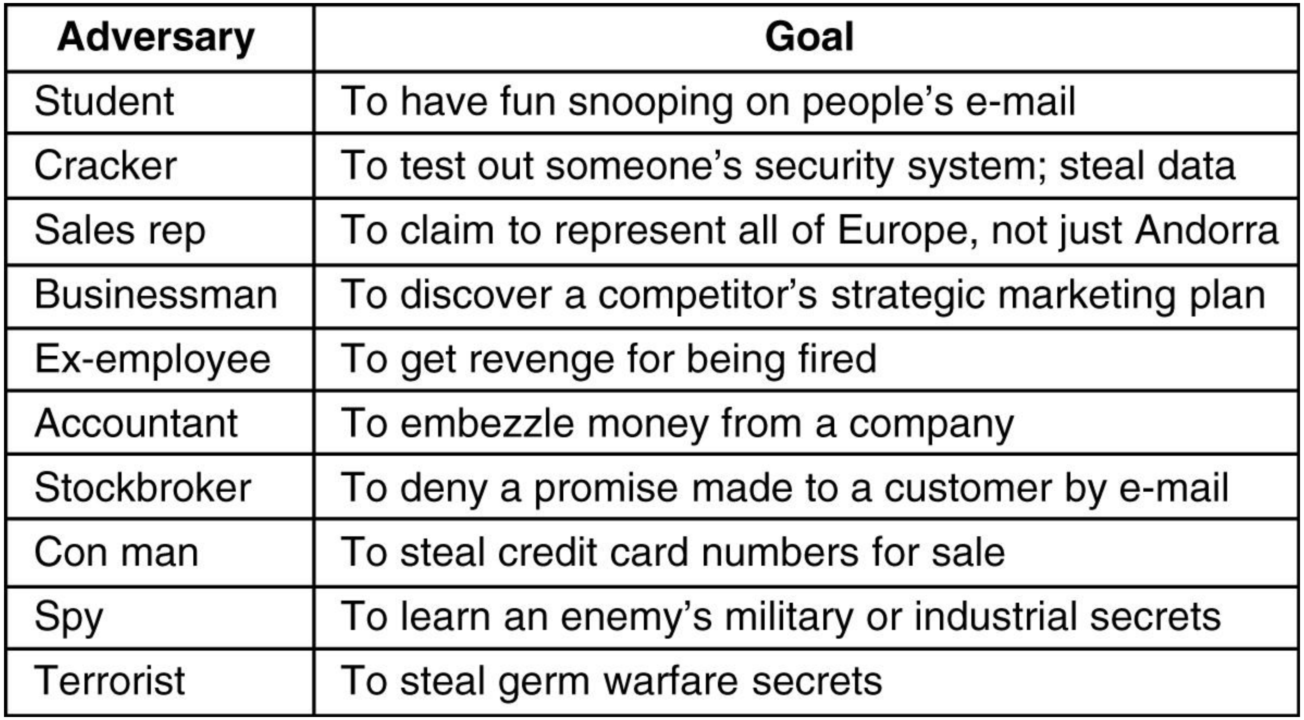
Chapter 8

Network Security

Cryptography

- Introduction to Cryptography
- Substitution Ciphers
- Transposition Ciphers
- One-Time Pads
- Two Fundamental Cryptographic Principles

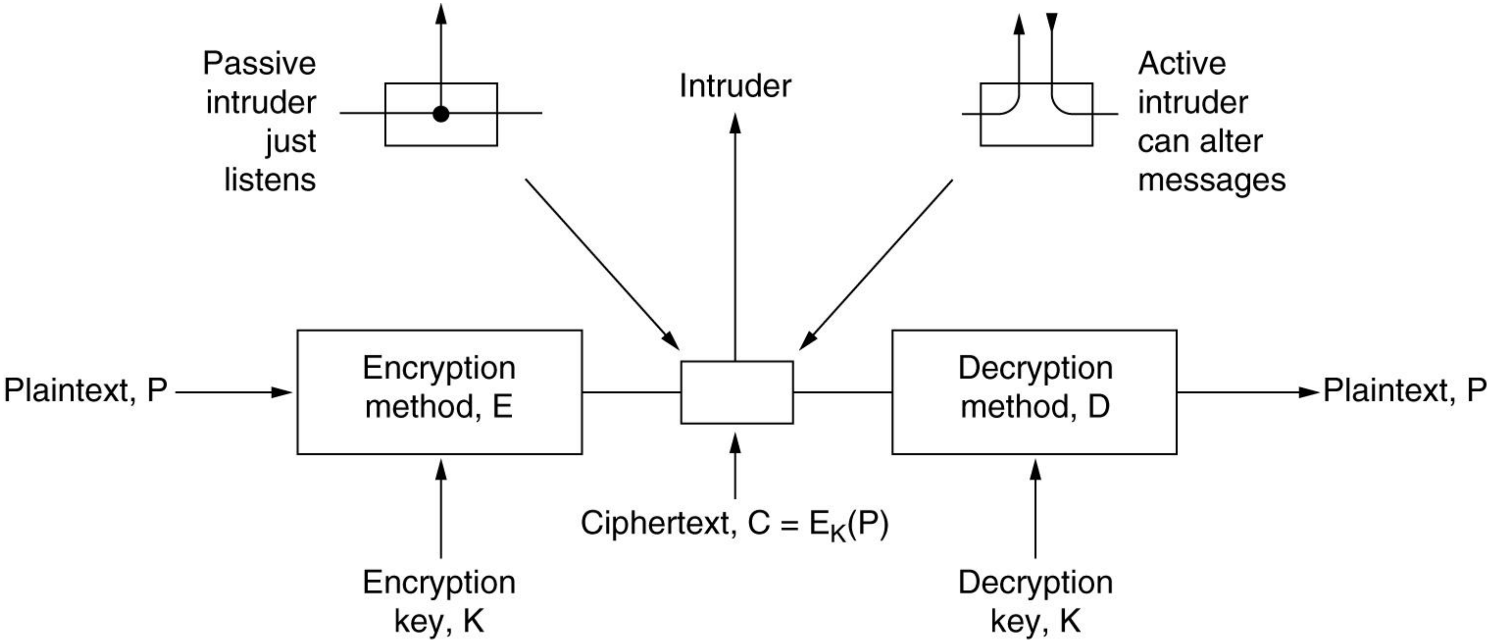
Need for Security



Adversary	Goal
Student	To have fun snooping on people's e-mail
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 e-mail
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

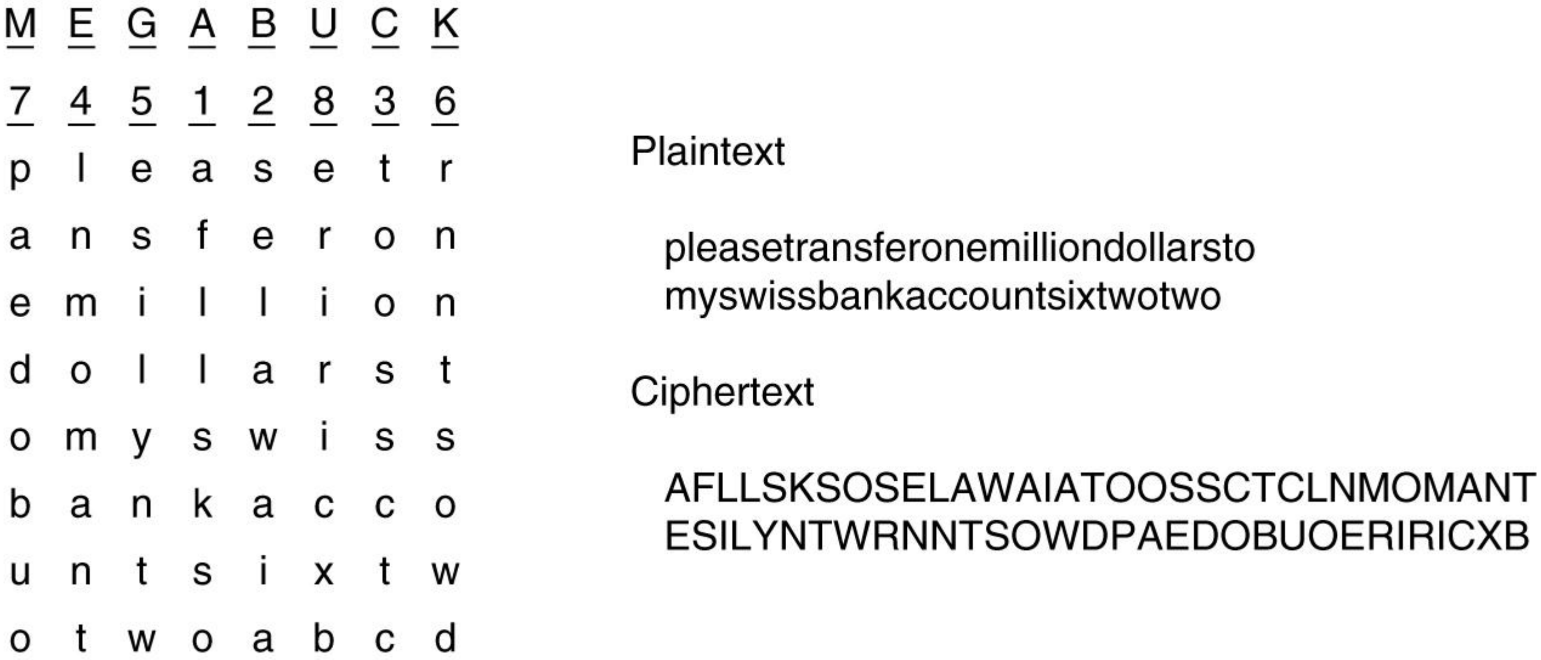
Some people who cause security problems and why.

An Introduction to Cryptography



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

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

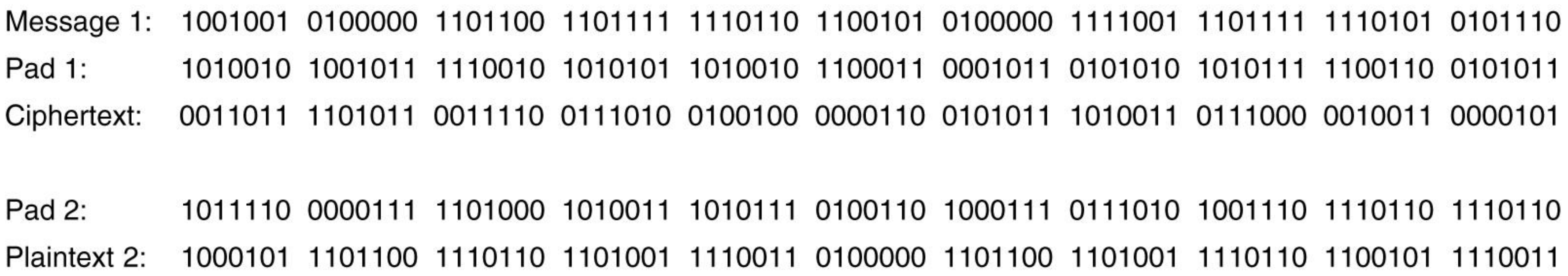
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

A transposition cipher.

One-Time Pads



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.

Quantum Cryptography

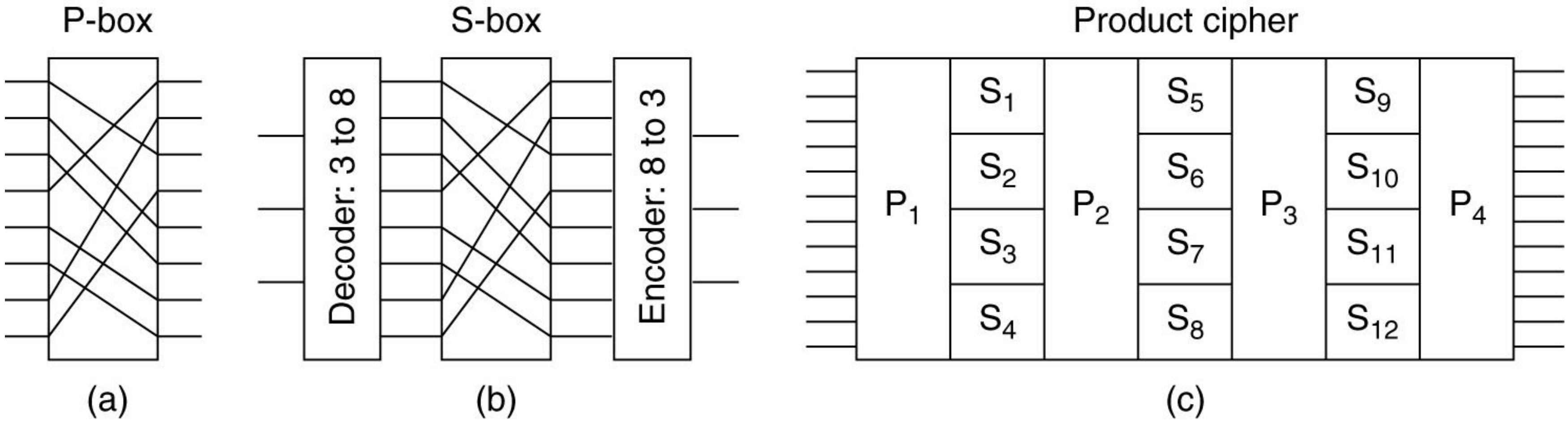
Bit number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Data	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1	0	
(a)	⤡	↕	↕	⤡	↔	⤡	⤢	⤢	↔	↕	↔	⤢	⤢	↔	↔	↕	What Alice sends
(b)	✛	✛	✕	✕	✕	✛	✛	✕	✛	✕	✛	✕	✕	✕	✛	✕	Bob's bases
(c)	↕	↕	⤢	⤡	⤡	↕	↔	⤢	↔	⤢	↔	⤢	⤢	⤡	↔	⤢	What Bob gets
(d)	No	Yes	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Correct 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.

