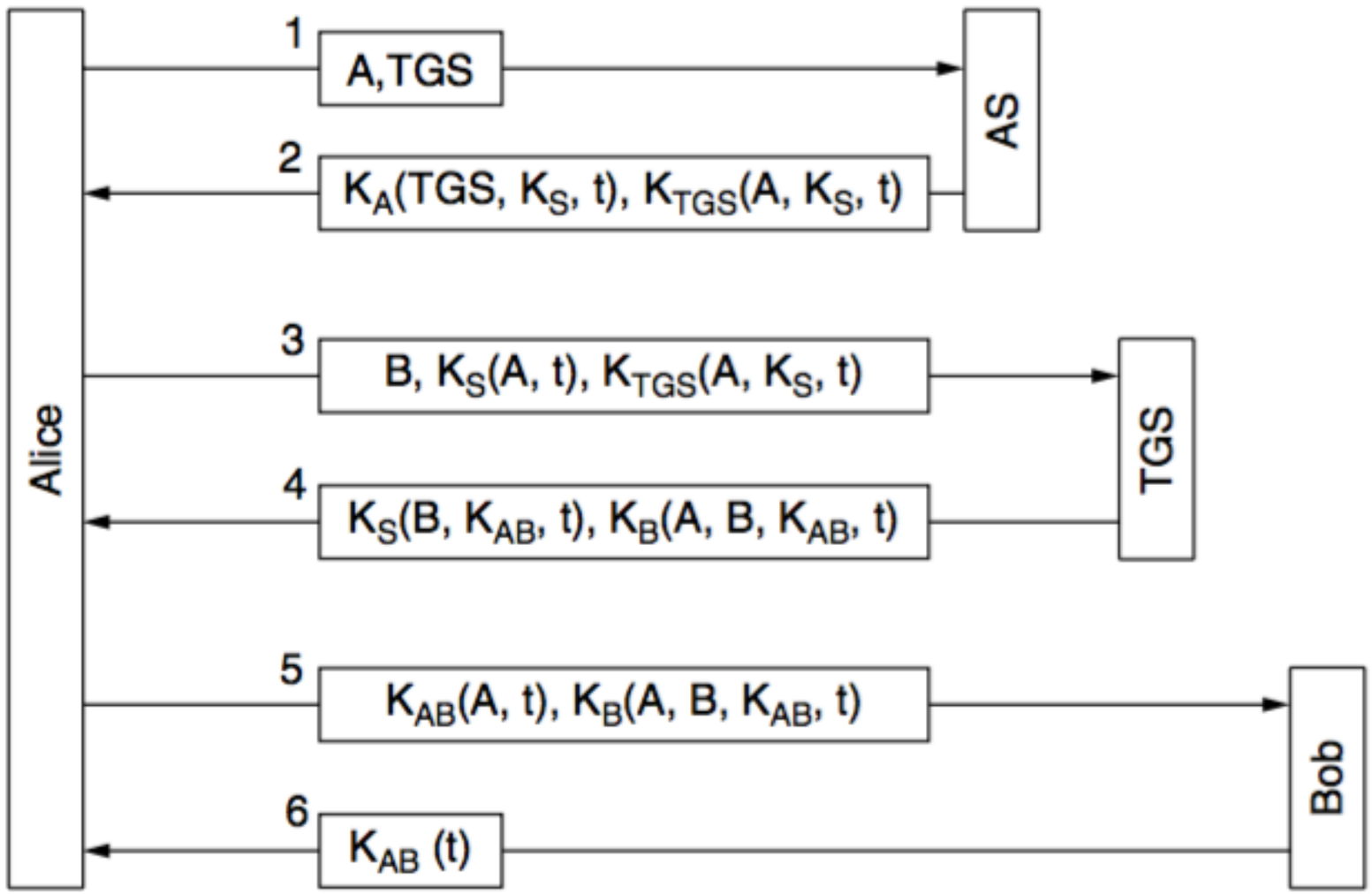
Otway-Rees protocol



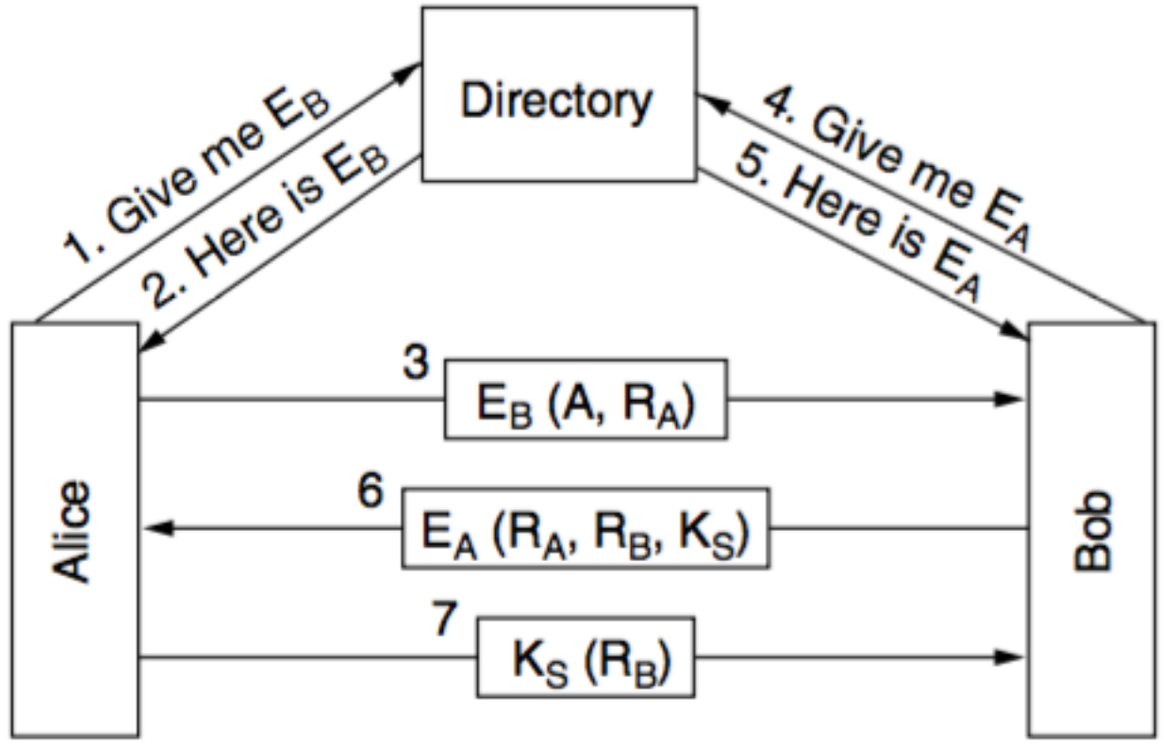
Authentication Using Kerberos

Authentication Server (AS)
Verifies users during login. Similar to KDC.

Ticket-Granting Server (TGS)
Issues "proof of identity tickets."



Authentication Using Public-Key Cryptography



1. Alice asks for Bob's public key
2. X.509 certificate containing Bob's public key
3. Alice sends Bob a nonce R_A
4. Bob asks for Alice's public key
5. X.509 certificate containing Alice's public key
6. Bob sends Alice's R_A , his own nonce, R_B , and a proposed session key, K_S
7. Alice sends back R_B encrypted with K_S

