Network Security

Chapter 8

Network Security

Adversary	**Goal**
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

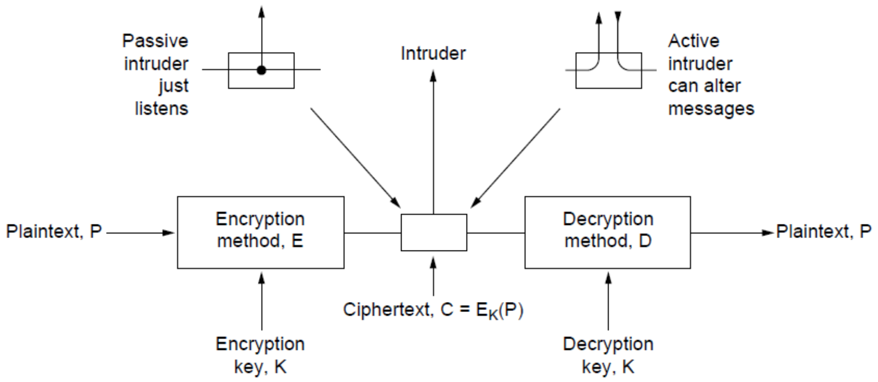
Some people who cause security problems and why.

Cryptography

- Introduction
- Substitution ciphers
- Transposition ciphers
- One-time pads
- Fundamental cryptographic principles

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

Introduction



The encryption model (for a symmetric-key cipher).

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

Substitution Ciphers

plaintext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ciphertext:	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Monoalphabetic substitution

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

Transposition Ciphers

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

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

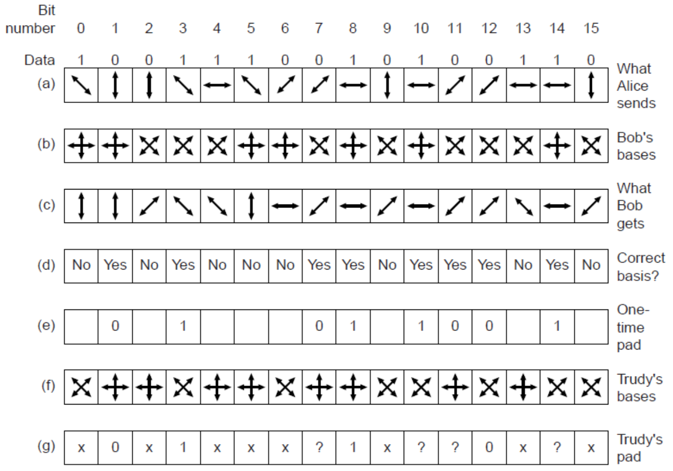
One-Time Pads (1)

Message 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Pad 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Ciphertext:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Pad 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Plaintext 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011

The use of a one-time pad for encryption and the possibility of getting any possible plaintext from the ciphertext by the use of some other pad.

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

One-Time Pads (2)



Bit number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Data	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1	0	
(a)	⤡	↕	↕	⤡	↔	⤡	⤢	⤢	↔	↕	↔	⤢	⤢	↔	↔	↕	What Alice sends
(b)	✛	✛	✕	✕	✕	✛	✛	✕	✛	✕	✛	✕	✕	✕	✛	✕	Bob's bases
(c)	↕	↕	⤢	⤡	⤡	↕	↔	⤢	↔	⤢	↔	⤢	⤢	⤡	↔	⤢	What Bob gets
(d)	No	Yes	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Correct basis?
(e)		0		1				0	1		1	0	0		1		One-time pad
(f)	✕	✛	✛	✕	✛	✛	✕	✛	✛	✕	✕	✛	✕	✛	✕	✕	Trudy's bases
(g)	x	0	x	1	x	x	x	?	1	x	?	?	0	x	?	x	Trudy's pad

An example of quantum cryptography

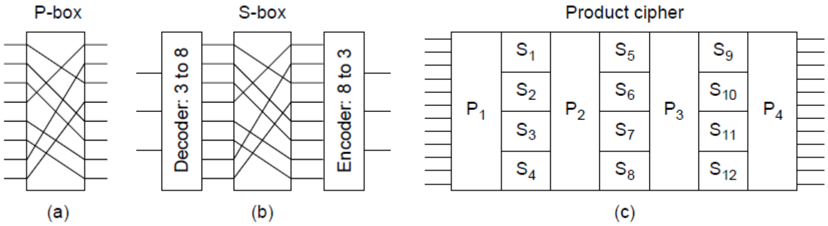
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Fundamental Cryptographic Principles

1. Messages must contain some redundancy

2. Some method is needed to foil replay attacks

Symmetric-key Algorithms (1)

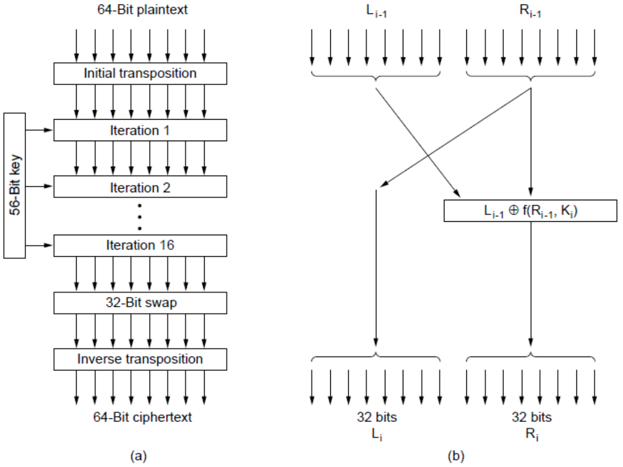


Basic elements of product ciphers.
(a) P-box. (b) S-box. (c) Product.

Symmetric-key Algorithms (2)

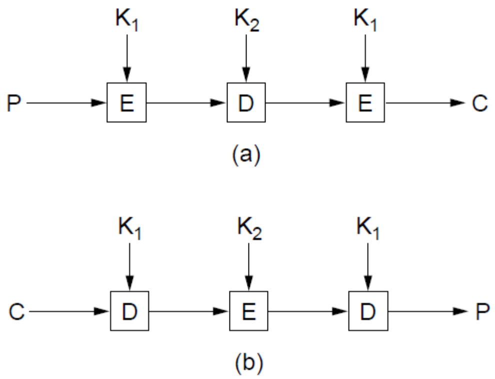
- Data encryption standard
- Advanced encryption standard
- Cipher modes
- Other ciphers
- Cryptanalysis

Data Encryption Standard (1)



The data encryption standard. (a) General outline. (b) Detail of one iteration. The circled + means exclusive OR

Data Encryption Standard (2)



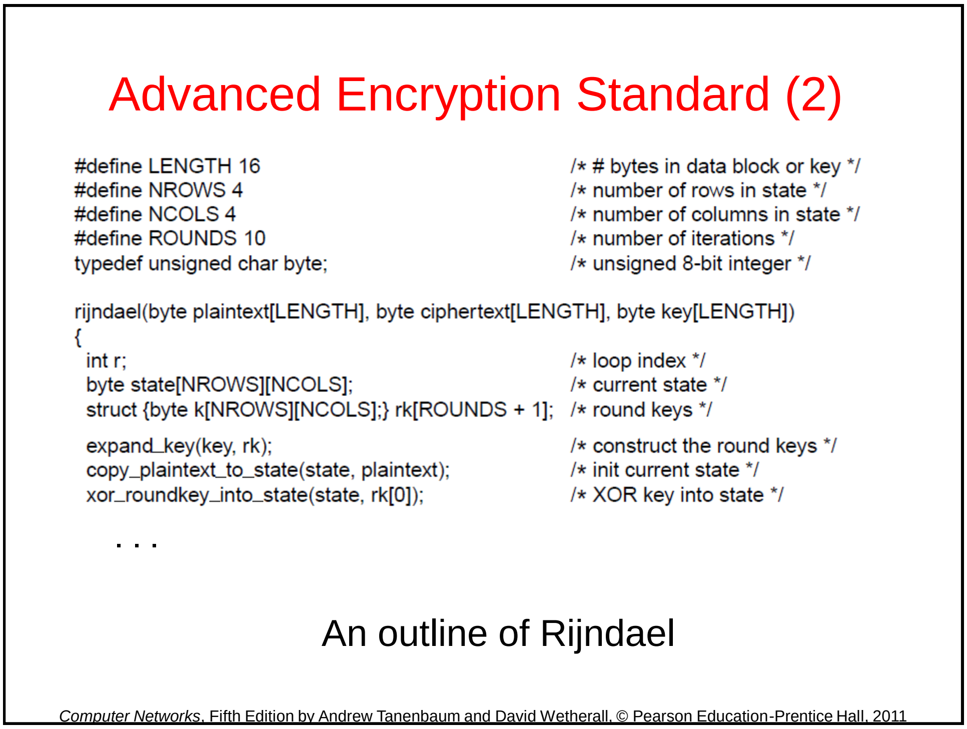
(a)

(b)

(a) Triple encryption using DES. (b) Decryption

Advanced Encryption Standard (1)

1. Algorithm symmetric block cipher.
2. Full design must be public.
3. Key lengths of 128, 192, and 256 bits supported.
4. Software and hardware implementations possible.
5. Algorithm public or licensed on nondiscriminatory terms.