Symmetric-Key Algorithms

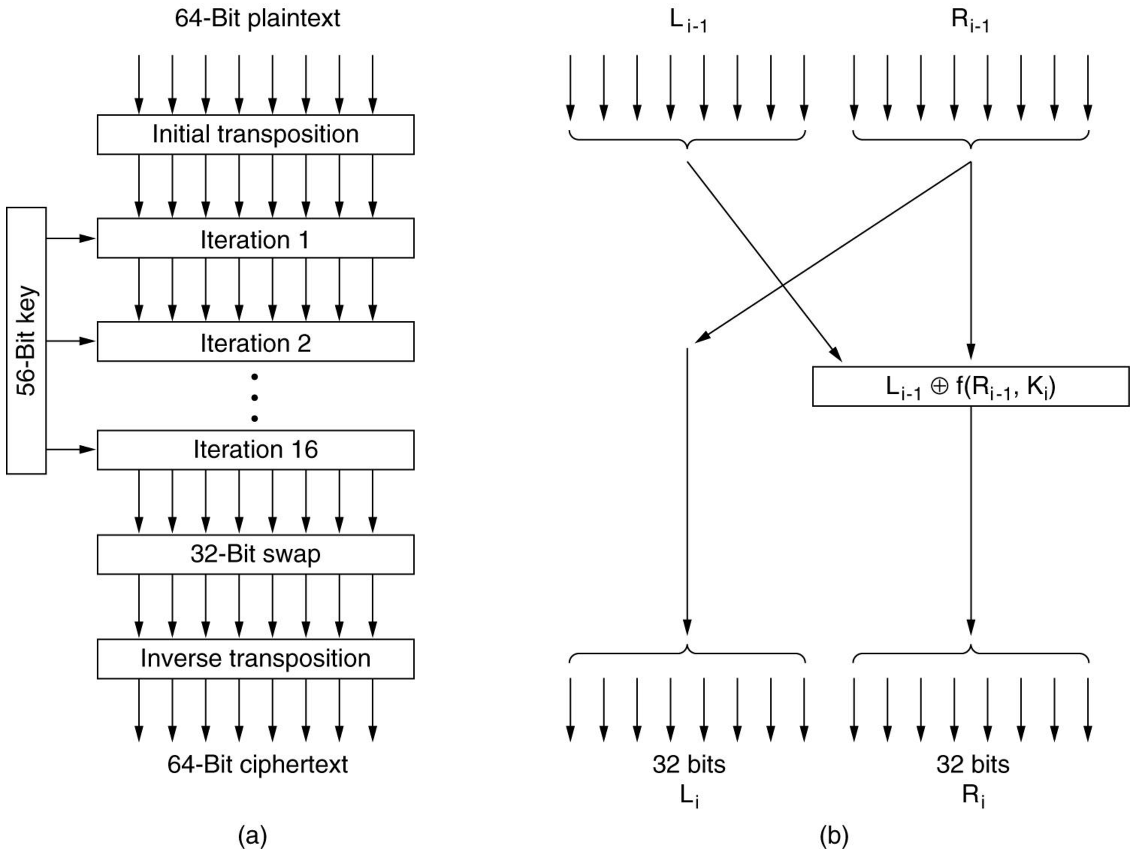
- DES – The Data Encryption Standard
- AES – The Advanced Encryption Standard
- Cipher Modes
- Other Ciphers
- Cryptanalysis

Product Ciphers



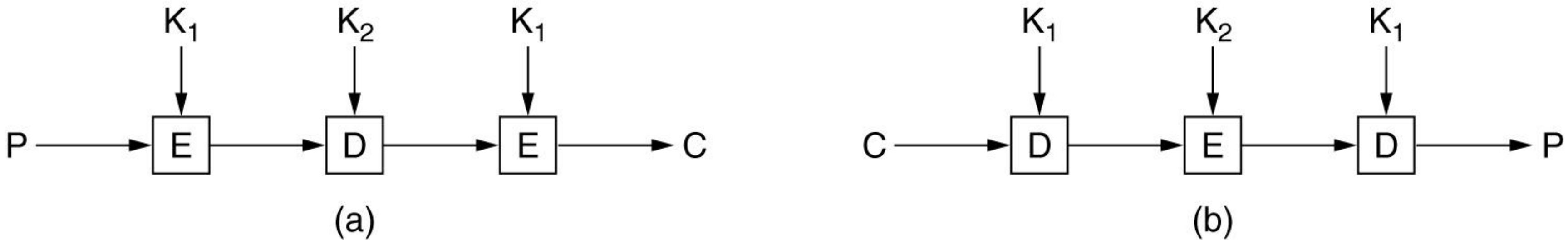
Basic elements of product ciphers. (a) P-box. (b) S-box. (c) Product.

Data Encryption Standard



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

Triple DES



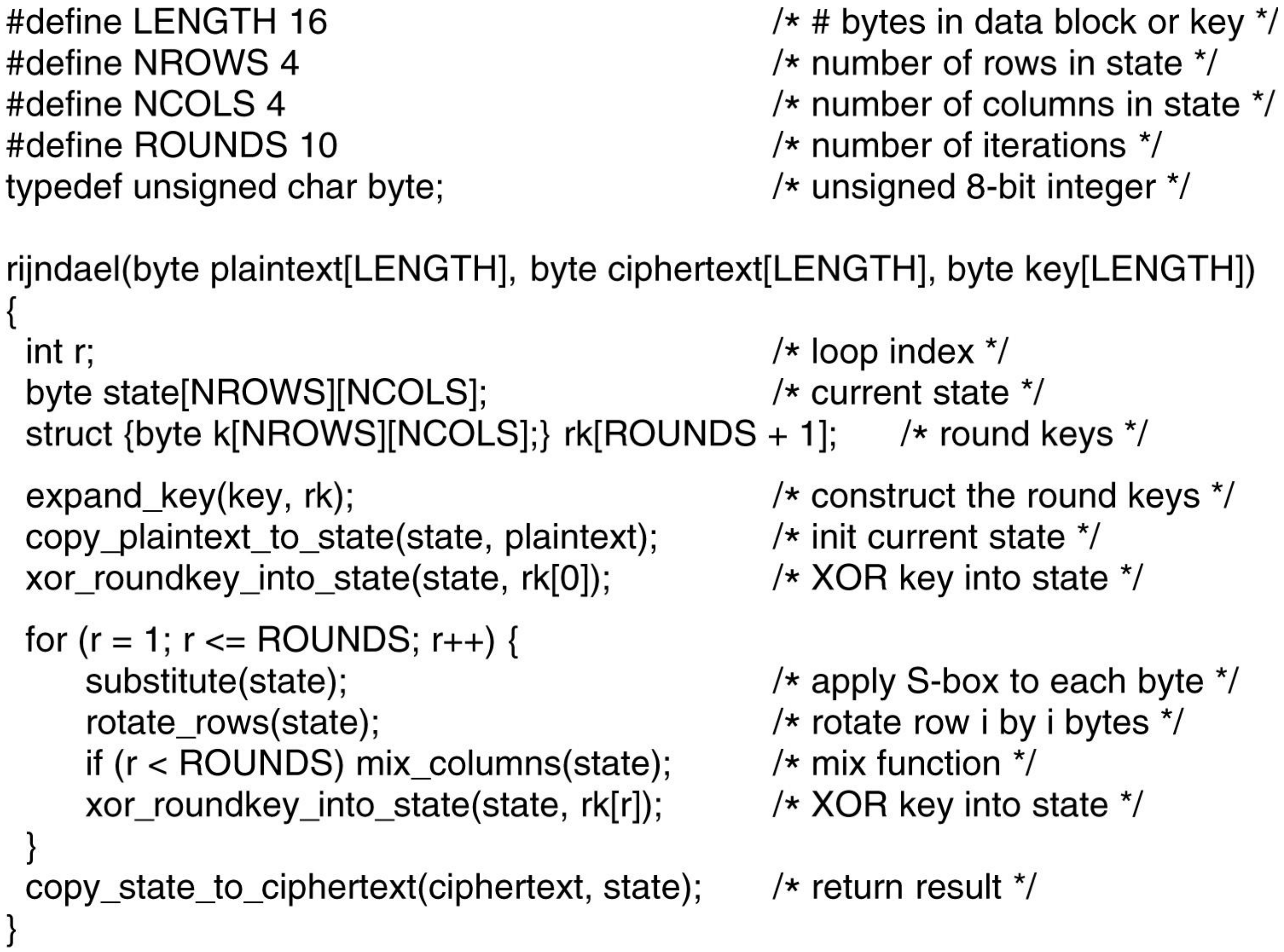
(a) Triple encryption using DES. (b) Decryption.

AES – The Advanced Encryption Standard

Rules for AES proposals

1. The algorithm must be a symmetric block cipher.
2. The full design must be public.
3. Key lengths of 128, 192, and 256 bits supported.
4. Both software and hardware implementations required
5. The algorithm must be public or licensed on nondiscriminatory terms.

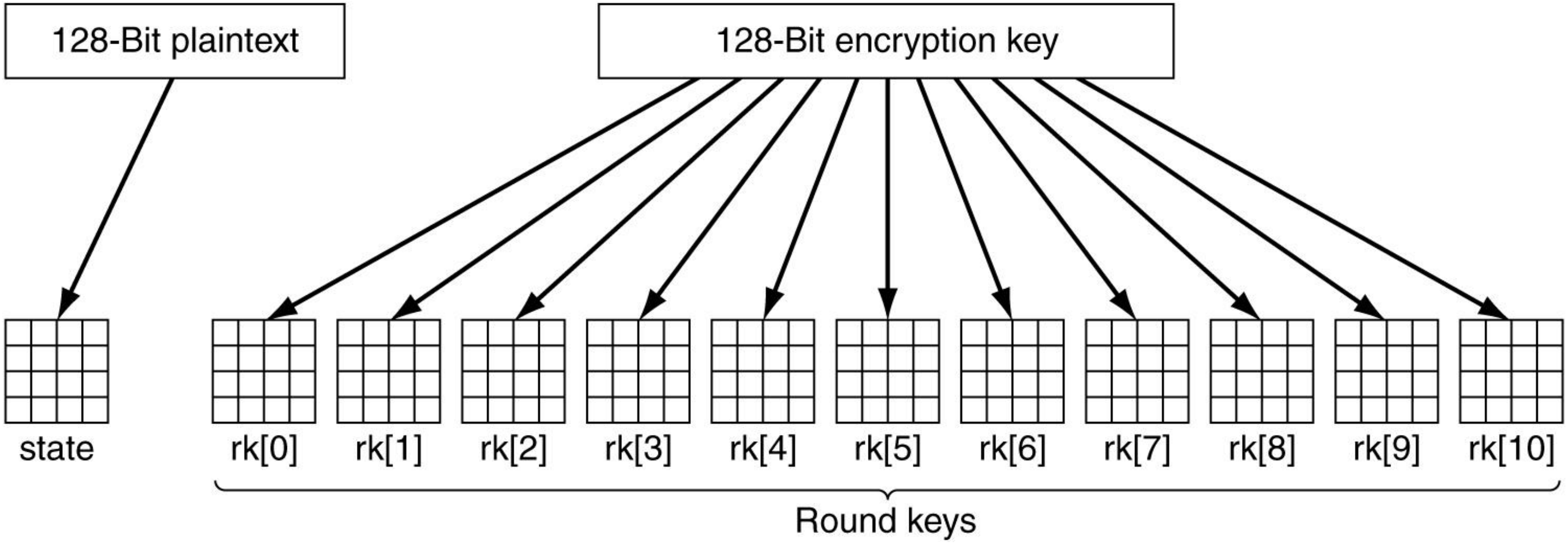
AES (2)



```
#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 */

  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 */
}
```

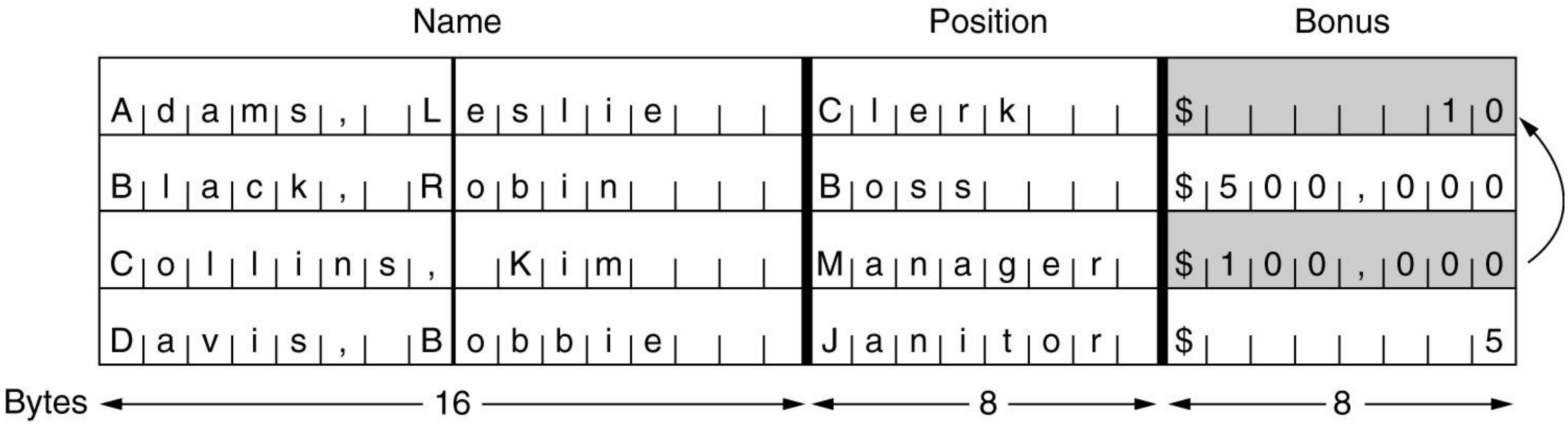
An outline of Rijndael.

AES (3)



Creating of the *state* and *rk* arrays.

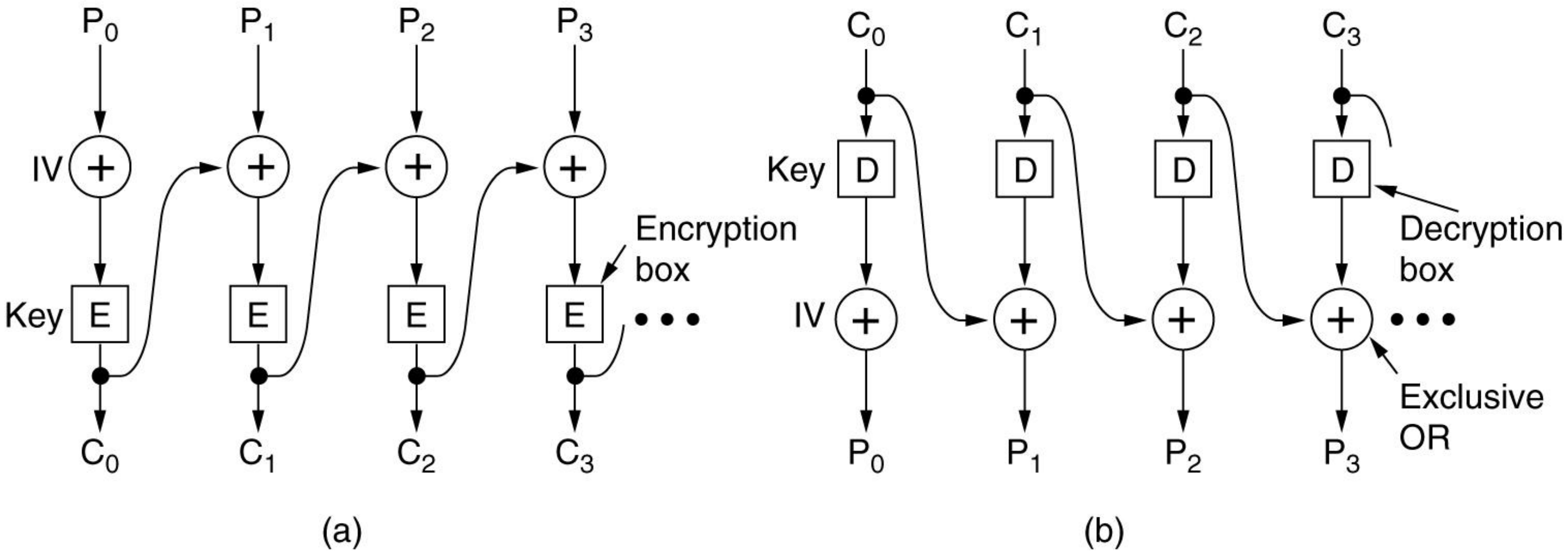
Electronic Code Book Mode



	Name	Position	Bonus
	Adams, Leslie	Clerk	$10
	Black, Robin	Boss	$500,000
	Collins, Kim	Manager	$100,000
	Davis, Bobbie	Janitor	$5
Bytes	16	8	8