Email Security

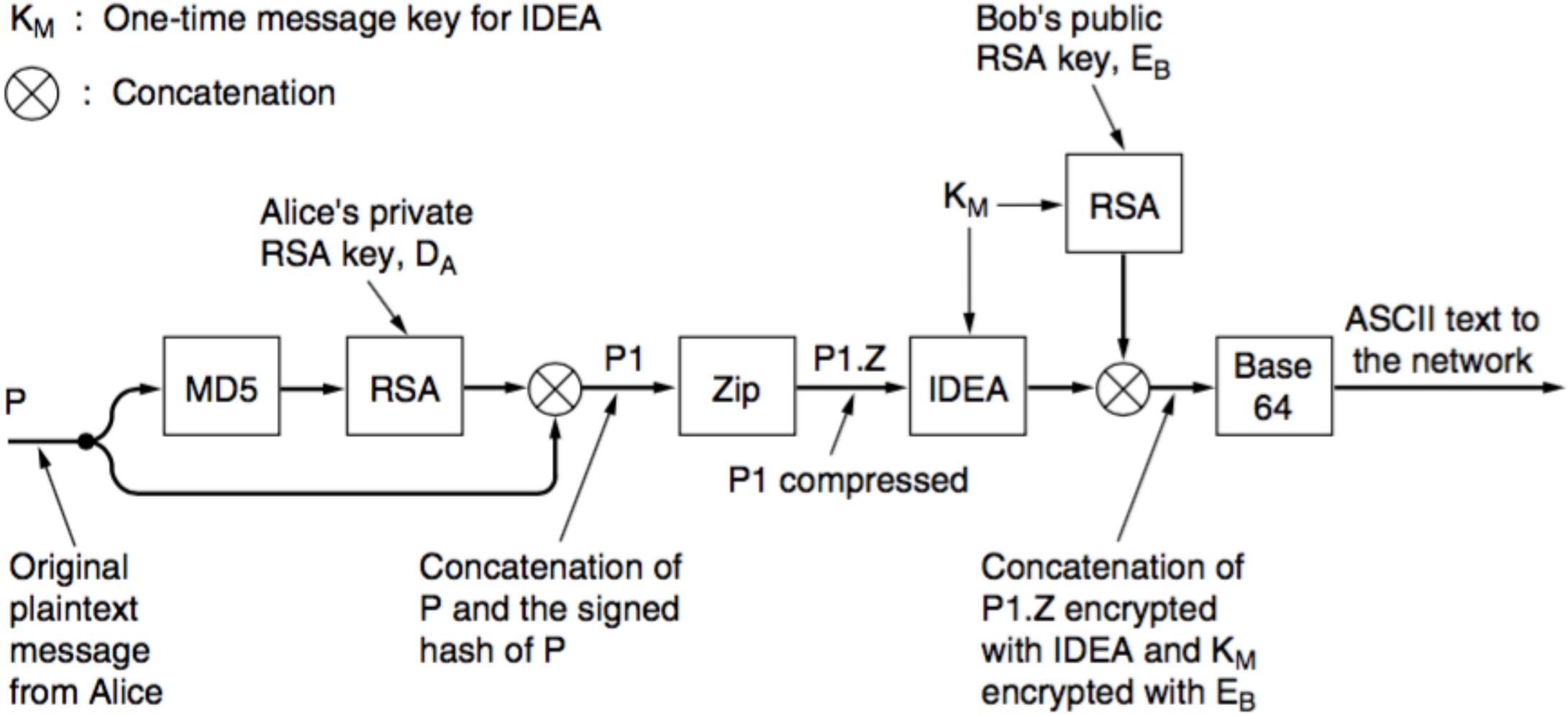
PGP (Pretty Good Privacy)

Encrypts data by using a block cipher called IDEA (International Data Encryption Algorithm), which uses 128-bit keys.