Advanced Encryption Standard (2)

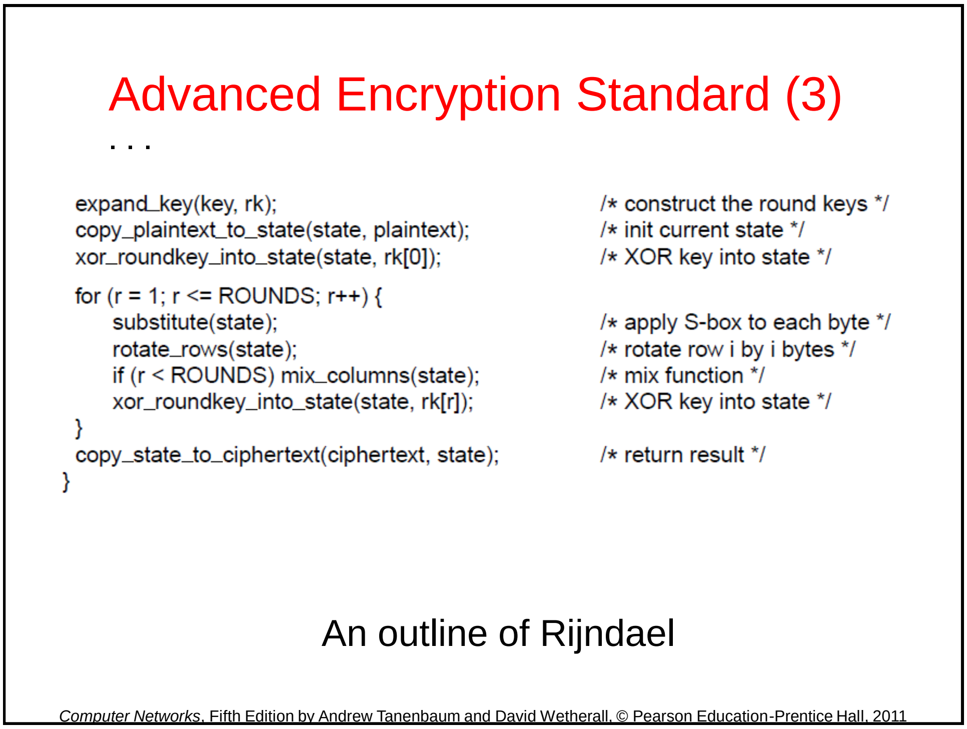
```
#define LENGTH 16                                 /* # bytes in data block or key */
#define NROWS 4                                   /* number of rows in state */
#define NCOLS 4                                   /* number of columns in state */
#define ROUNDS 10                                 /* number of iterations */
typedef unsigned char byte;                       /* unsigned 8-bit integer */

rijndael(byte plaintext[LENGTH], byte ciphertext[LENGTH], byte key[LENGTH])
{
  int r;                                          /* loop index */
  byte state[NROWS][NCOLS];                       /* current state */
  struct {byte k[NROWS][NCOLS];} rk[ROUNDS + 1];  /* round keys */

  expand_key(key, rk);                            /* construct the round keys */
  copy_plaintext_to_state(state, plaintext);      /* init current state */
  xor_roundkey_into_state(state, rk[0]);          /* XOR key into state */

     . . .
```

An outline of Rijndael



Advanced Encryption Standard (3)

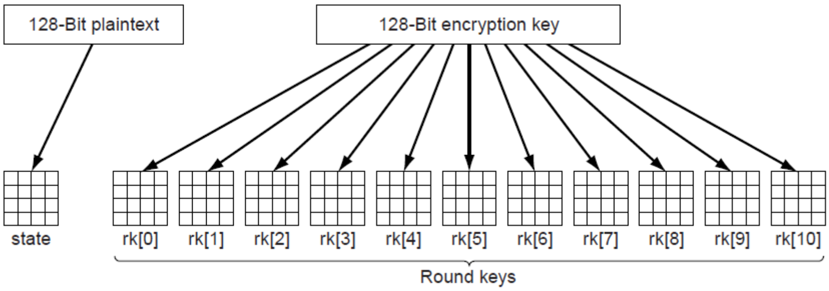
```
 . . .

 expand_key(key, rk);                              /* construct the round keys */
 copy_plaintext_to_state(state, plaintext);        /* init current state */
 xor_roundkey_into_state(state, rk[0]);            /* XOR key into state */

 for (r = 1; r <= ROUNDS; r++) {
       substitute(state);                          /* apply S-box to each byte */
       rotate_rows(state);                         /* rotate row i by i bytes */
       if (r < ROUNDS) mix_columns(state);         /* mix function */
       xor_roundkey_into_state(state, rk[r]);      /* XOR key into state */
 }
 copy_state_to_ciphertext(ciphertext, state);      /* return result */
}
```

An outline of Rijndael

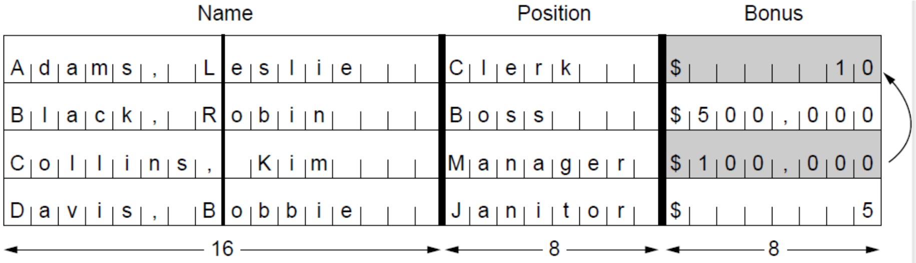
Advanced Encryption Standard (4)



Creating of the *state* and *rk* arrays

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

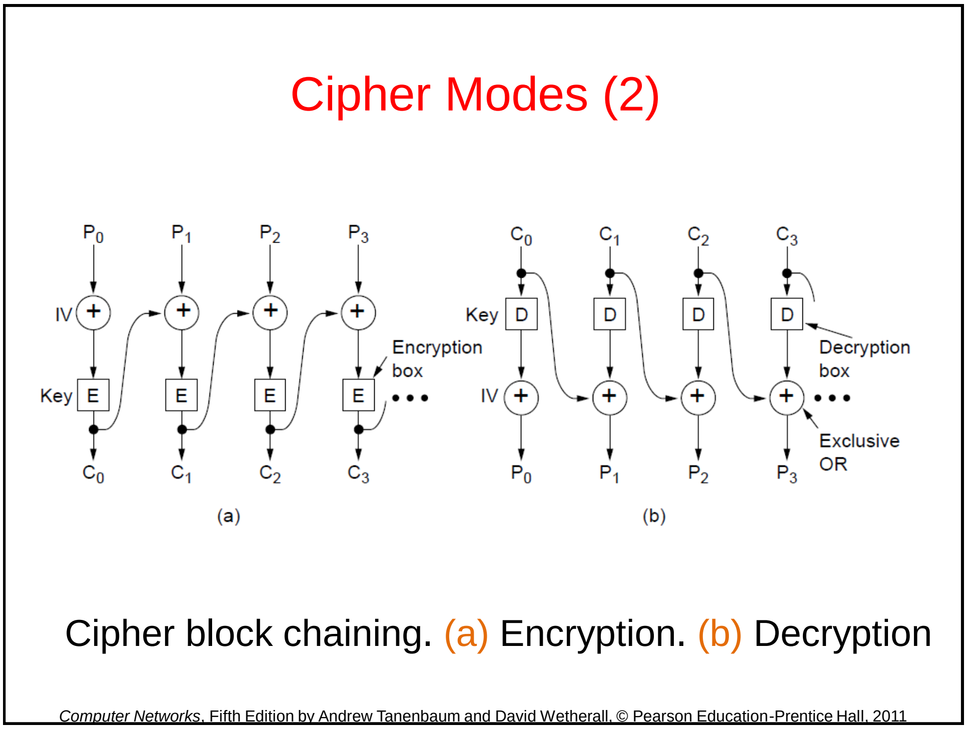
Cipher Modes (1)



Name	Position	Bonus
Adams, Leslie	Clerk	$10
Black, Robin	Boss	$500,000
Collins, Kim	Manager	$100,000
Davis, Bobbie	Janitor	$5

The plaintext of a file encrypted as 16 DES blocks.

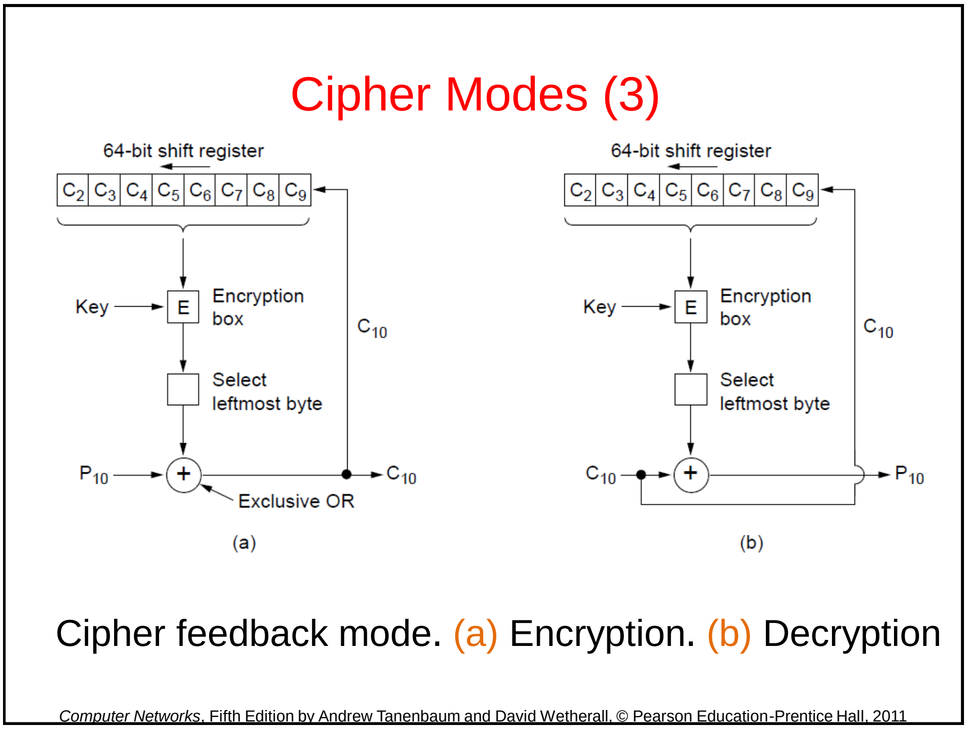
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011