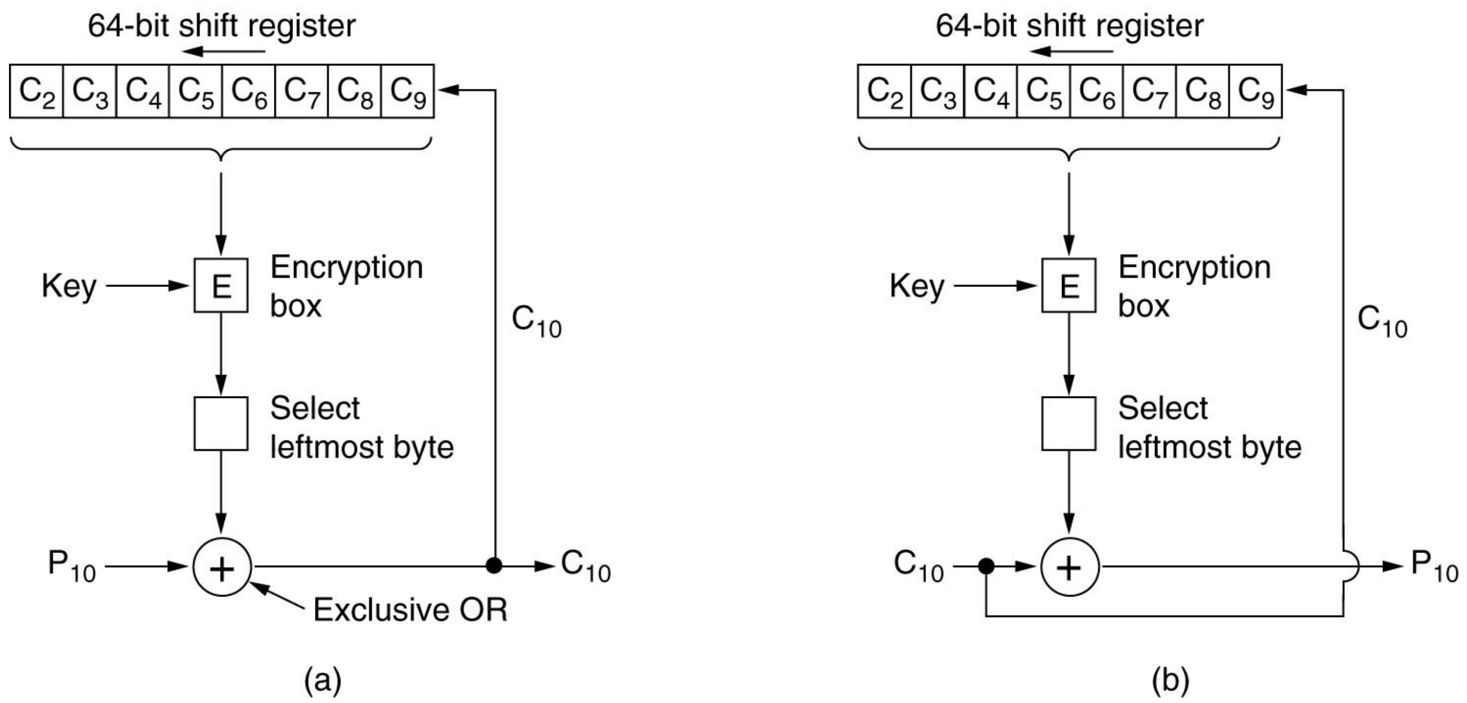
The plaintext of a file encrypted as 16 DES blocks.

Cipher Block Chaining Mode



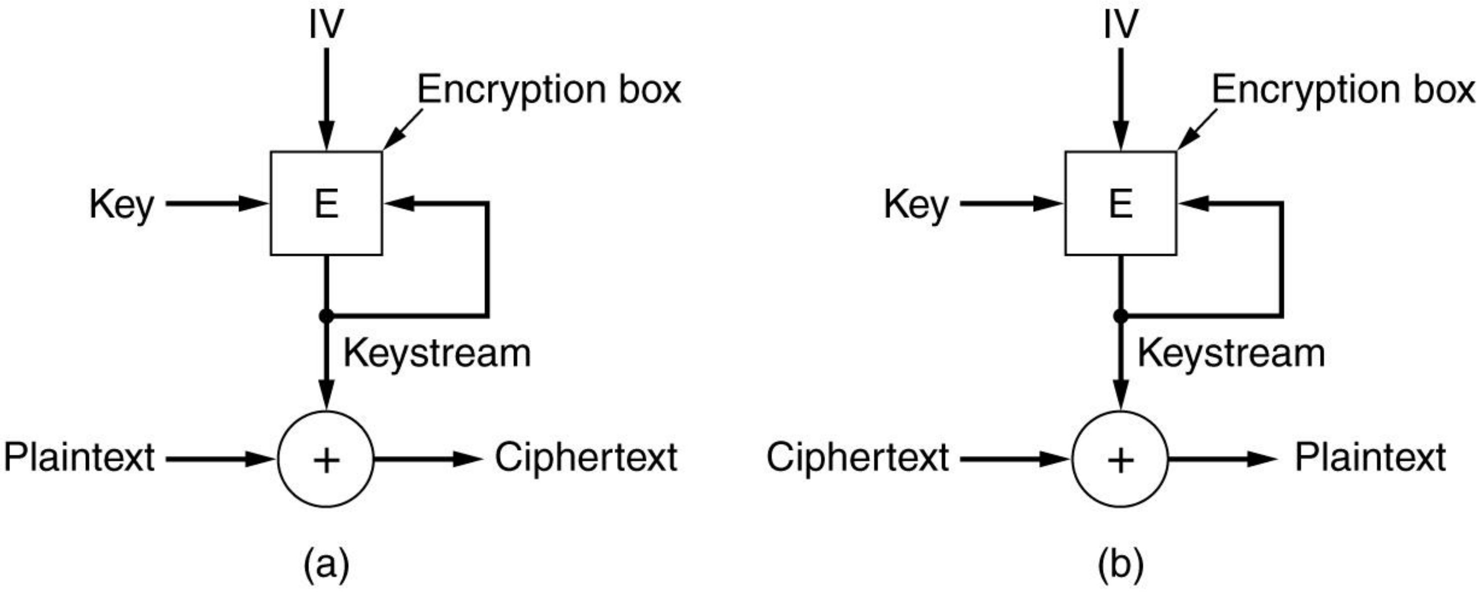
Cipher block chaining. (a) Encryption. (b) Decryption.

Cipher Feedback Mode



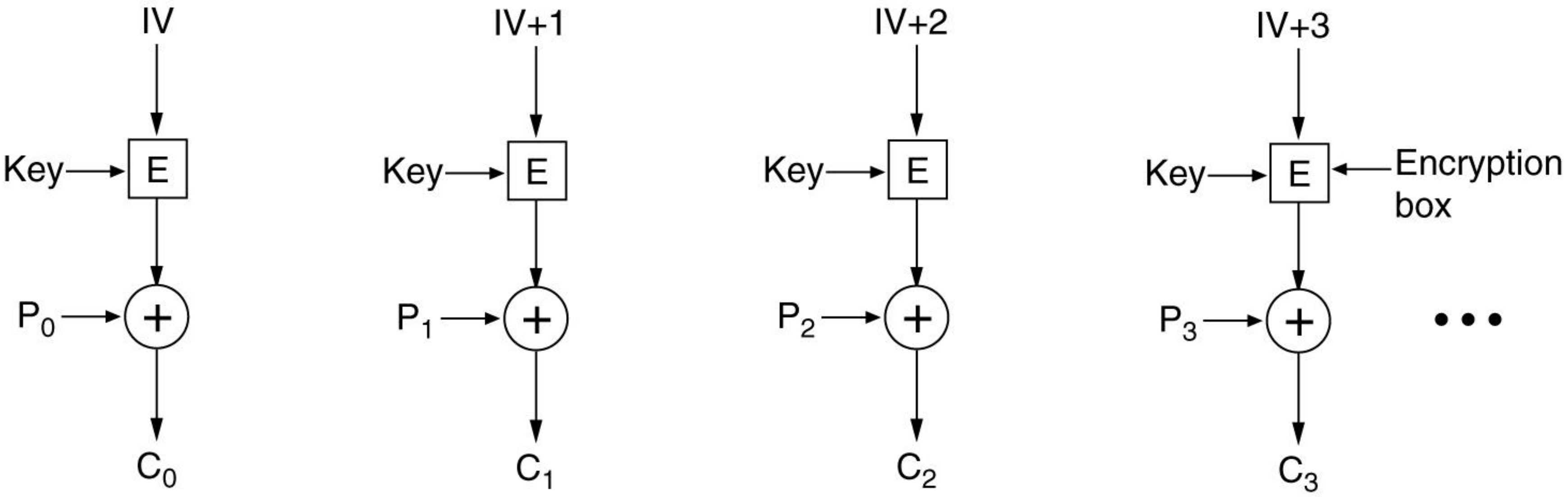
(a) Encryption. (c) Decryption.

Stream Cipher Mode



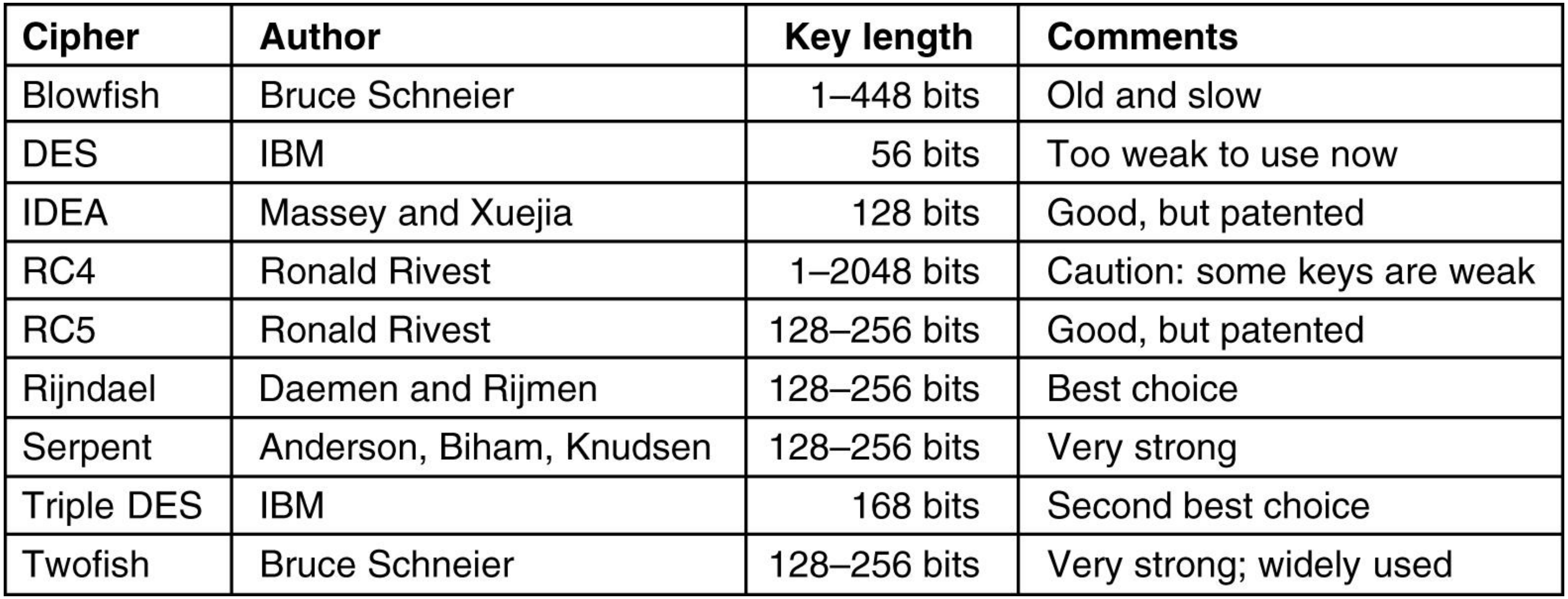
A stream cipher. (a) Encryption. (b) Decryption.

Counter Mode



Encryption using counter mode.

Cryptanalysis



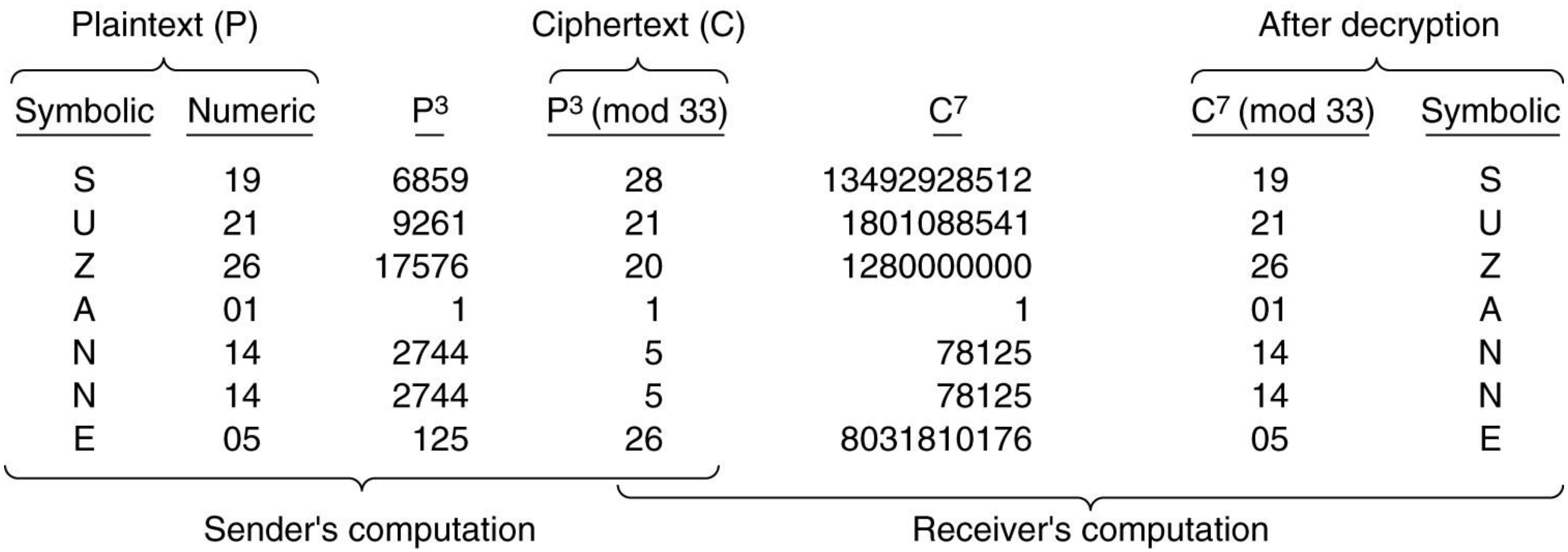
Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	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.