Key management uses RSA

Data integrity uses MD5

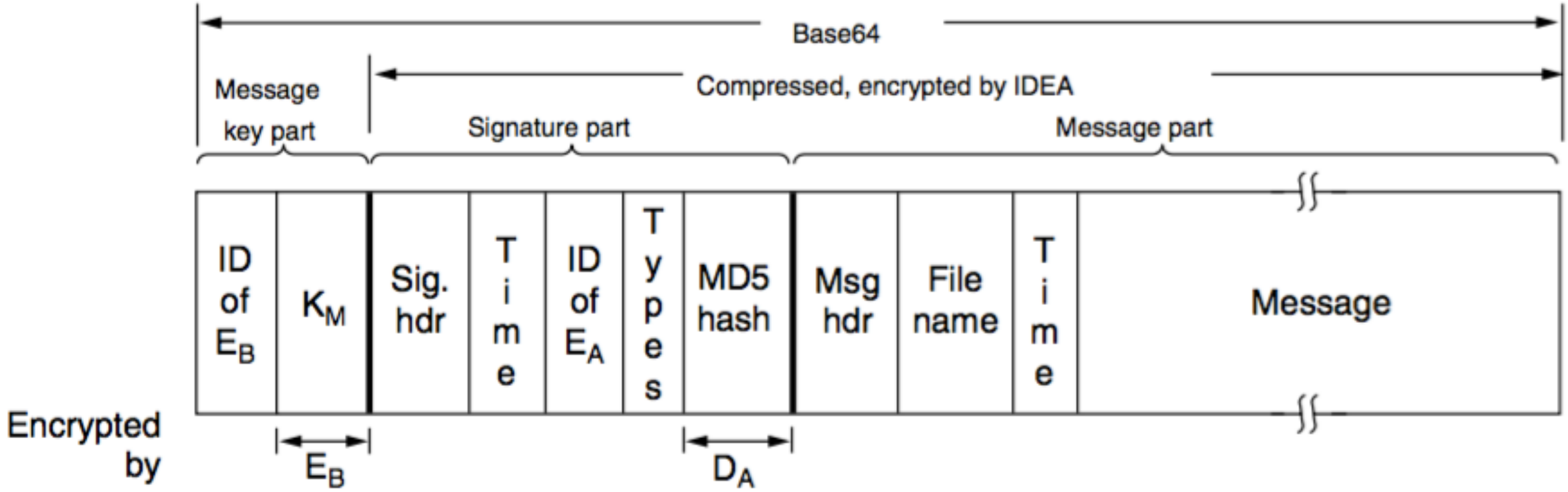
Open source



PGP

RSA key lengths

1. Casual (384 bits): Can be broken easily today.
2. Commercial (512 bits): Breakable by three-letter organizations.
3. Military (1024 bits): Not breakable by anyone on earth.
4. Alien (2048 bits): Not breakable by anyone on other planets, either.



Private/public key ring

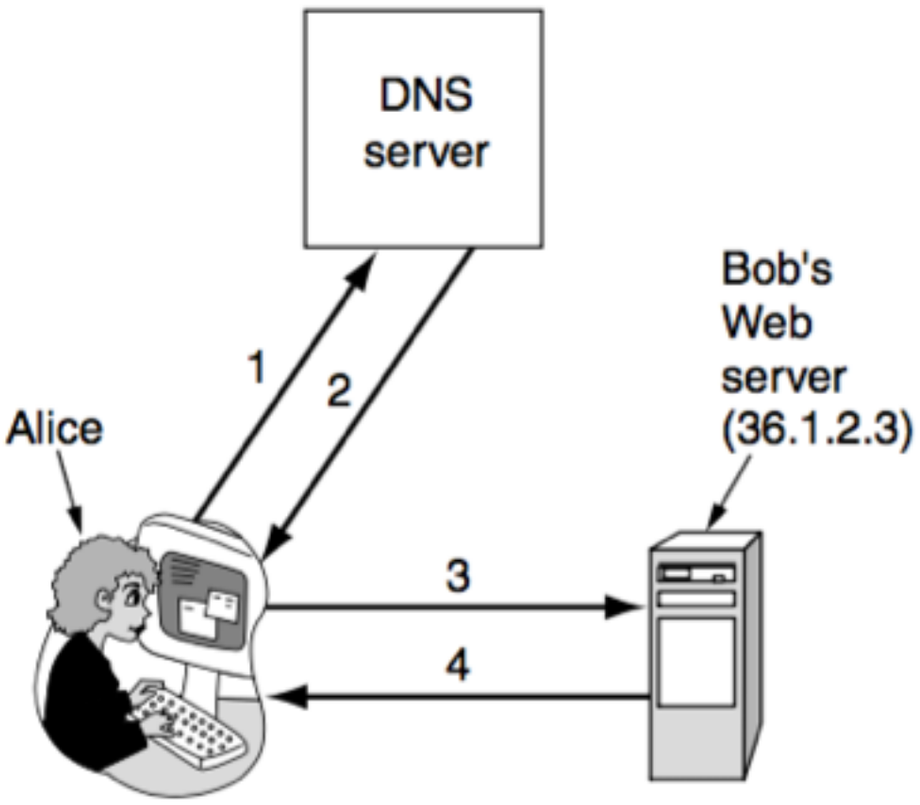
The reason for supporting multiple pairs per user is to permit users to change their public keys periodically or when one is thought to have been compromised, without invalidating messages currently in preparation or in transit.