Cipher Modes (2)

Cipher block chaining. (a) Encryption. (b) Decryption

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

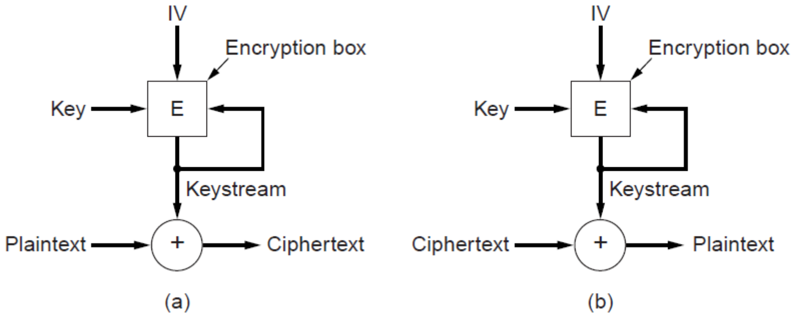


Cipher Modes (3)

Cipher feedback mode. (a) Encryption. (b) Decryption

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

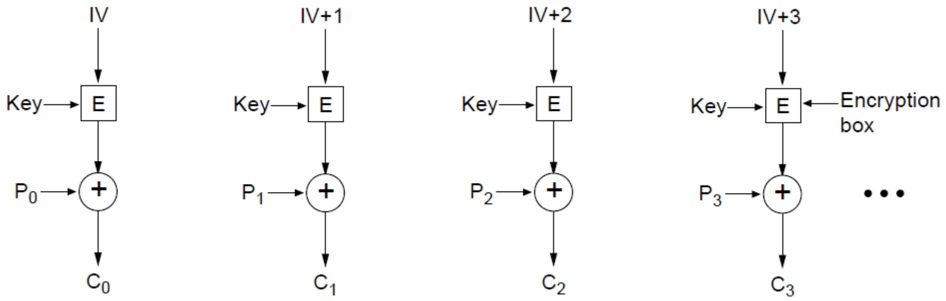
Cipher Modes (4)



A stream cipher. (a) Encryption. (b) Decryption

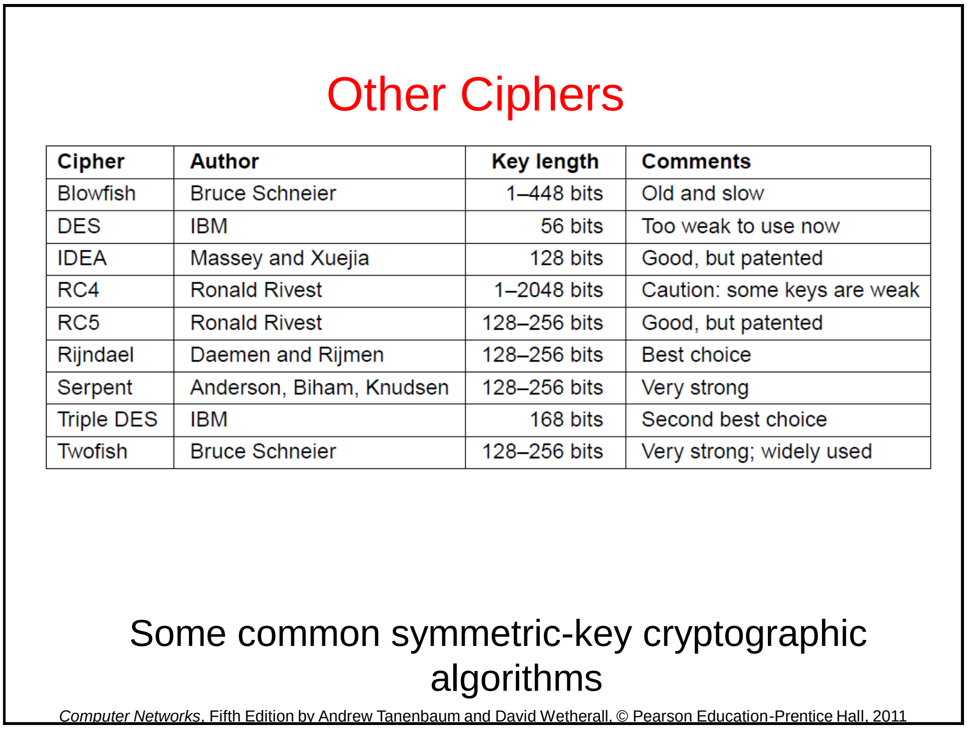
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Cipher Modes (5)



Encryption using counter mode

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

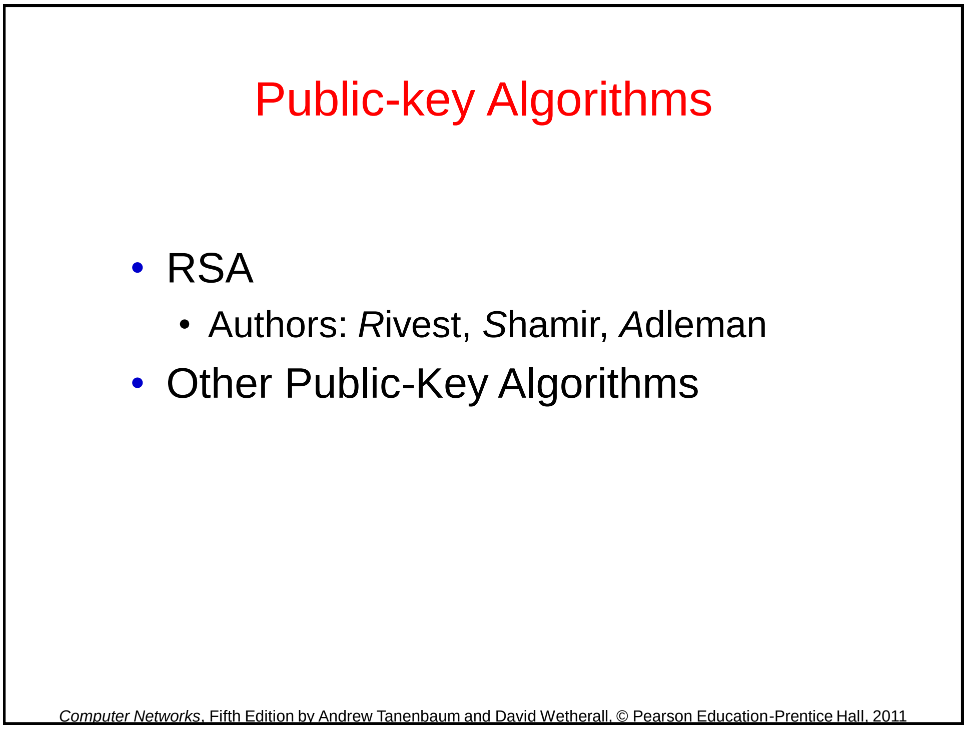


Other Ciphers

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Some common symmetric-key cryptographic algorithms

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



Public-key Algorithms

- RSA
  - Authors: *R*ivest, *S*hamir, *A*dleman
- Other Public-Key Algorithms

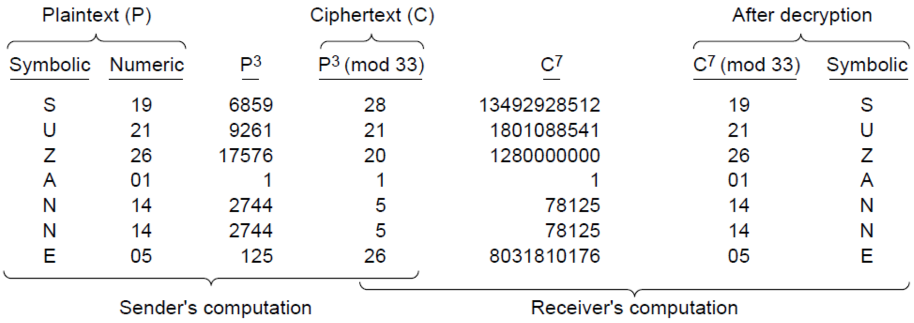
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

RSA (1)

Method Summary

1. Choose two large primes, *p* and *q*
2. Compute
   $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
3. Choose number relatively prime to *z* call it *d.*
4. Find *e* such that $e \times d = 1 \bmod z$.