Public-Key Algorithms

- RSA
- Other Public-Key Algorithms

RSA



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

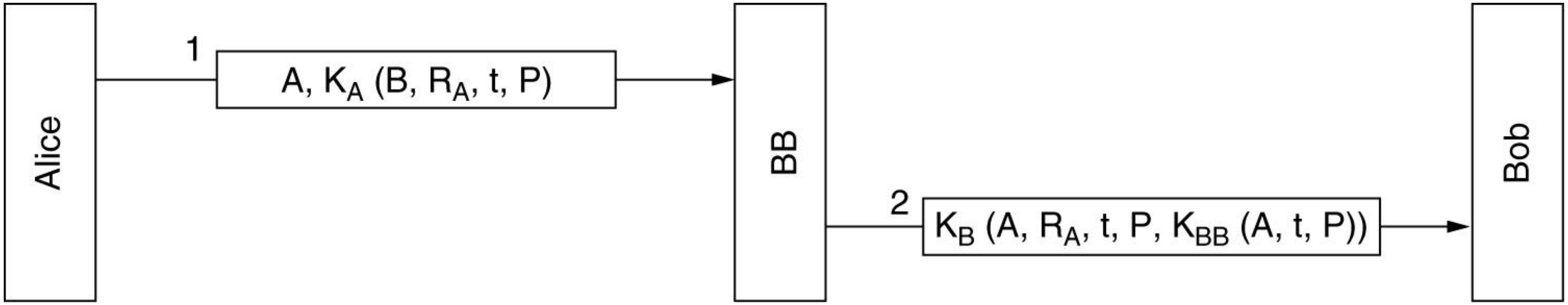
Receiver's computation

An example of the RSA algorithm.

Digital Signatures

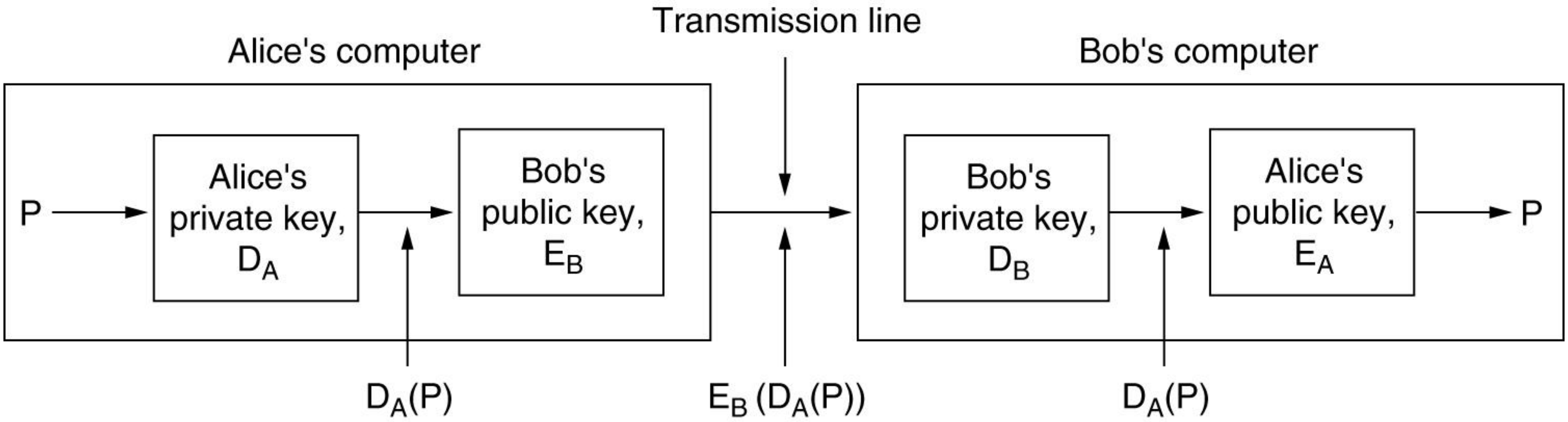
- Symmetric-Key Signatures
- Public-Key Signatures
- Message Digests
- The Birthday Attack

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

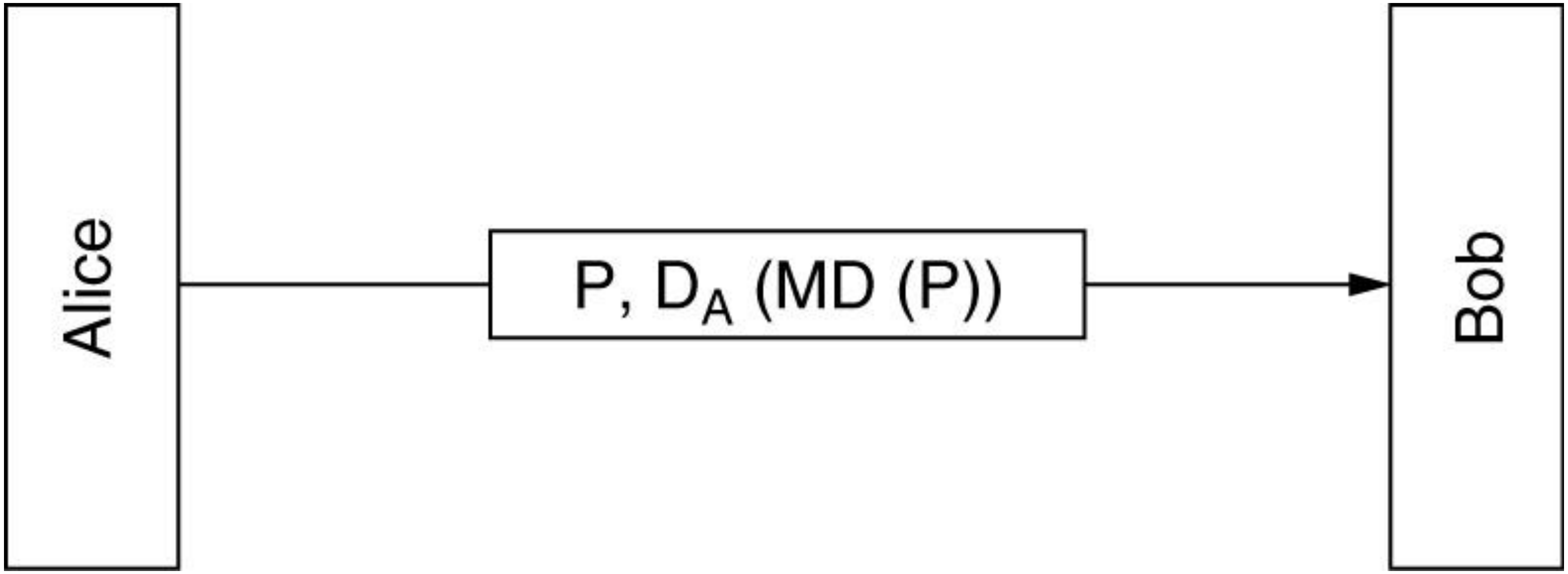
Digital signatures with Big Brother.

Public-Key Signatures



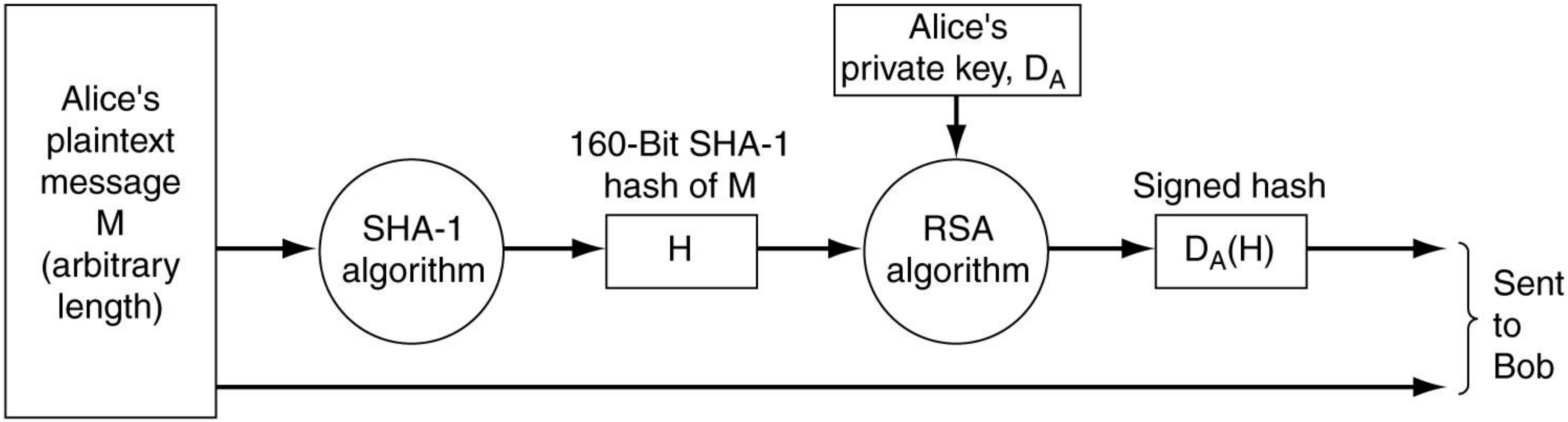
Digital signatures using public-key cryptography.

Message Digests



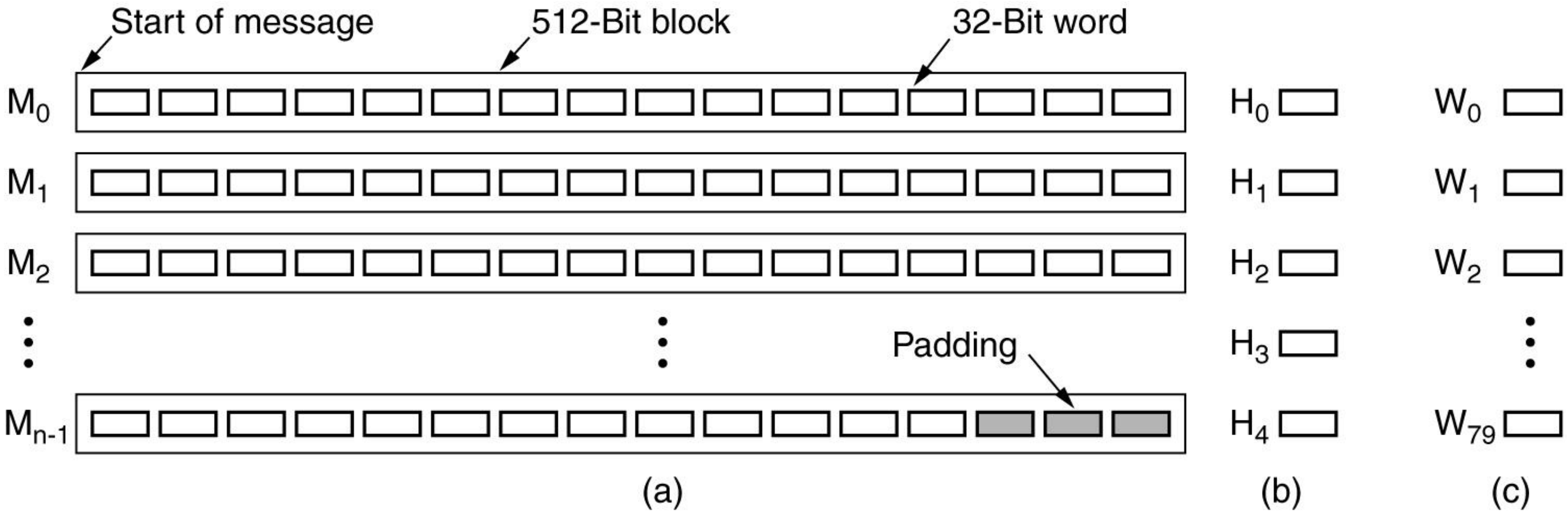
Digital signatures using message digests.

SHA-1



Use of SHA-1 and RSA for signing nonsecret messages.

SHA-1 (2)

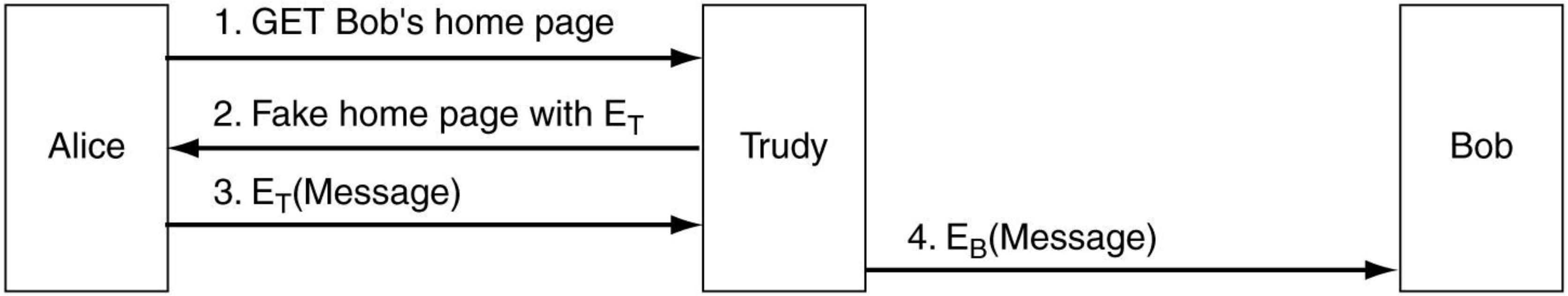


(a) A message padded out to a multiple of 512 bits.
(b) The output variables. (c) The word array.