Web Security

Possible web attacks

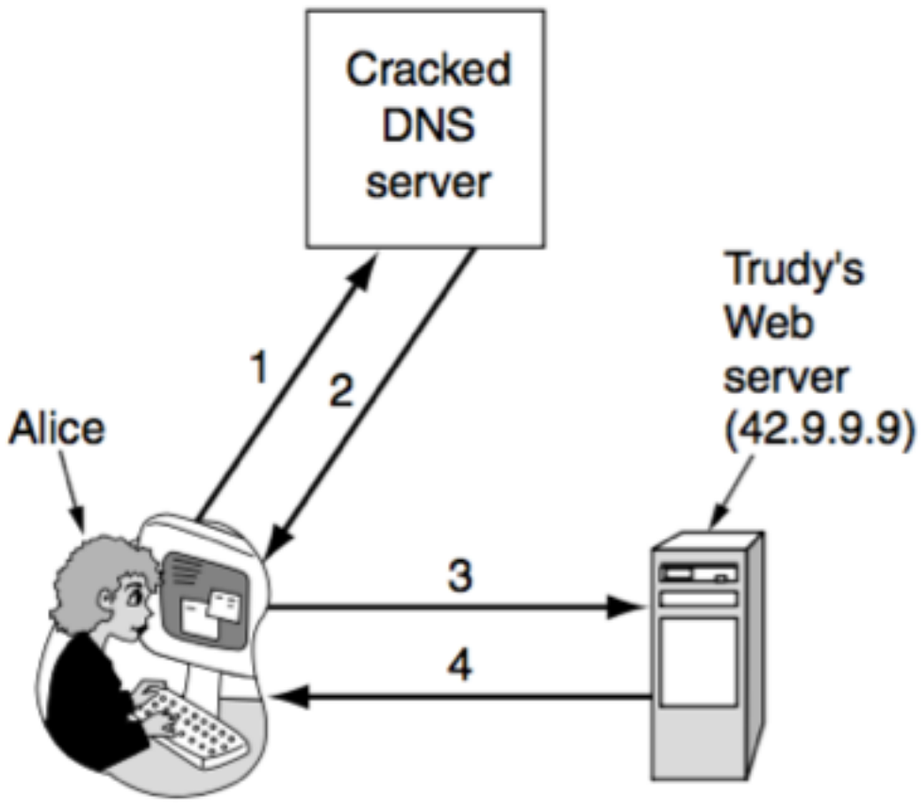
Rewriting webpage content
DDoS
Impersonate websites
Identity theft

DNS spoofing



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

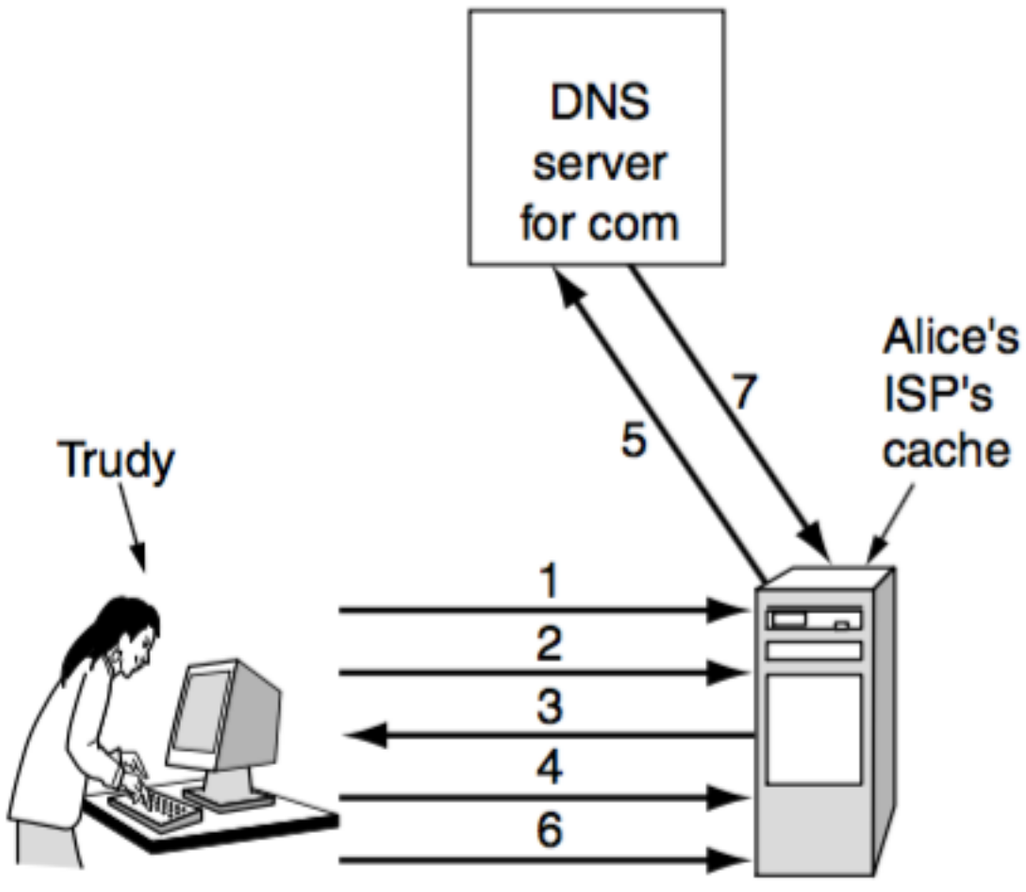
(a)