RSA (2)

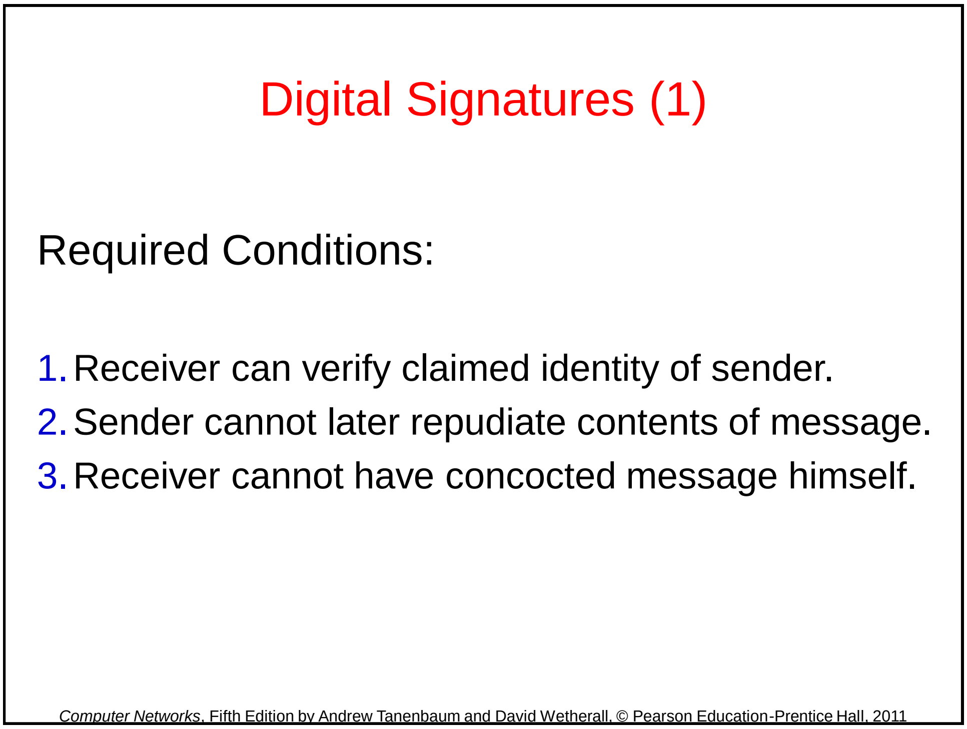


Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

Receiver's computation

An example of the RSA algorithm

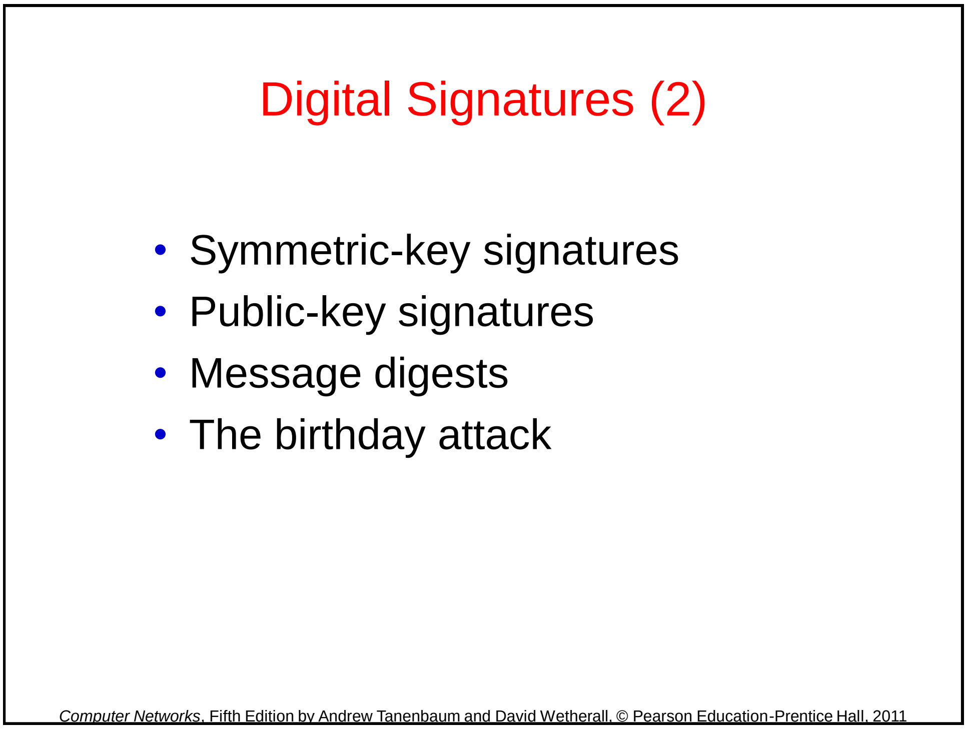


Digital Signatures (1)

Required Conditions:

1. Receiver can verify claimed identity of sender.
2. Sender cannot later repudiate contents of message.
3. Receiver cannot have concocted message himself.

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

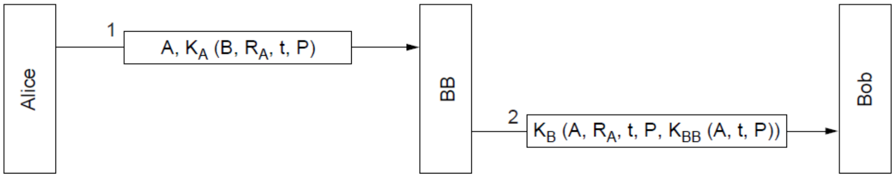


Digital Signatures (2)

- Symmetric-key signatures
- Public-key signatures
- Message digests
- The birthday attack

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

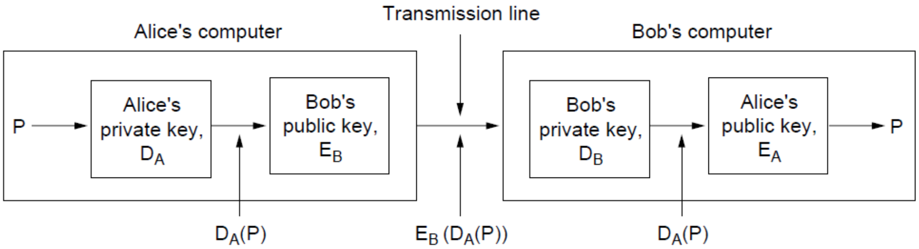
Symmetric-key Signatures


Alice
1
A, K_A (B, R_A, t, P)
BB
2
K_B (A, R_A, t, P, K_{BB} (A, t, P))
Bob

Digital signatures with Big Brother

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

Public-Key Signatures (1)



Digital signatures using public-key cryptography.

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

Public-Key Signatures (2)

Criticisms of DSS:

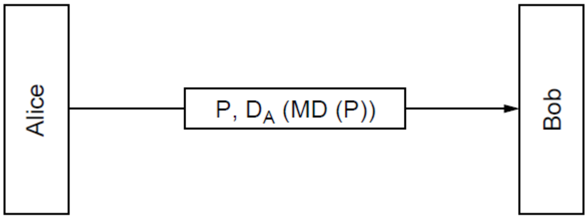
1. Too secret
2. Too slow
3. Too new
4. Too insecure

Message Digests (1)

Message Digest properties

1. Given *P*, easy to compute *MD(P).*
2. Given *MD(P),* effectively impossible to find *P.*
3. Given *P* no one can find *P′* such that *MD(P′) = MD(P).*
4. Change to input of even 1 bit produces very different output.

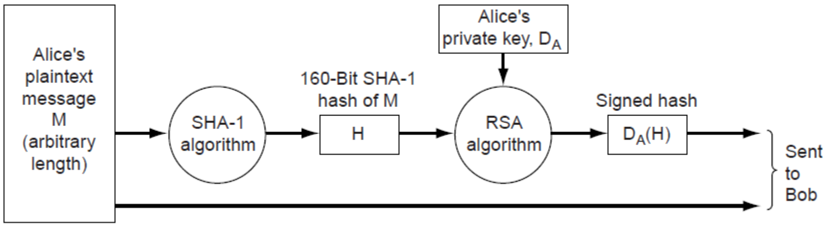
Message Digests (2)



Digital signatures using message digests

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

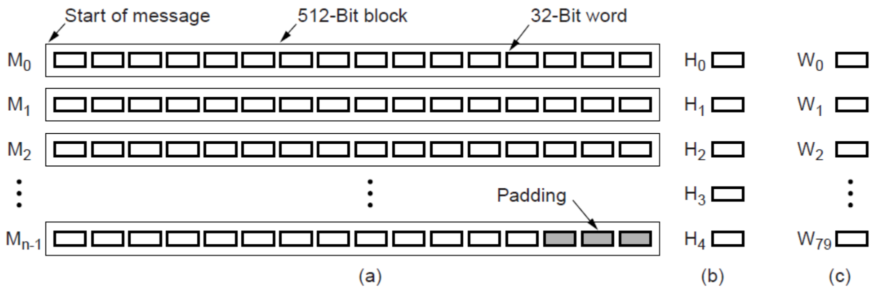
Message Digests (3)



Use of SHA-1 and RSA for signing nonsecret messages

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

Message Digests (4)



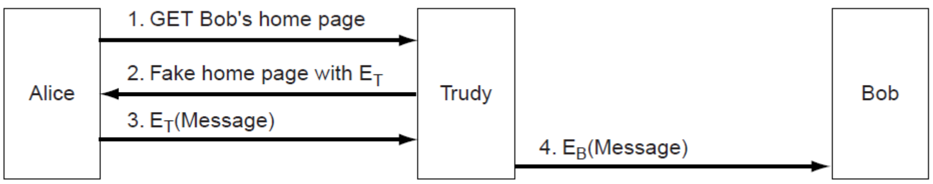
(a)A message padded out to a multiple of 512 bits.

(b)The output variables.

(c)The word array.