Management of Public Keys

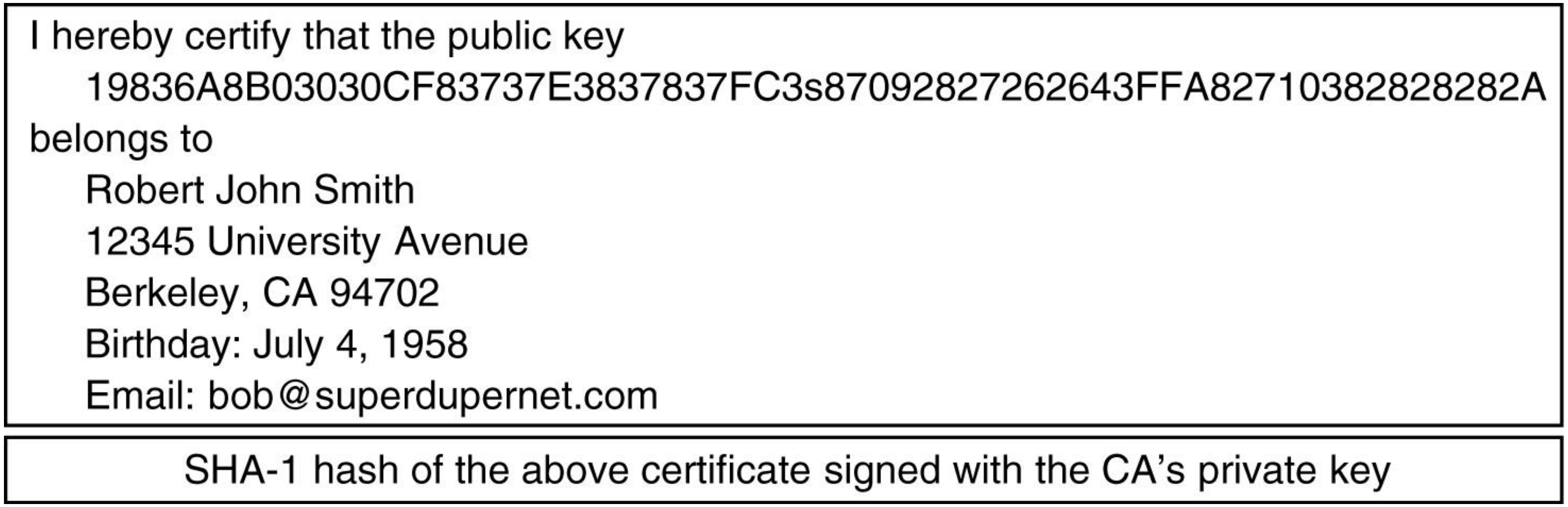
- Certificates
- X.509
- Public Key Infrastructures

Problems with Public-Key Encryption



A way for Trudy to subvert public-key encryption.

Certificates



I hereby certify that the public key

19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A

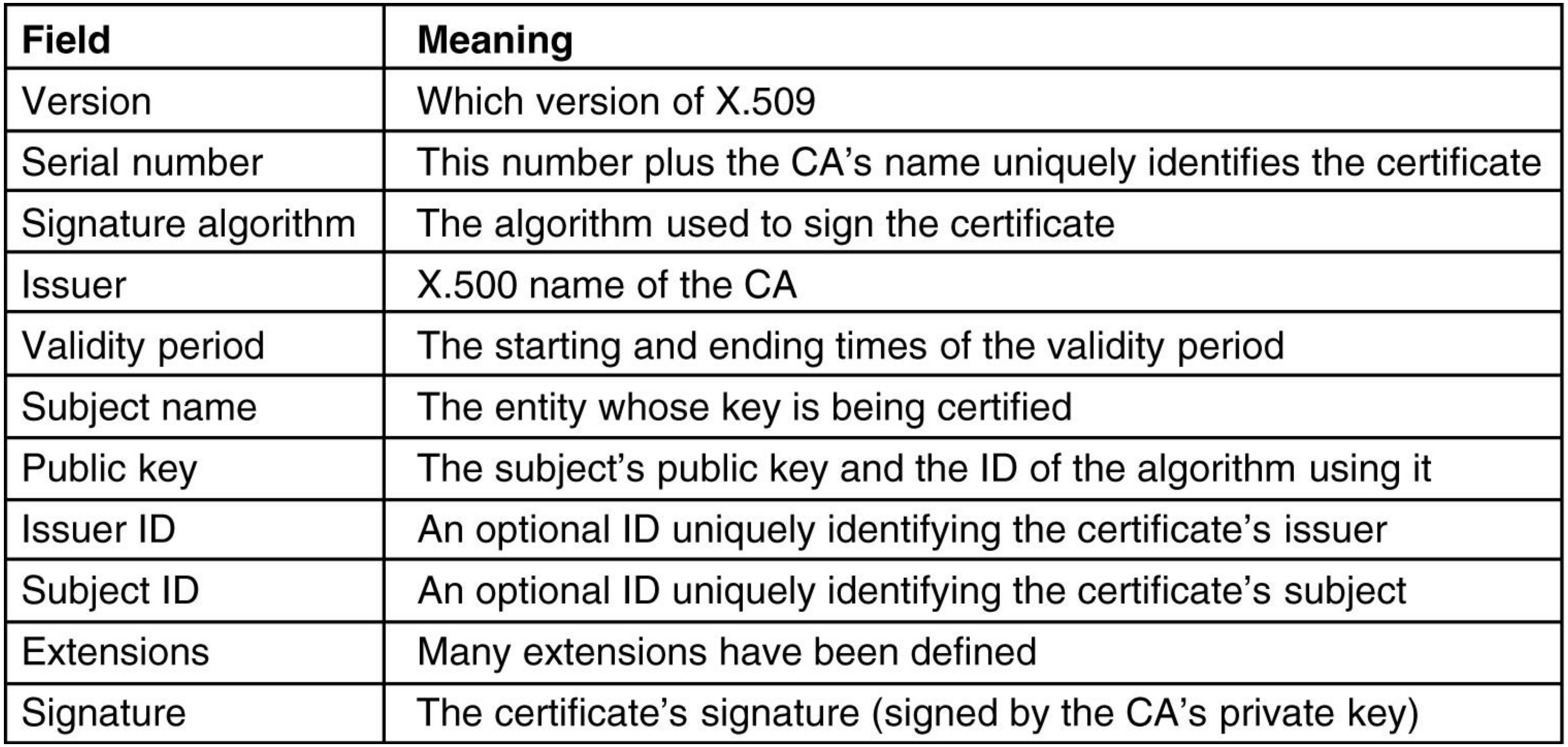
belongs to

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.

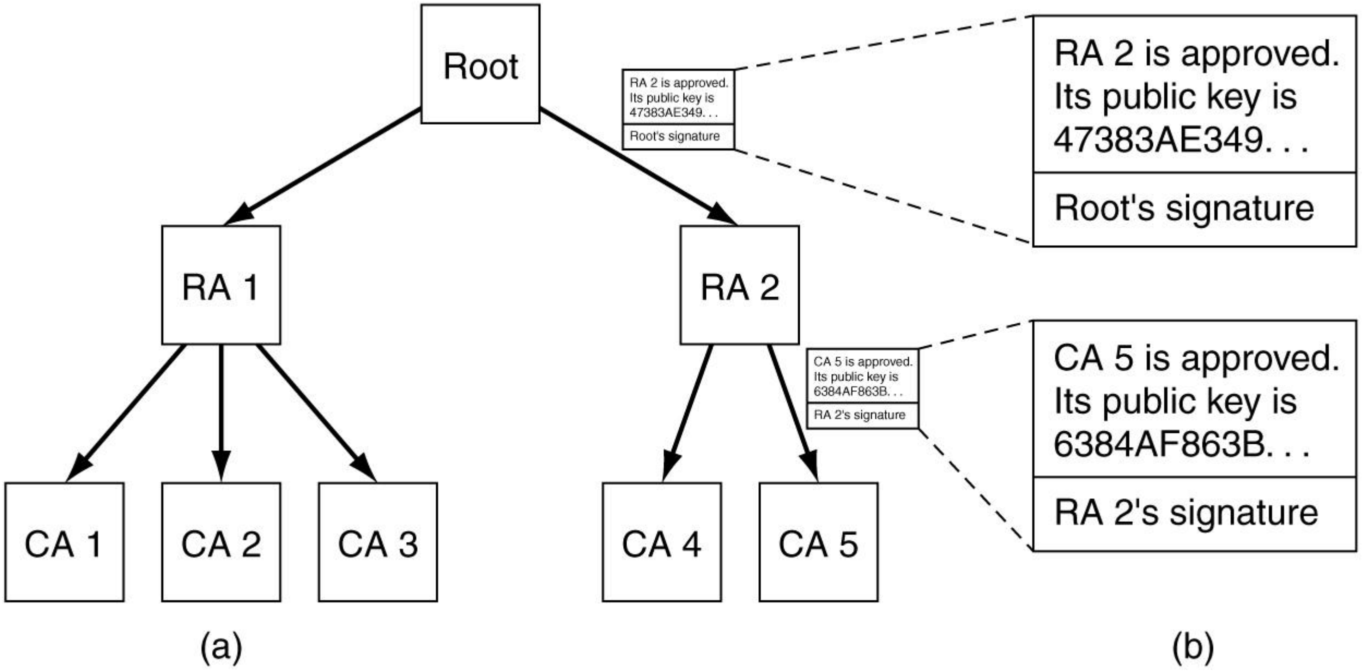
X.509



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.

Public-Key Infrastructures

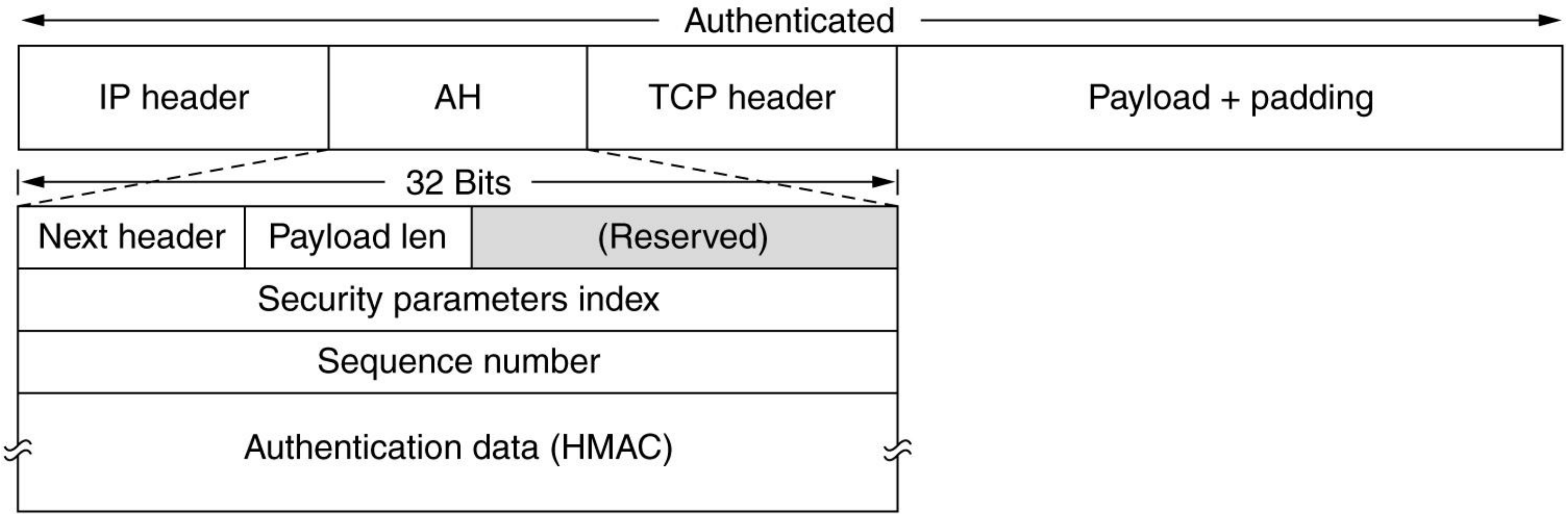

Root
RA 1
RA 2
CA 1
CA 2
CA 3
CA 4
CA 5
RA 2 is approved. Its public key is 47383AE349. . .
Root's signature
RA 2 is approved. Its public key is 47383AE349. . .
Root's signature
CA 5 is approved. Its public key is 6384AF863B. . .
RA 2's signature
CA 5 is approved. Its public key is 6384AF863B. . .
RA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

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

Communication Security

- IPsec
- Firewalls
- Virtual Private Networks
- Wireless Security

IPsec



Authenticated

IP header

AH

TCP header

Payload + padding

32 Bits

Next header

Payload len

(Reserved)

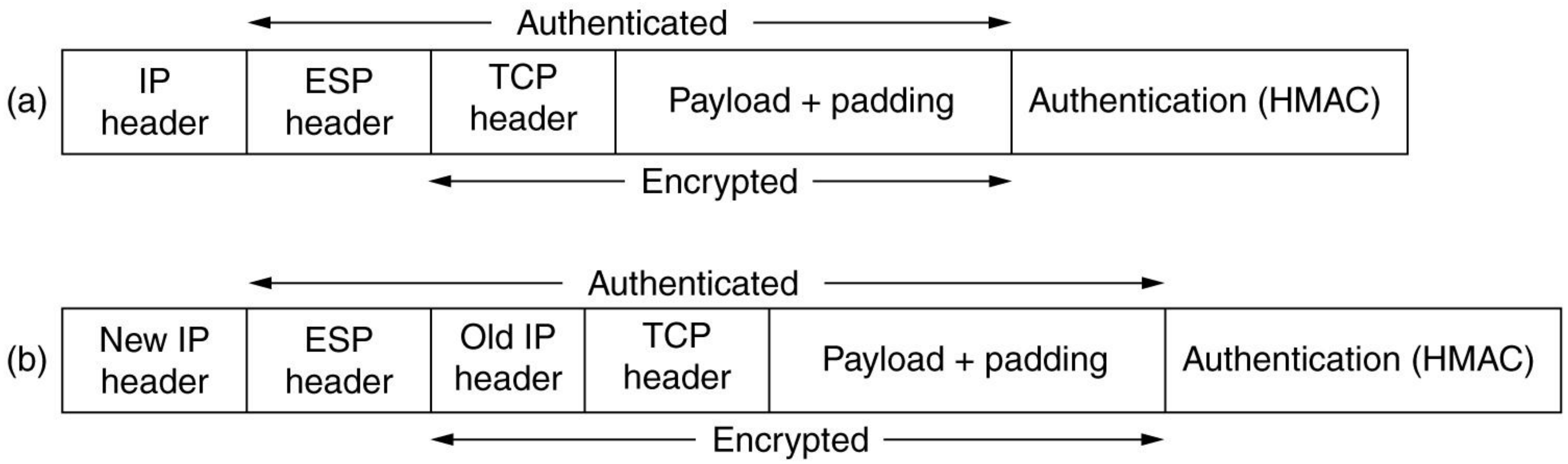
Security parameters index

Sequence number

Authentication data (HMAC)