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)

DNS spoofing



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)

<u>DNSsec</u>

1. Proof of where the data originated.
2. Public key distribution.
3. Transaction and request authentication.

RRSets (Resource Record Sets)

- group of DNS records -

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...

KEY: Holds the public key of a zone, user, host
SIG: Holds the signed hash according to the algorithm specified in the KEY
CERT: Used for storing (e.g., X.509) certificates

Private keys can be stored offline except when it is inserted into the disconnected machine for signing the day's new RRSets

SSL—The Secure Sockets Layer

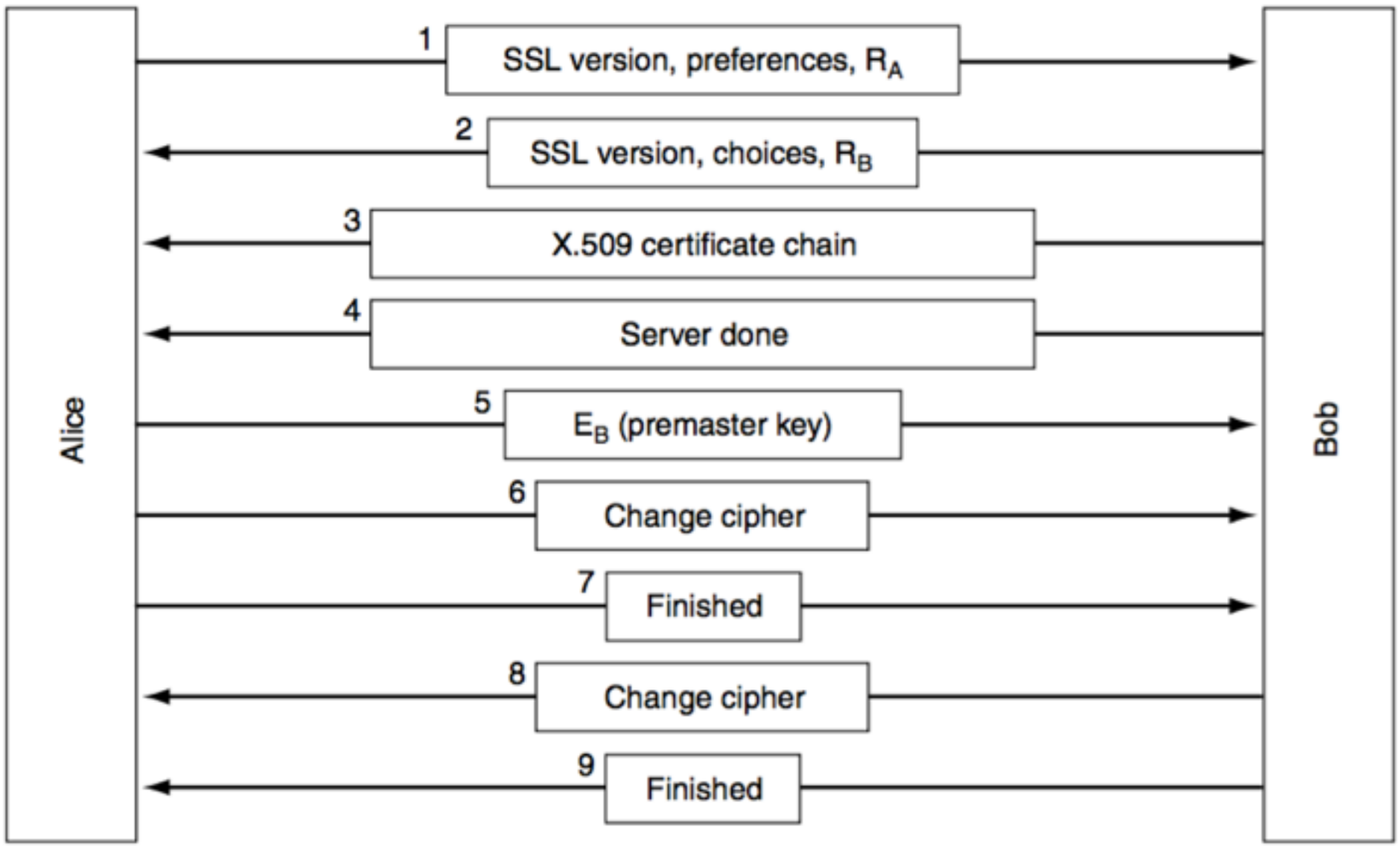
SSL handles

1. Parameter negotiation between client and server.
2. Authentication of the server by the client.
3. Secret communication.
4. Data integrity protection.

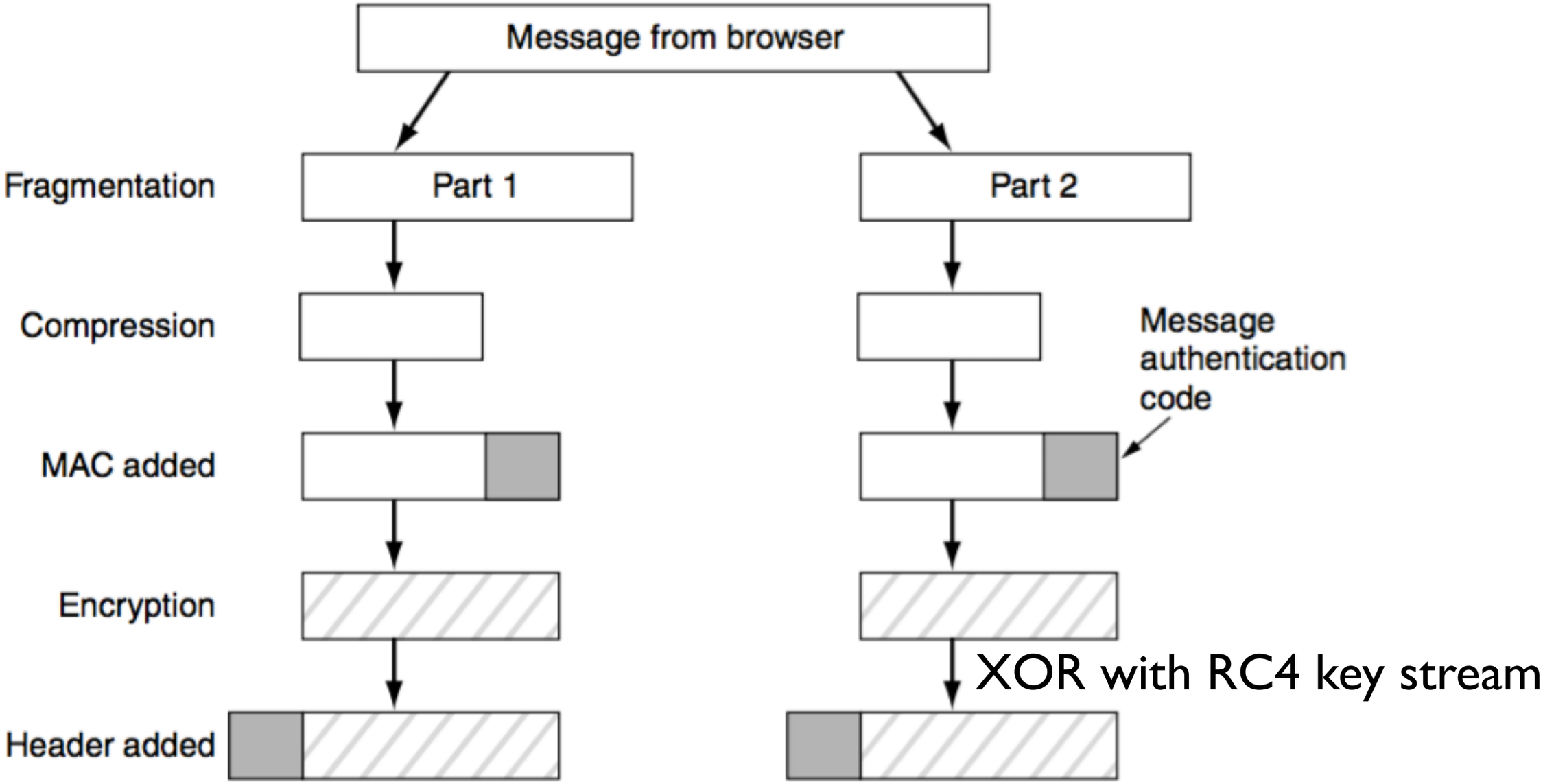
Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

http + ssl = https

SSL connection establishment



SSL Transmission



RC4 + MD5 ⟶ triple DES + SHA-1

SSL ⟶ TLS (Transport Layer Security)