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

Management of Public Keys (1)



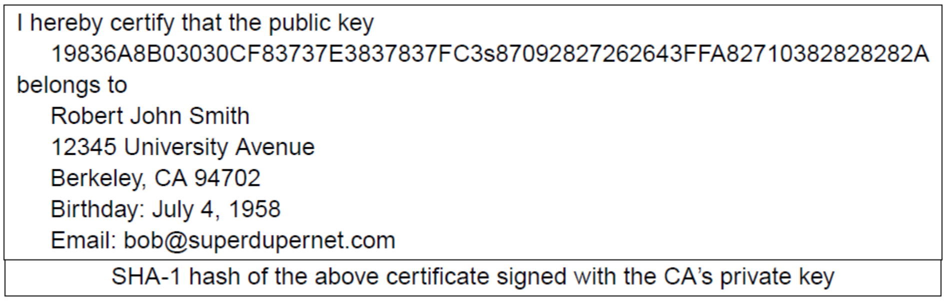
A way for Trudy to subvert public-key encryption

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

Management of Public Keys (2)

- Certificates
- X.509
- Public key infrastructures

Certificates



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

A possible certificate and its signed hash

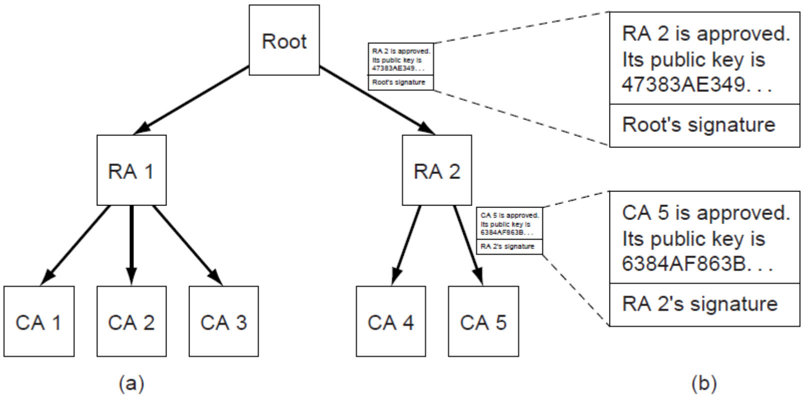
X.509

Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The entity whose key is being certified
Public key	The subject's public key and the ID of the algorithm using it
Issuer ID	An optional ID uniquely identifying the certificate's issuer
Subject ID	An optional ID uniquely identifying the certificate's subject
Extensions	Many extensions have been defined
Signature	The certificate's signature (signed by the CA's private key)

The basic fields of an X.509 certificate

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

Public Key Infrastructures


Root
RA 1
RA 2
CA 1
CA 2
CA 3
CA 4
CA 5
RA 2 is approved. Its public key is 47383AE349. . .
Root's signature
CA 5 is approved. Its public key is 6384AF863B. . .
RA 2's signature
(a)
(b)

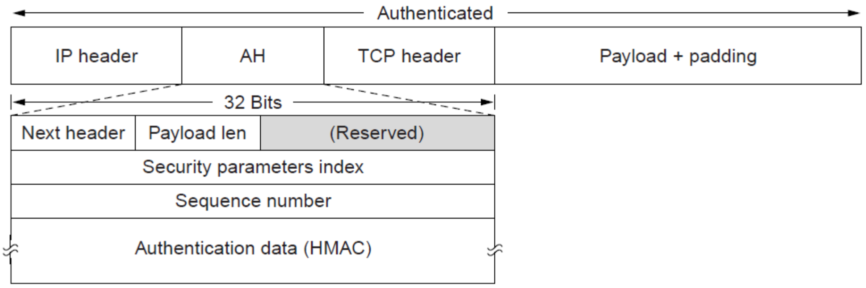
(a) A hierarchical PKI. (b) A chain of certificates.

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

Communication Security

- IPsec
- Firewalls
- Virtual private networks
- Wireless security

IPsec (1)



Authenticated

IP header | AH | TCP header | Payload + padding

32 Bits

Next header | Payload len | (Reserved)

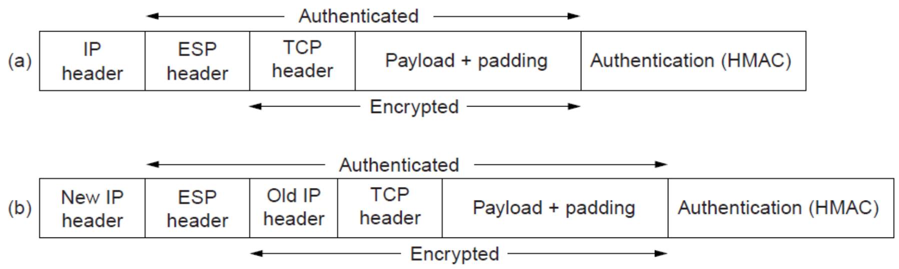
Security parameters index

Sequence number

Authentication data (HMAC)

The IPsec authentication header in transport mode for IPv4.

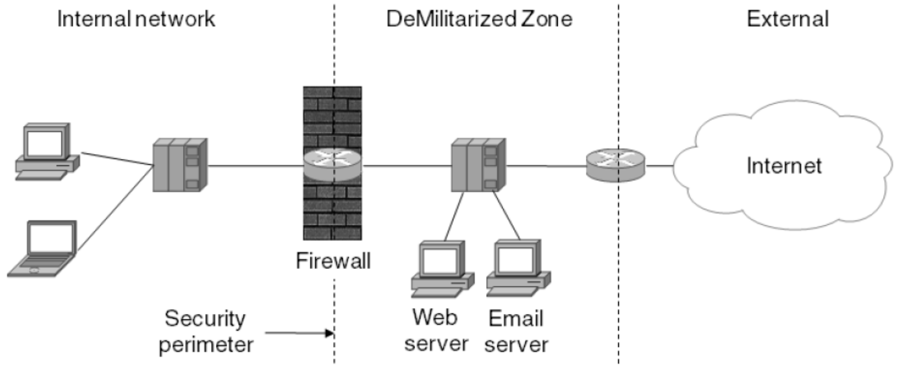
IPsec (2)



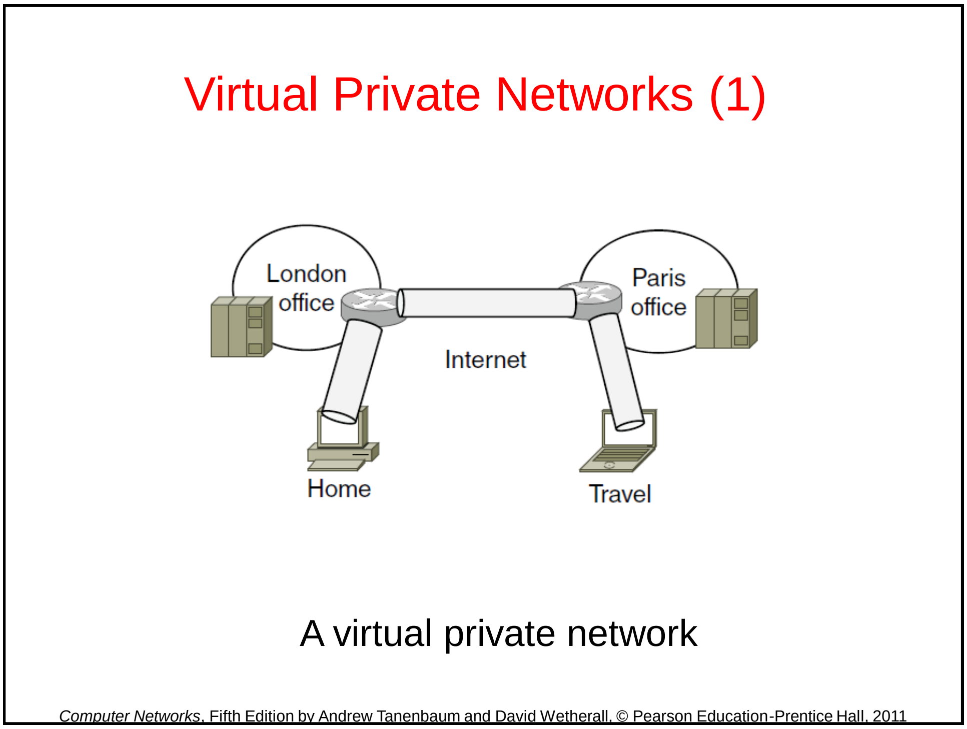
(a) ESP in transport mode. (b) ESP in tunnel mode.