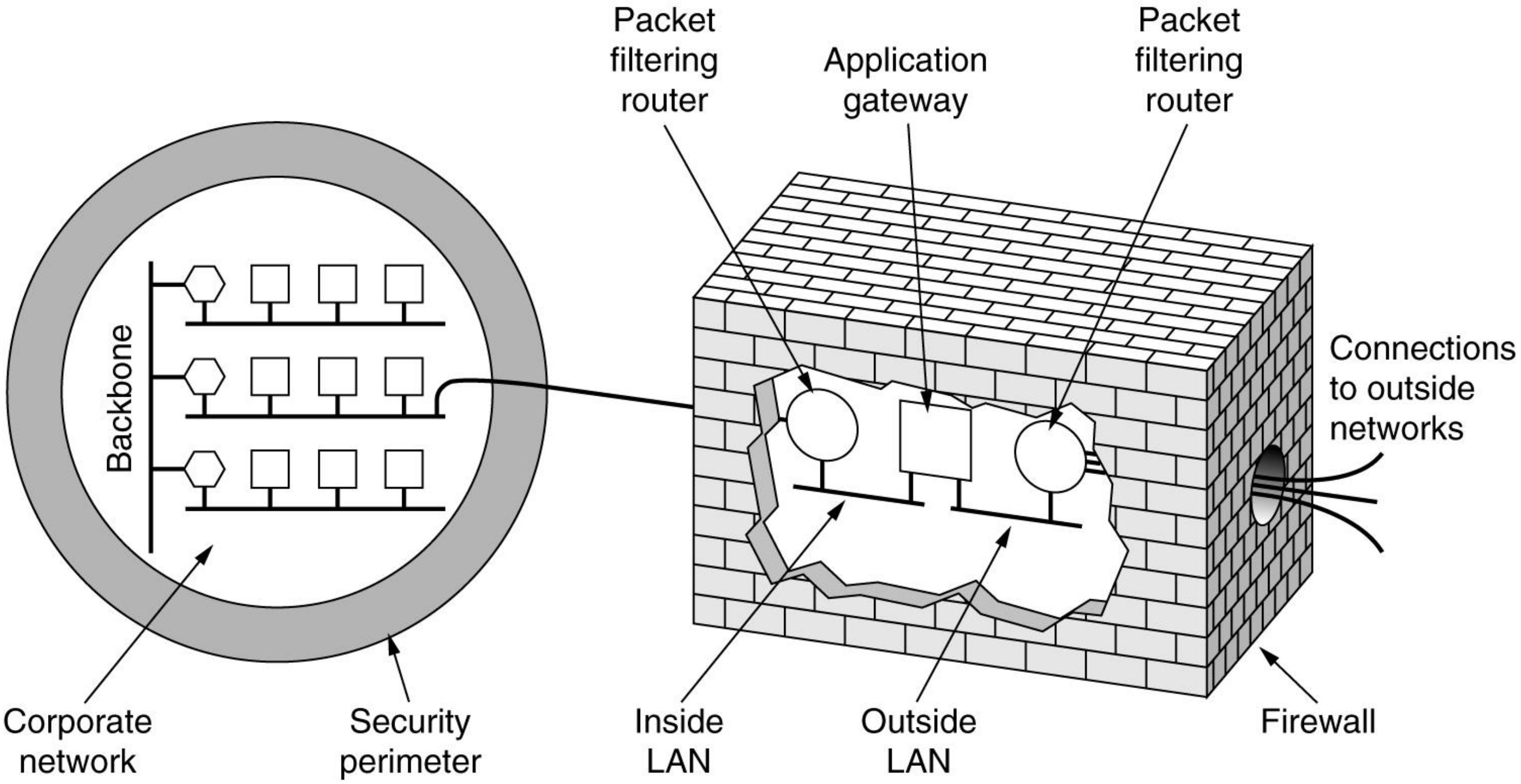
The IPsec authentication header in transport mode for IPv4.

IPsec (2)



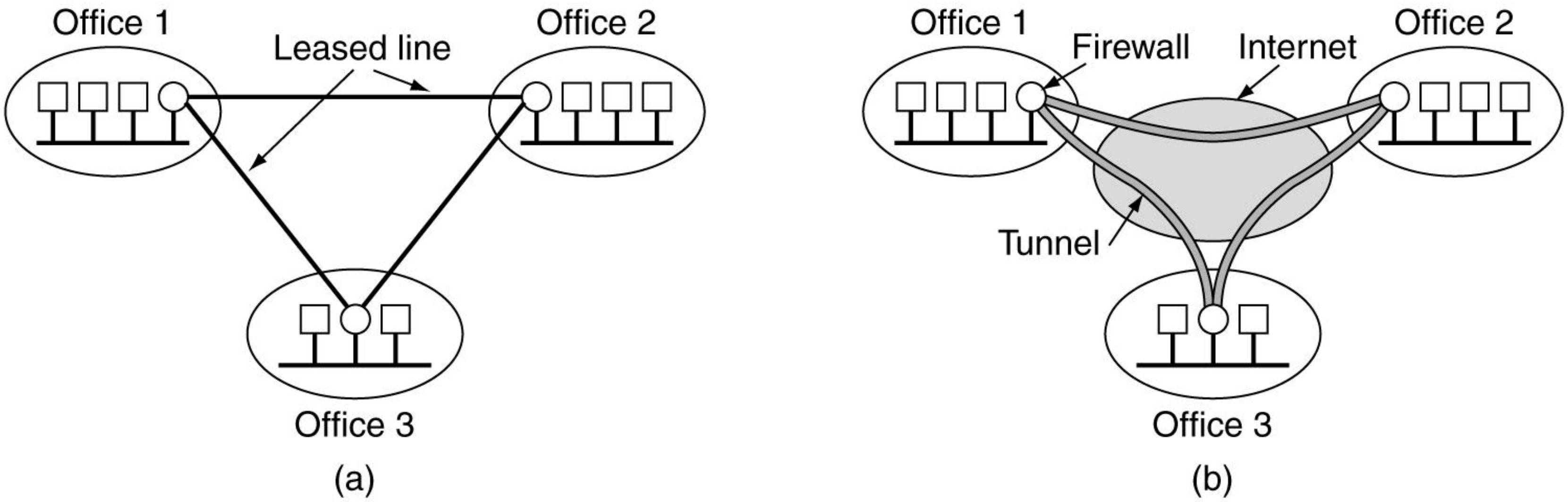
(a) ESP in transport mode. (b) ESP in tunnel mode.

Firewalls



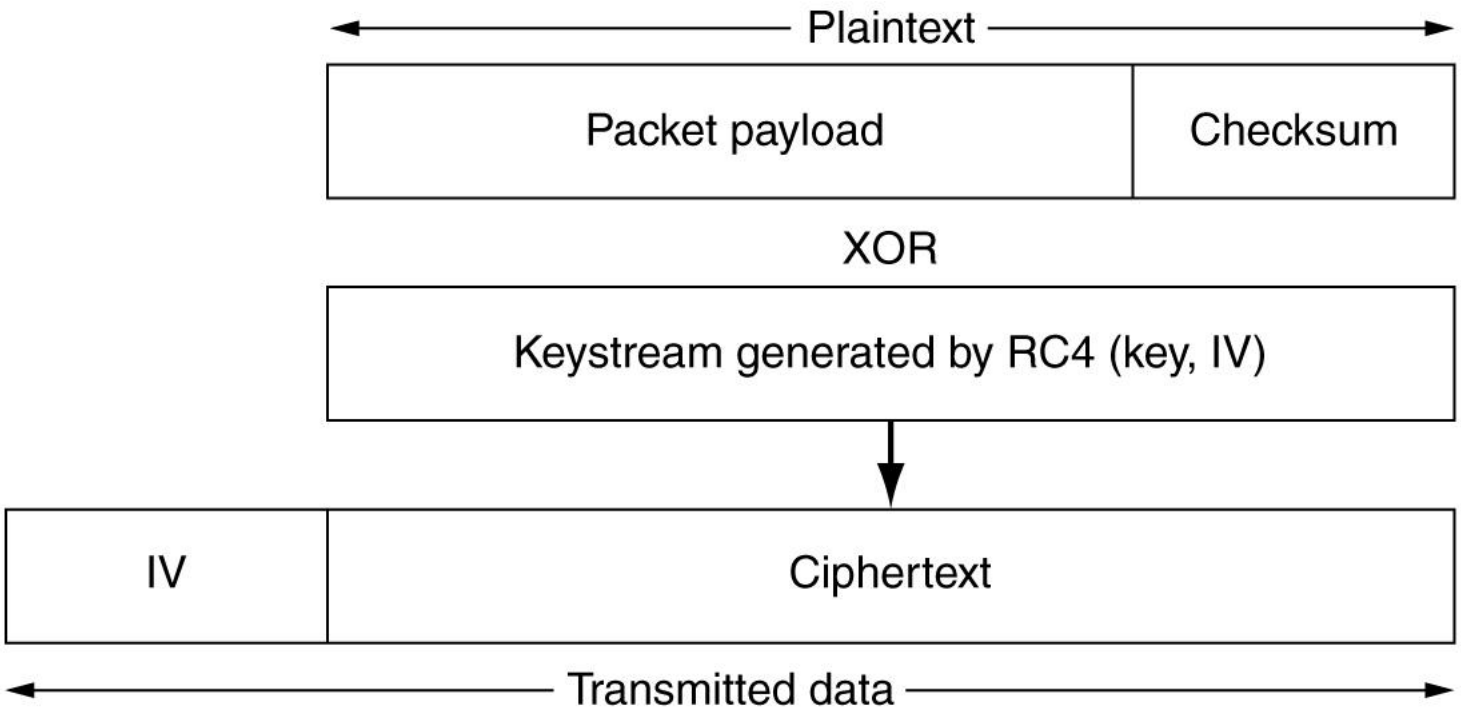
A firewall consisting of two packet filters and an application gateway.

Virtual Private Networks



(a) A leased-line private network. (b) A virtual private network.

802.11 Security

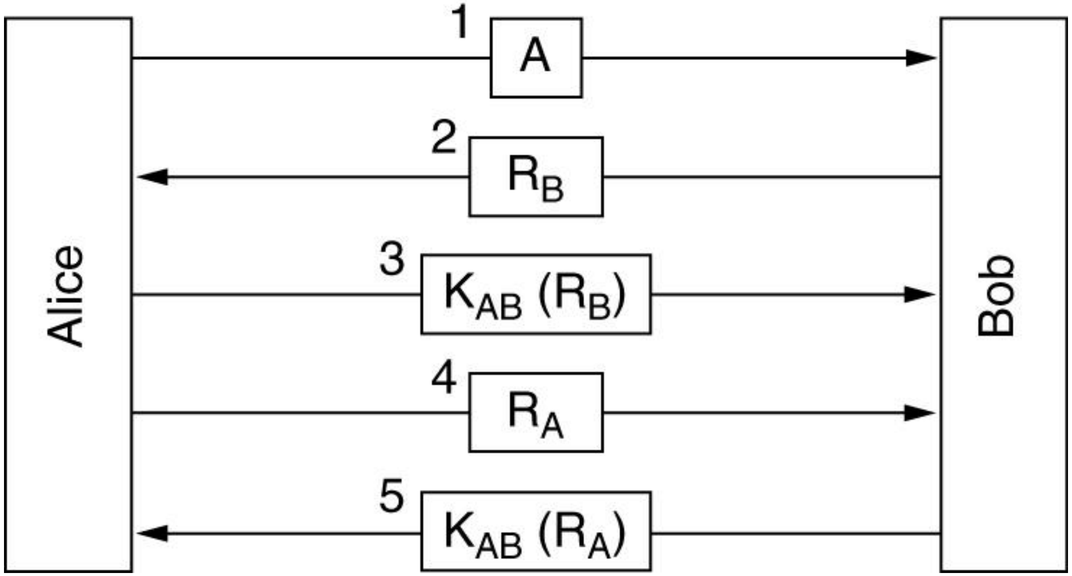


Packet encryption using WEP.

Authentication Protocols

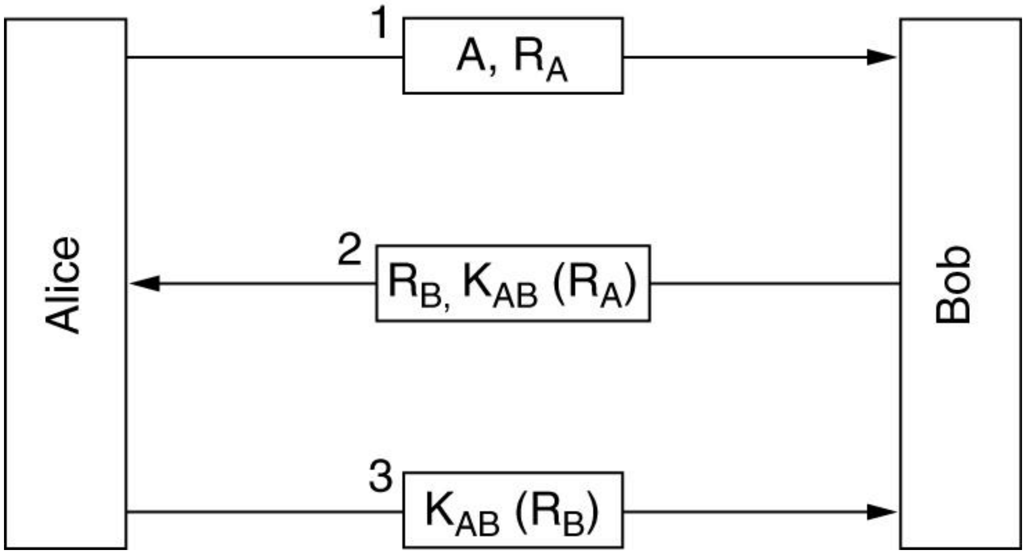
- Authentication Based on a Shared Secret Key
- Establishing a Shared Key: Diffie-Hellman
- Authentication Using a Key Distribution Center
- Authentication Using Kerberos
- Authentication Using Public-Key Cryptography

Authentication Based on a Shared Secret Key



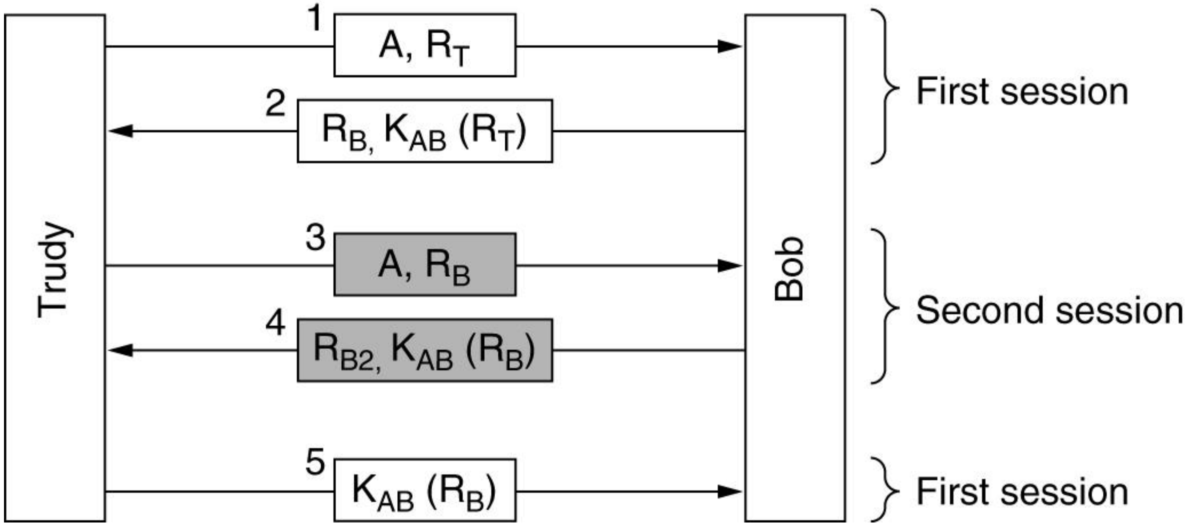
Two-way authentication using a challenge-response protocol.