Mobile Code Security

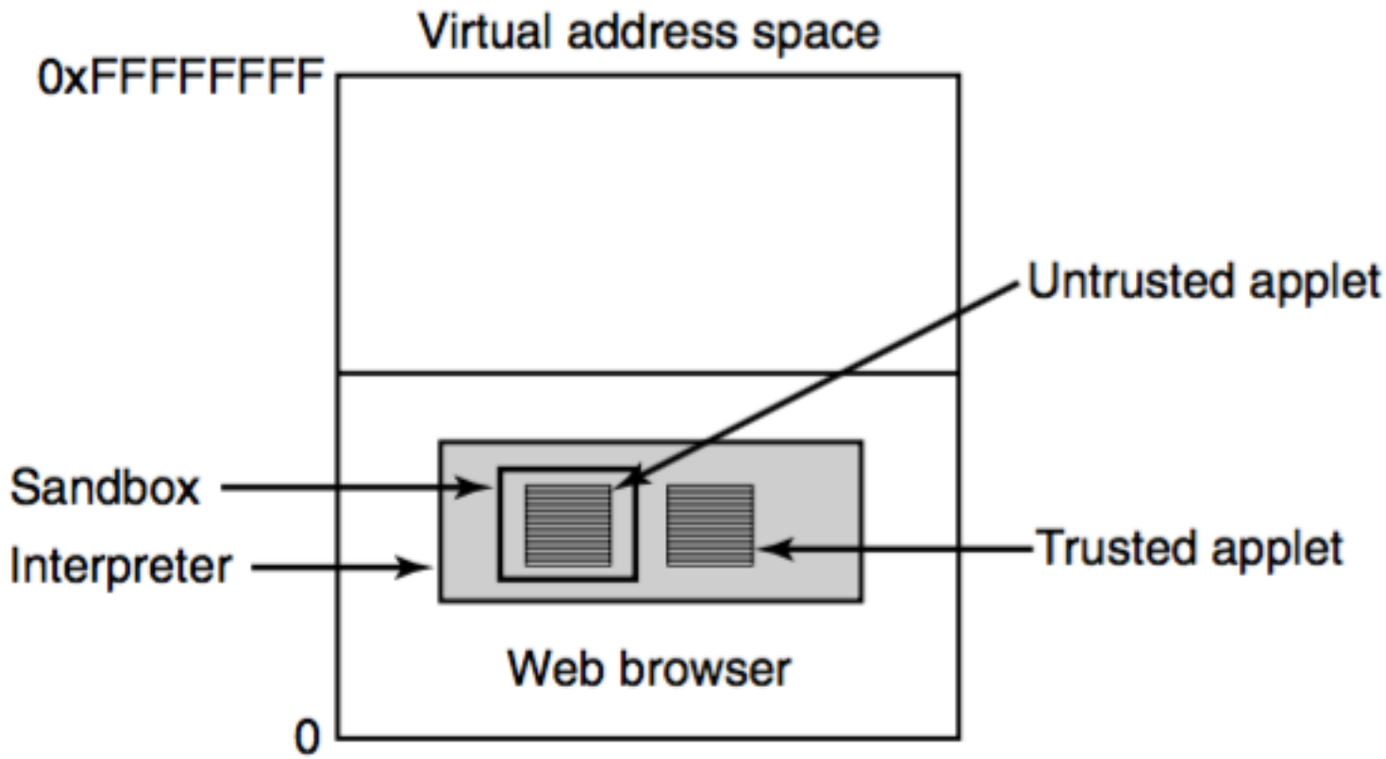
Java Applets

Java applets are small Java programs compiled to a stack-oriented machine language called JVM (Java Virtual Machine). They can be placed on a Web page for downloading along with the page.

ActiveX

x86 binary programs that can be embedded in Web pages.

Each ActiveX control is accompanied by a digital signature.



Other security risks

Javascript
PDF
Flash
Viruses