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

IPsec (3)



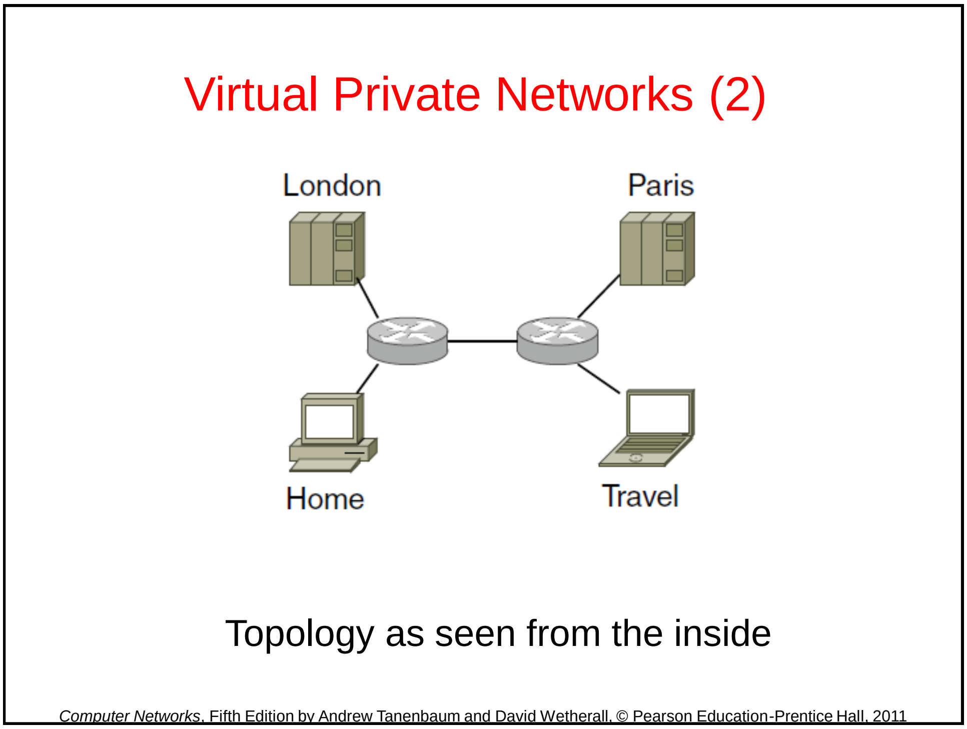
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011



Virtual Private Networks (1)

A virtual private network

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

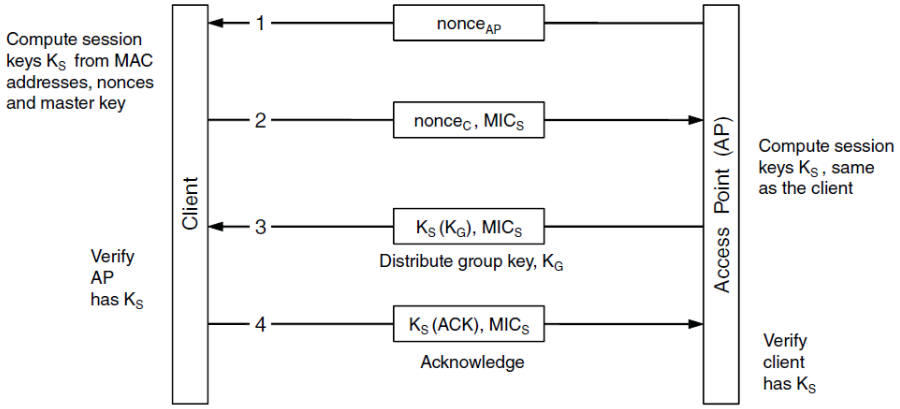


Virtual Private Networks (2)

Topology as seen from the inside

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

Wireless Security



Client

Access Point (AP)

Compute session keys K_S from MAC addresses, nonces and master key

1 nonce$_{AP}$

2 nonce$_C$, MIC$_S$

Compute session keys K_S, same as the client

3 K_S (K_G), MIC$_S$

Distribute group key, K_G

Verify AP has K_S

4 K_S (ACK), MIC$_S$

Acknowledge

Verify client has K_S

The 802.11i key setup handshake

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

Authentication Protocols

- Shared secret key
- Establishing a shared key:
  the Diffie-Hellman key exchange
- Key distribution center
- Kerberos
- Public-key cryptography

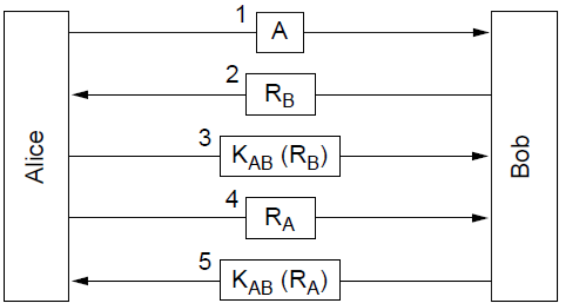
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Shared Secret Key (1)

Notation for discussing protocols

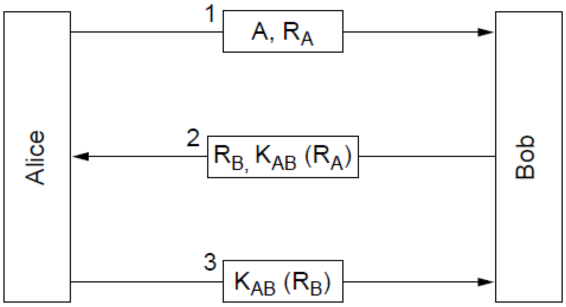
- *A, B* are the identities of Alice and Bob*.*
- R_i*'s* are the challenges, where the subscript identifies the challenger*.*
- K_i are keys, where *i* indicates the owner.
- K_S is the session key.

Shared Secret Key (2)



Two-way authentication using a challenge-response protocol.

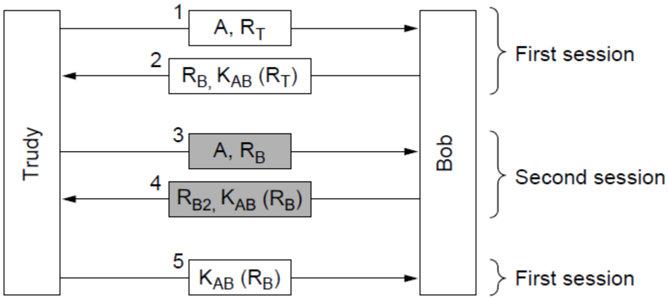
Shared Secret Key (3)



A shortened two-way authentication protocol

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

Shared Secret Key (4)



The reflection attack.

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

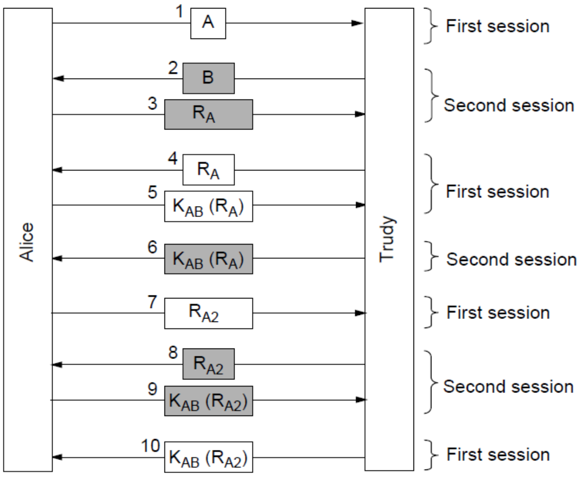
Shared Secret Key (5)

General design rules

1. Have initiator prove who she is before responder
2. Initiator, responder use different keys
3. Draw challenges from different sets
4. Make protocol resistant to attacks involving second parallel session

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

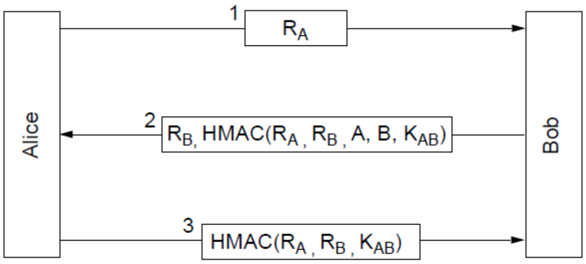
Shared Secret Key (6)



A reflection attack on the protocol of Fig. 8-32

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

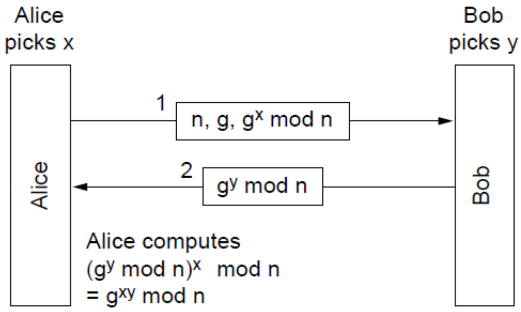
Shared Secret Key (7)


Alice
Bob
1
R_A
2
R_B, HMAC(R_A, R_B, A, B, K_{AB})
3
HMAC(R_A, R_B, K_{AB})

Authentication using HMACs

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

The Diffie-Hellman Key Exchange (1)



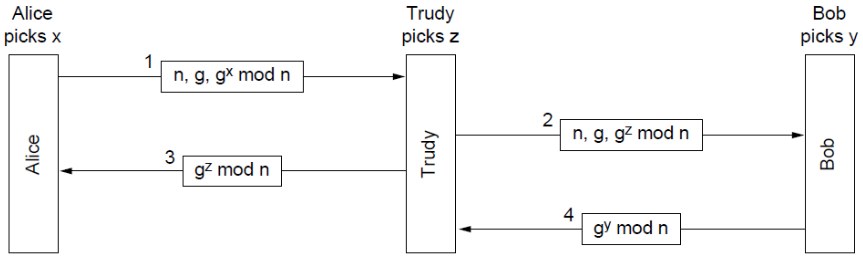
Alice computes
$(g^y \bmod n)^x \bmod n$
$= g^{xy} \bmod n$

Bob computes
$(g^x \bmod n)^y \bmod n$
$= g^{xy} \bmod n$

The Diffie-Hellman key exchange

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

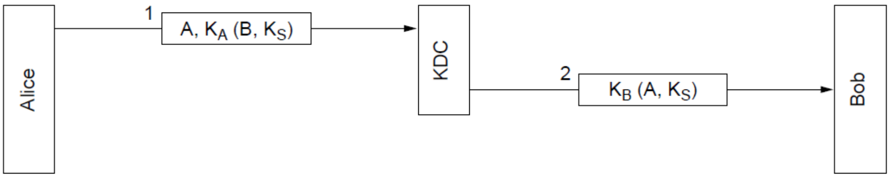
The Diffie-Hellman Key Exchange (2)



The man-in-the-middle attack

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

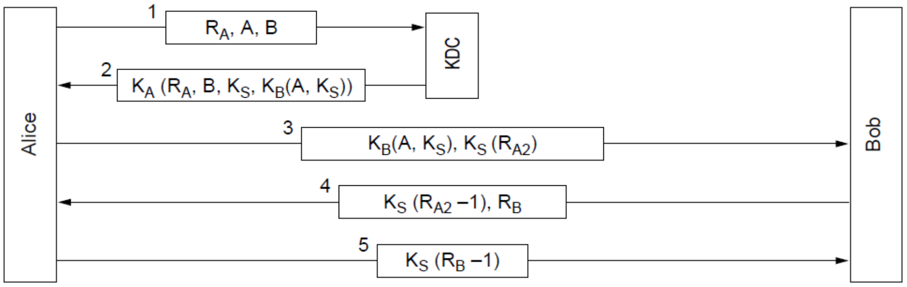
Key Distribution Center (1)



A first attempt at an authentication protocol using a KDC.