Authentication Based on a Shared Secret Key (2)



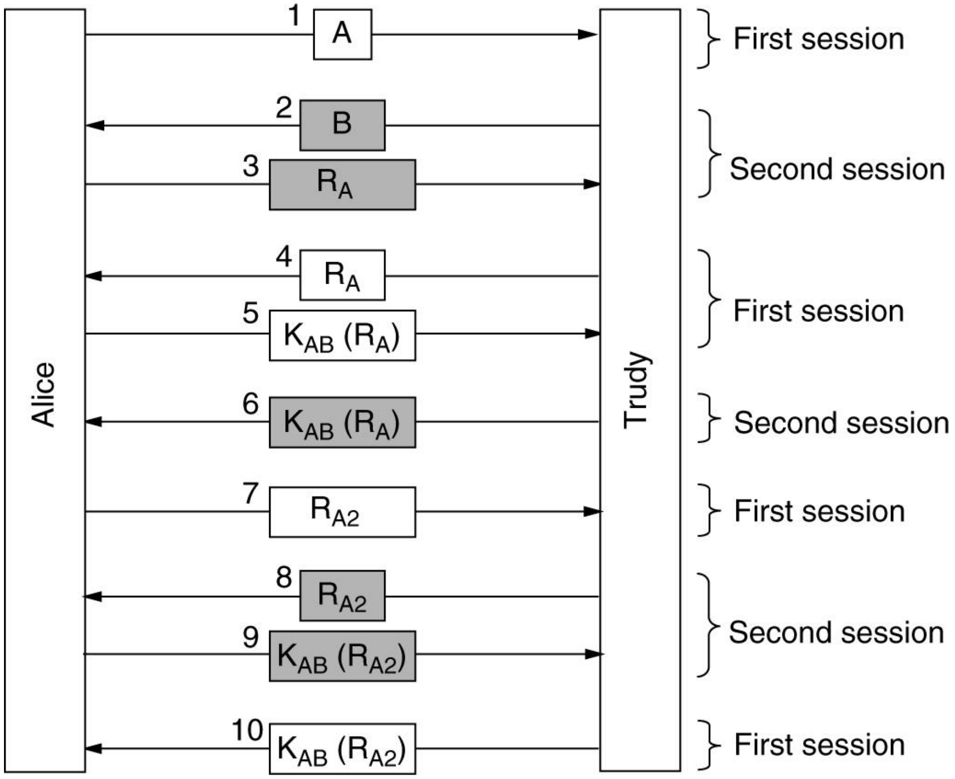
A shortened two-way authentication protocol.

Authentication Based on a Shared Secret Key (3)



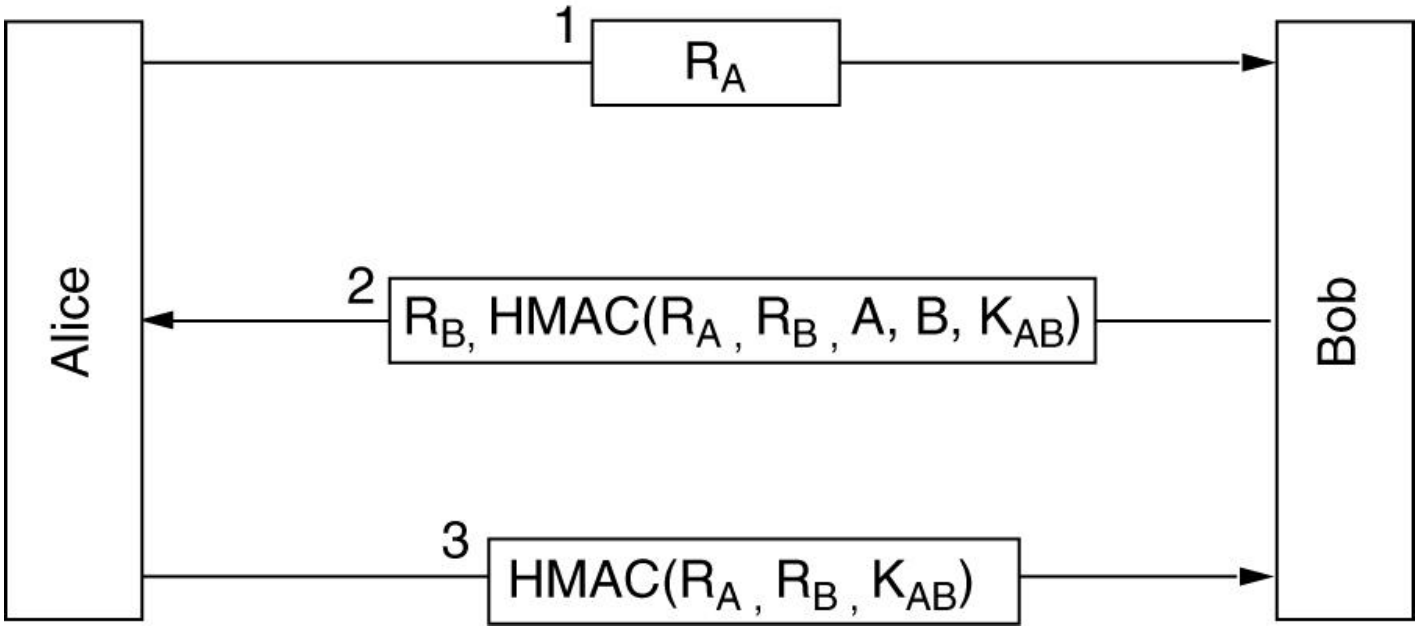
The reflection attack.

Authentication Based on a Shared Secret Key (4)



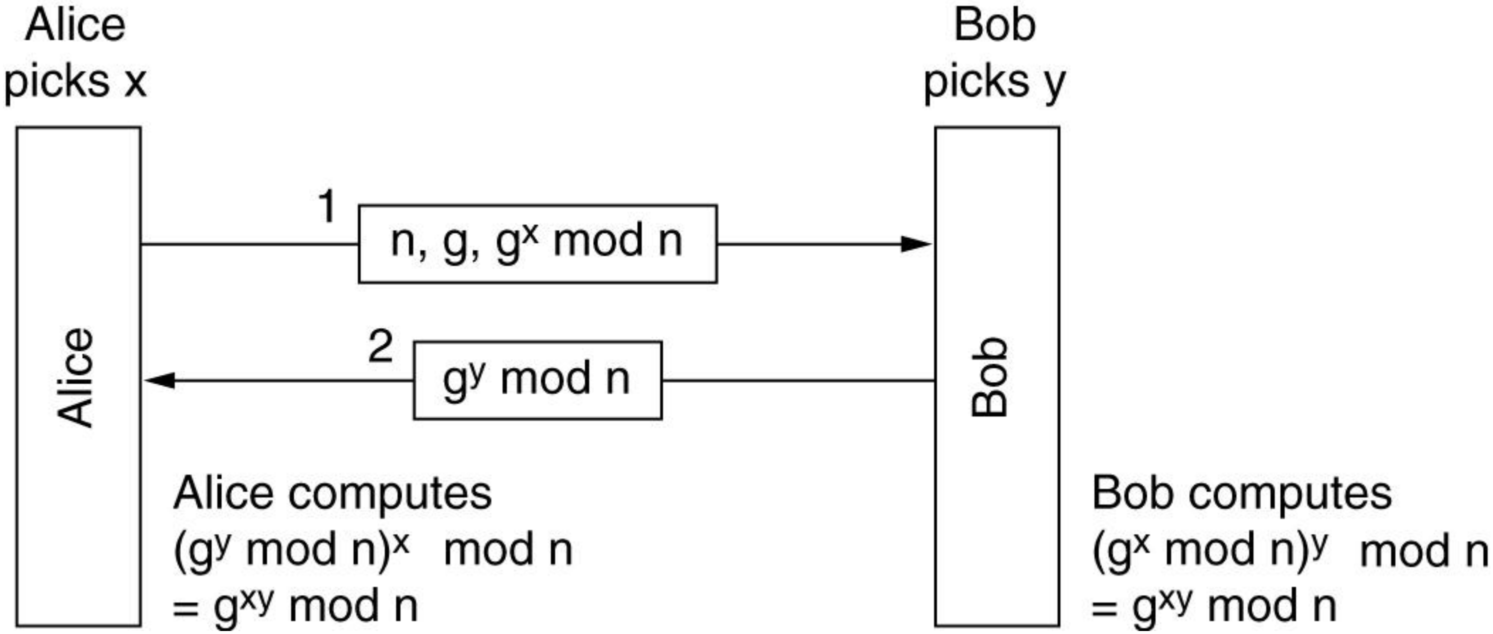
A reflection attack on the protocol of Fig. 8-32.

Authentication Based on a Shared Secret Key (5)


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})

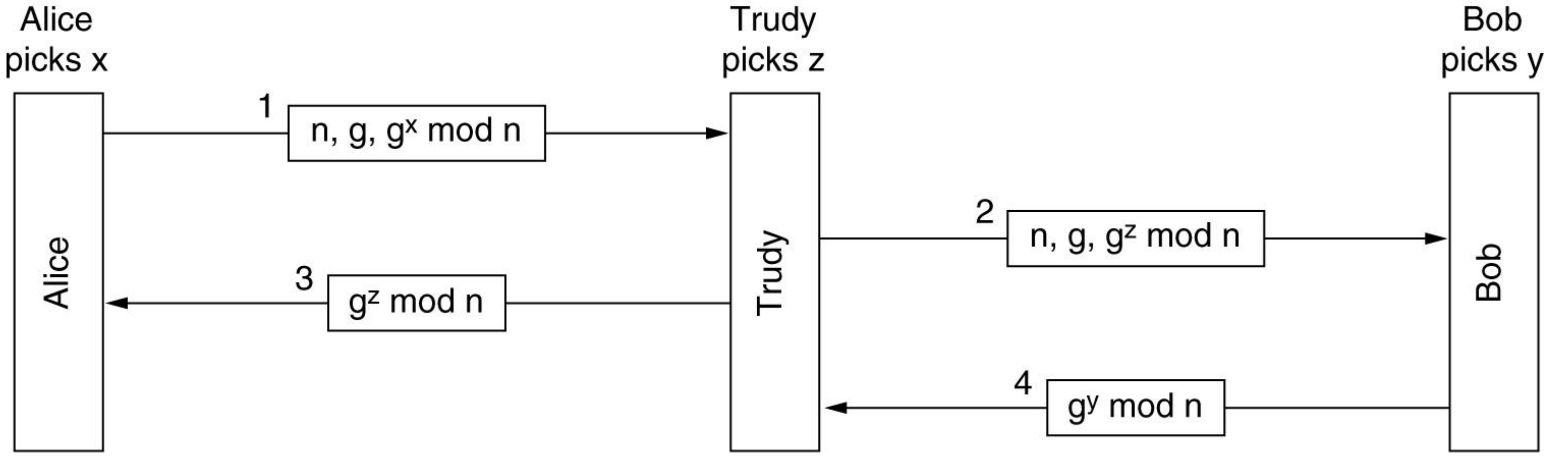
Authentication using HMACs.

Establishing a Shared Key: The Diffie-Hellman Key Exchange



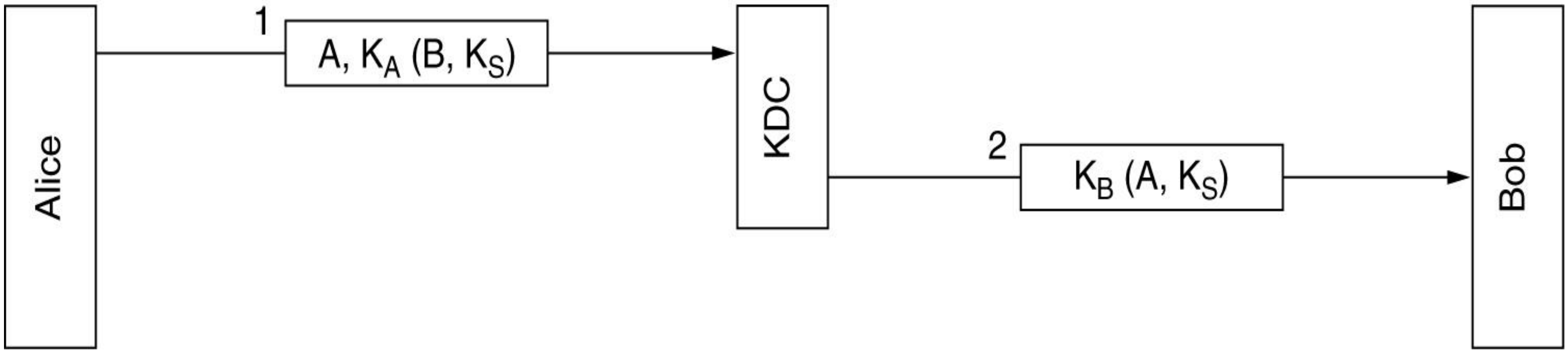
The Diffie-Hellman key exchange.

Establishing a Shared Key: The Diffie-Hellman Key Exchange



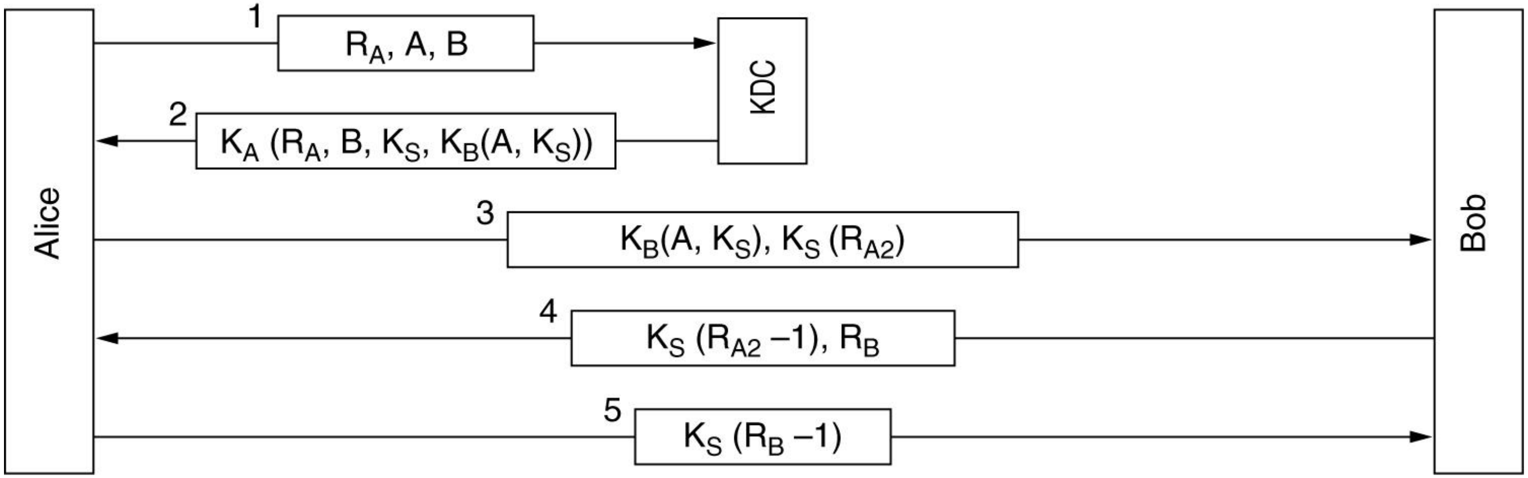
The bucket brigade or man-in-the-middle attack.