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

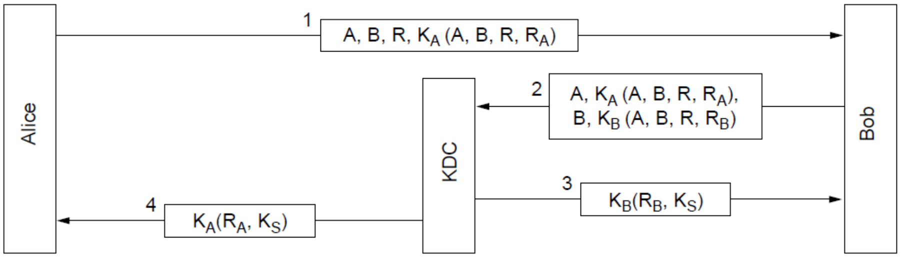
Key Distribution Center (2)


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)

The Needham-Schroeder authentication protocol

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

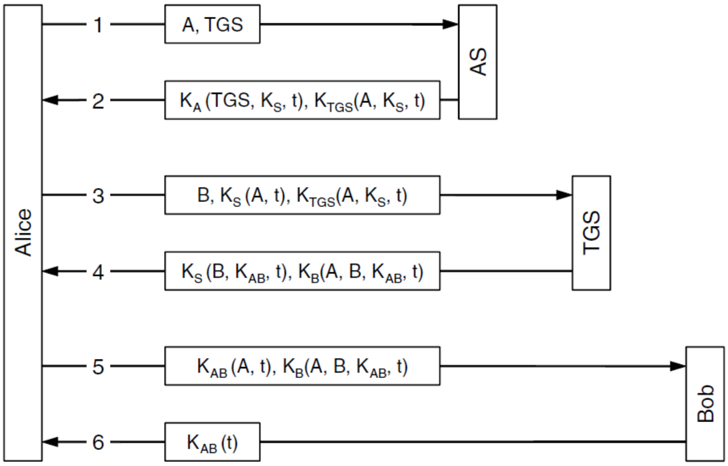
Key Distribution Center (3)


Alice
KDC
Bob
1 A, B, R, K_A (A, B, R, R_A)
2 A, K_A (A, B, R, R_A), B, K_B (A, B, R, R_B)
3 K_B(R_B, K_S)
4 K_A(R_A, K_S)

The Otway-Rees authentication protocol (slightly simplified).

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

Kerberos



Alice

AS

TGS

Bob

1 A, TGS

2 K_A (TGS, K_S, t), K_{TGS}(A, K_S, t)

3 B, K_S (A, t), K_{TGS}(A, K_S, t)

4 K_S (B, K_{AB}, t), K_B(A, B, K_{AB}, t)

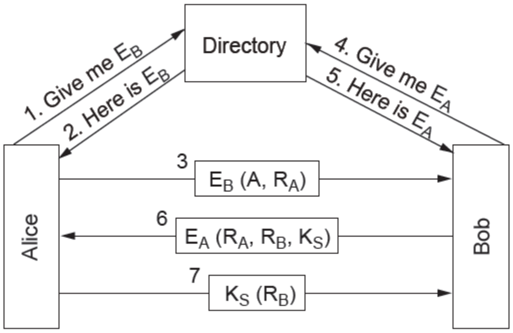
5 K_{AB} (A, t), K_B(A, B, K_{AB}, t)

6 K_{AB} (t)

The operation of Kerberos V5

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

Public-Key Cryptography



Directory

Alice

Bob

1. Give me E_B

2. Here is E_B

4. Give me E_A

5. Here is E_A

3 E_B (A, R_A)

6 E_A (R_A, R_B, K_S)

7 K_S (R_B)

Mutual authentication using public-key cryptography

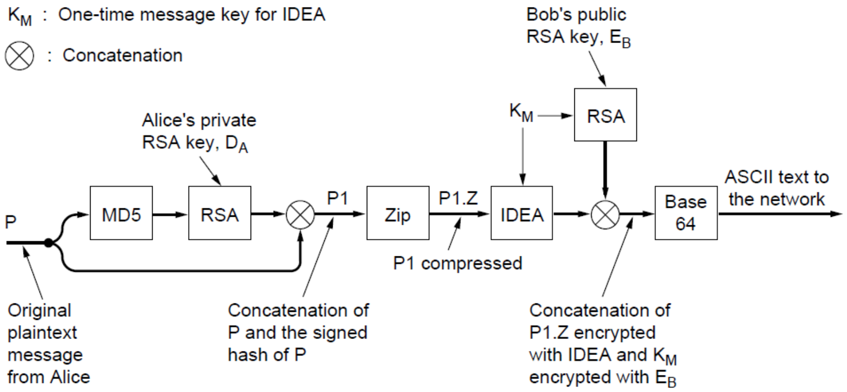
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Email Security

- PGP—Pretty Good Privacy
- S/MIME

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

PGP—Pretty Good Privacy (1)


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
P
MD5
RSA
P1
Zip
P1.Z
IDEA
Base 64
ASCII text to the network
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

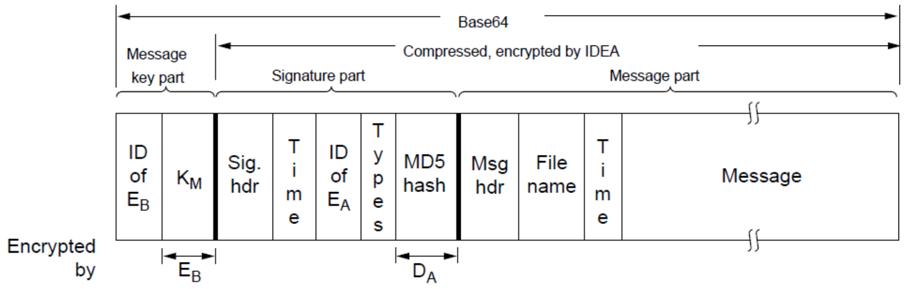
PGP in operation for sending a message

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

PGP—Pretty Good Privacy (2)

- Casual (384 bits):
  - Can be broken easily today.
- Commercial (512 bits): b
  - Breakable by three-letter organizations.
- Military (1024 bits):
  - Not breakable by anyone on earth.
- Alien (2048 bits):
  - Unbreakable by anyone on other planets

PGP—Pretty Good Privacy (3)

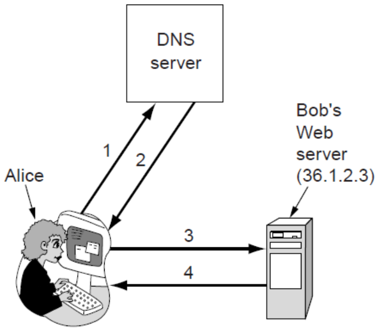


A PGP message

Web Security

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

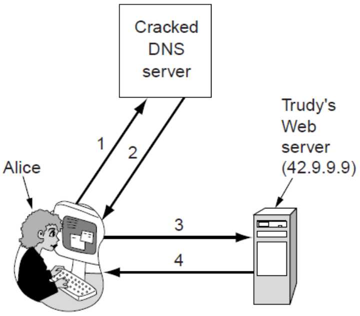
Secure Naming (1)



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)

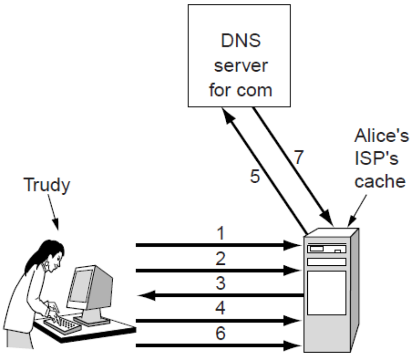


1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page

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

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

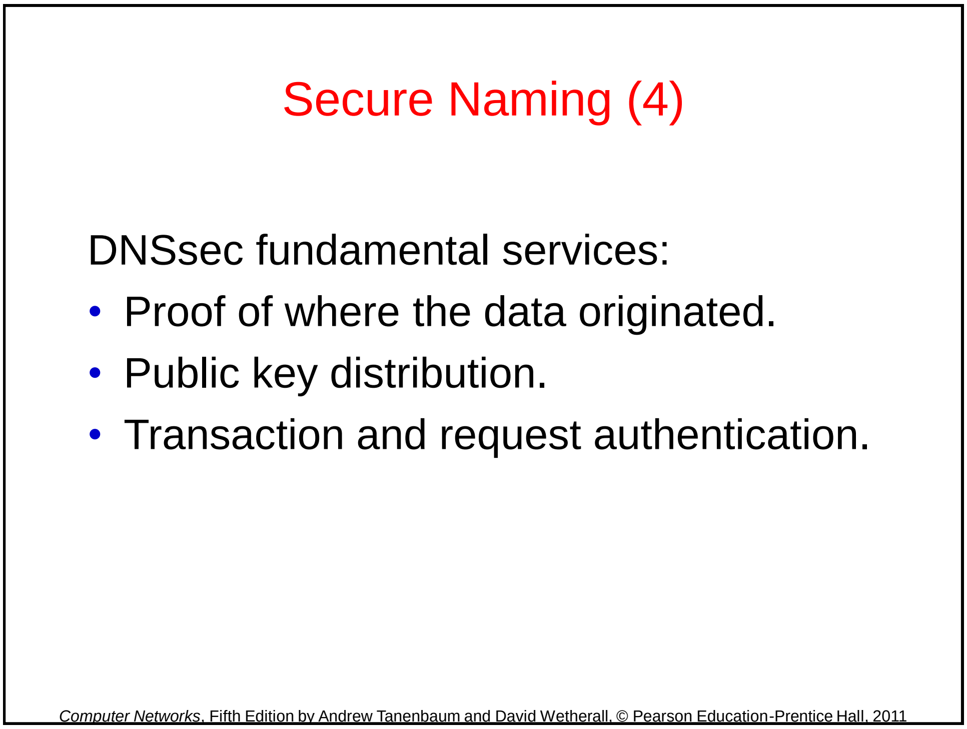
Secure Naming (3)



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.

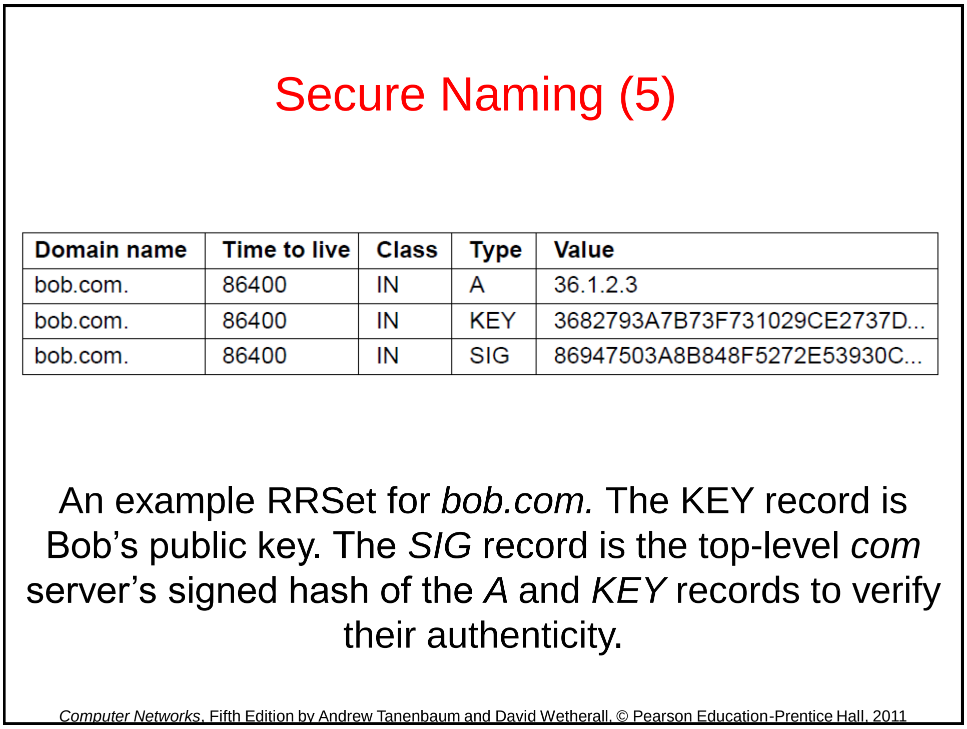
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011



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.

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

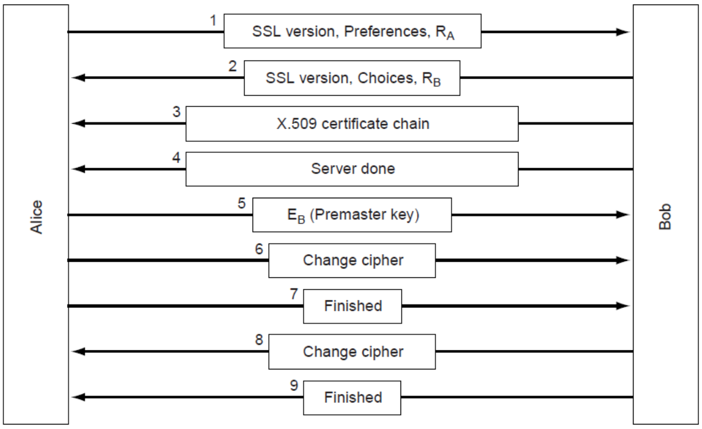
SSL—The Secure Sockets Layer (2)

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.

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

SSL—The Secure Sockets Layer (3)



Alice

Bob

1 SSL version, Preferences, R_A

2 SSL version, Choices, R_B

3 X.509 certificate chain

4 Server done

5 E_B (Premaster key)

6 Change cipher

7 Finished

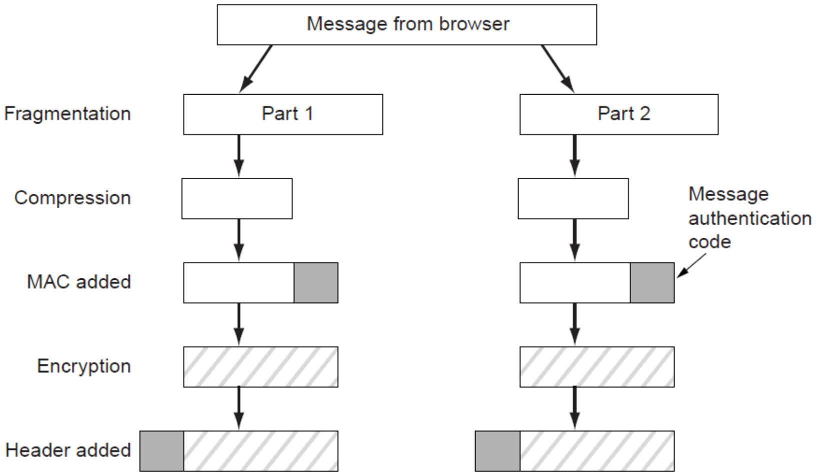
8 Change cipher

9 Finished

A simplified version of the SSL connection establishment subprotocol.

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

SSL—The Secure Sockets Layer (4)



Message from browser

Fragmentation

Part 1

Part 2

Compression

Message authentication code

MAC added

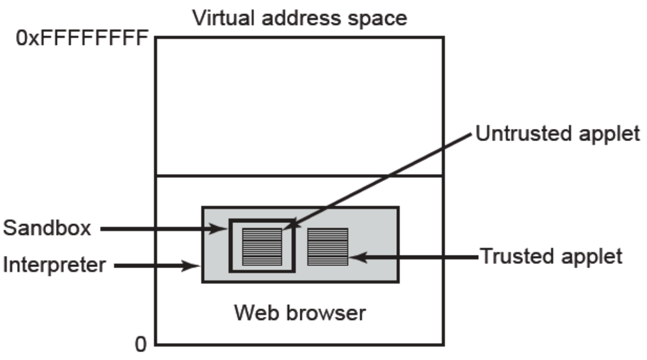
Encryption

Header added

Data transmission using SSL

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

Mobile Code Security



Applets can be interpreted by a Web browser

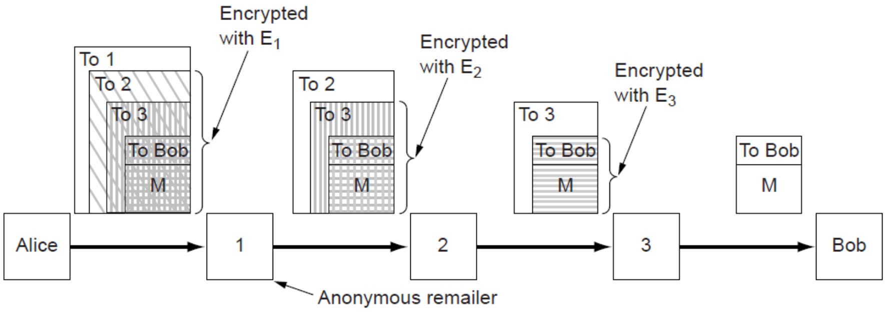
Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

Social Issues

- Privacy
- Freedom of speech
- Copyright

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

Privacy



How Alice uses 3 remailers to send Bob a message

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

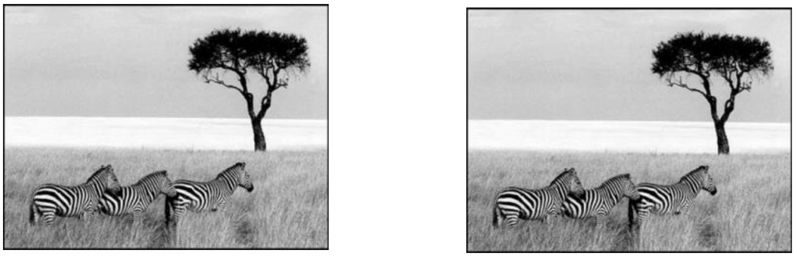
Freedom of Speech (1)

Possible banned material:

- Inappropriate for children
- Hate aimed at various groups
- Information about democracy
- History that contradicts government position
- Manuals for potentially illegal activities

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

Freedom of Speech (2)



(a)

(b)

(a) Three zebras and a tree.

(b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.

End

Chapter 8