Authentication Using a Key Distribution Center



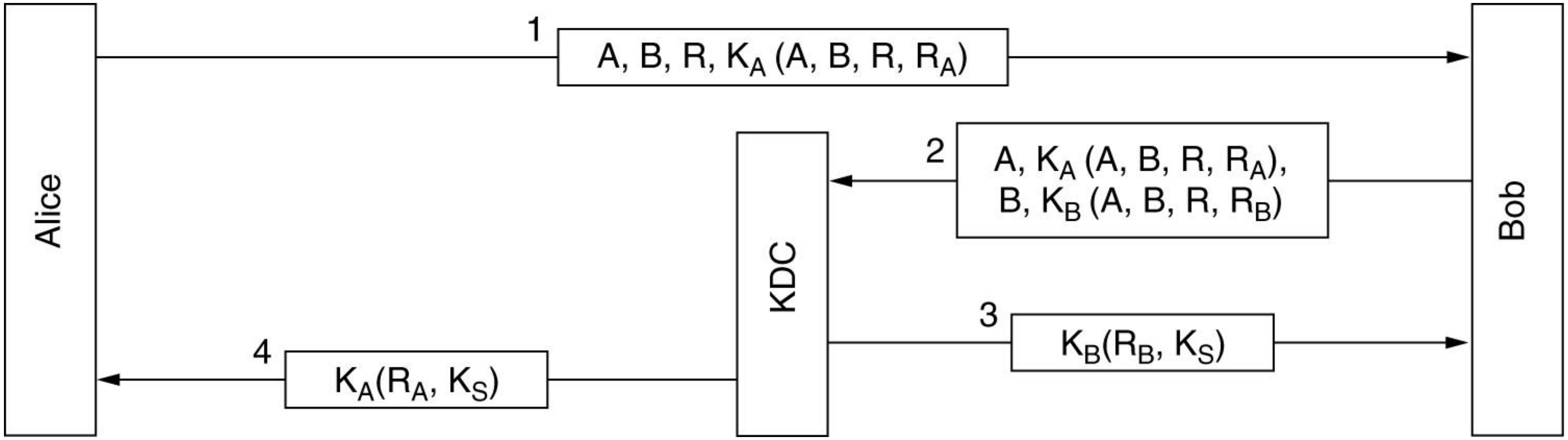
A first attempt at an authentication protocol using a KDC.

Authentication Using a Key Distribution Center (2)


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)

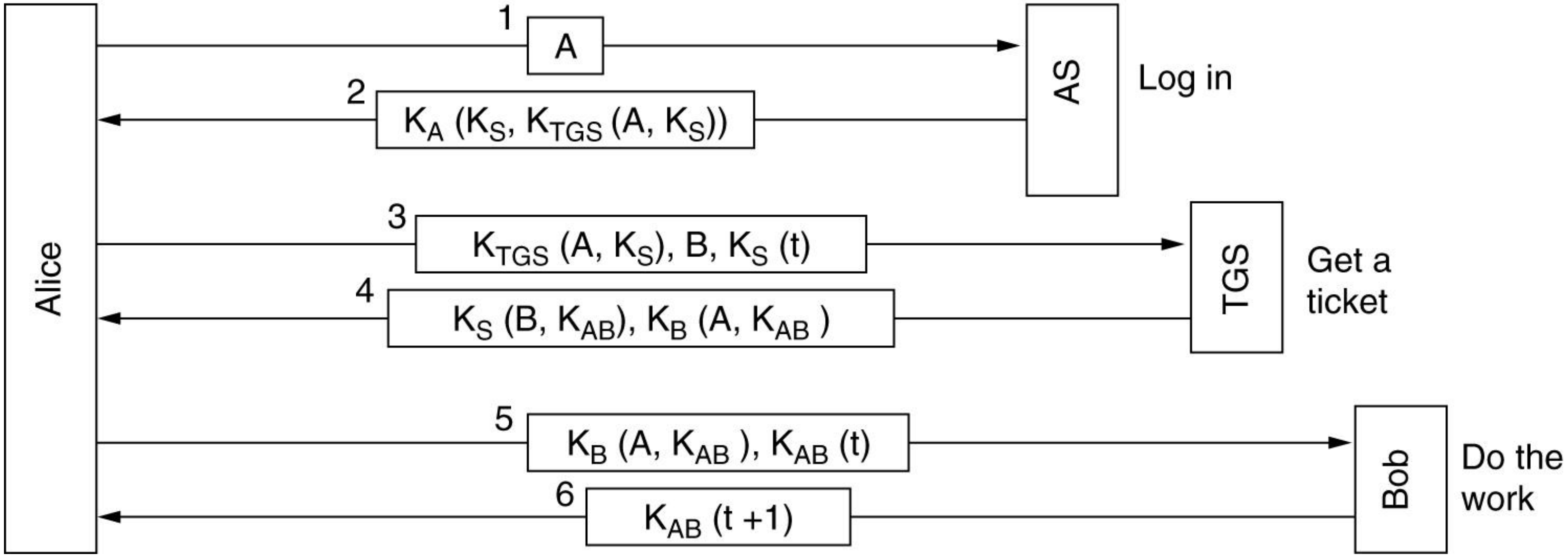
The Needham-Schroeder authentication protocol.

Authentication Using a Key Distribution Center (3)



The Otway-Rees authentication protocol (slightly simplified).

Authentication Using Kerberos



Alice

1 A

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

AS

Log in

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

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

TGS

Get a ticket

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

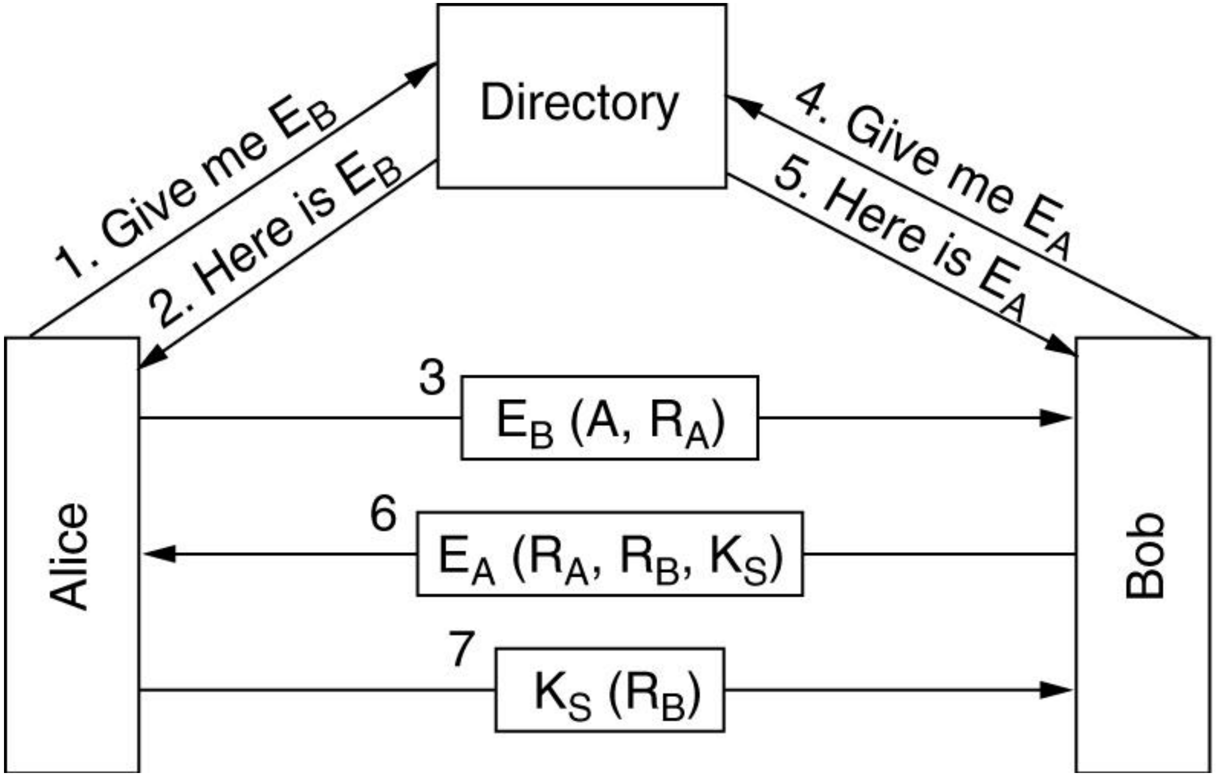
6 $K_{AB} (t +1)$

Bob

Do the work

The operation of Kerberos V4.

Authentication Using Public-Key Cryptography

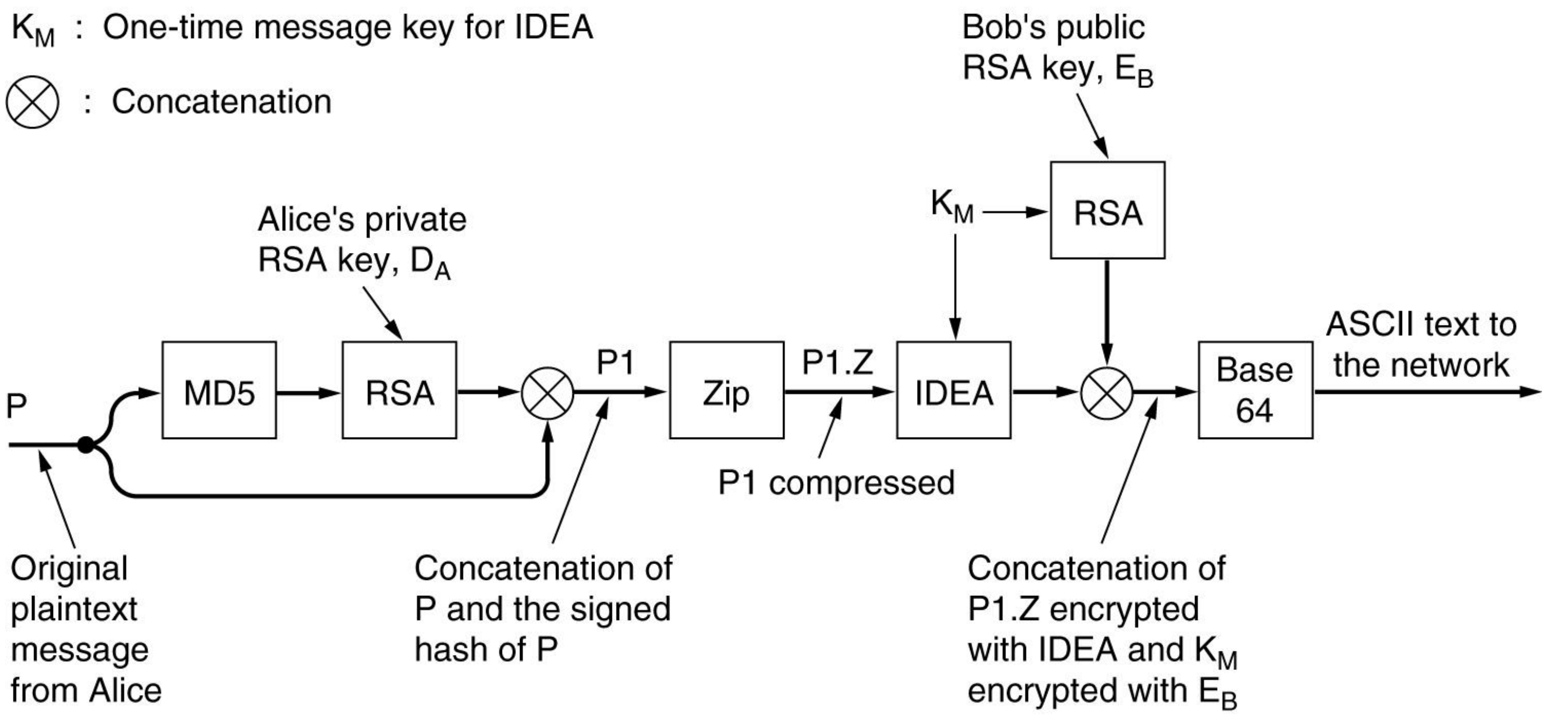


Mutual authentication using public-key cryptography.

E-Mail Security

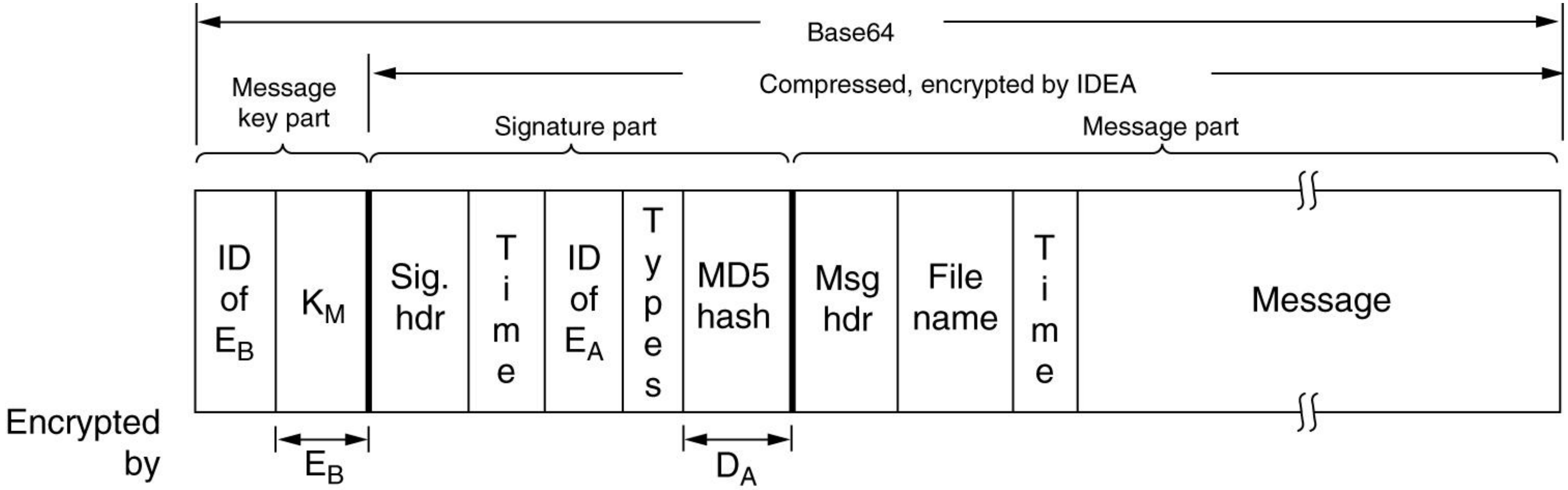
- PGP – Pretty Good Privacy
- PEM – Privacy Enhanced Mail
- S/MIME

PGP – Pretty Good Privacy


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 in operation for sending a message.

PGP – Pretty Good Privacy (2)

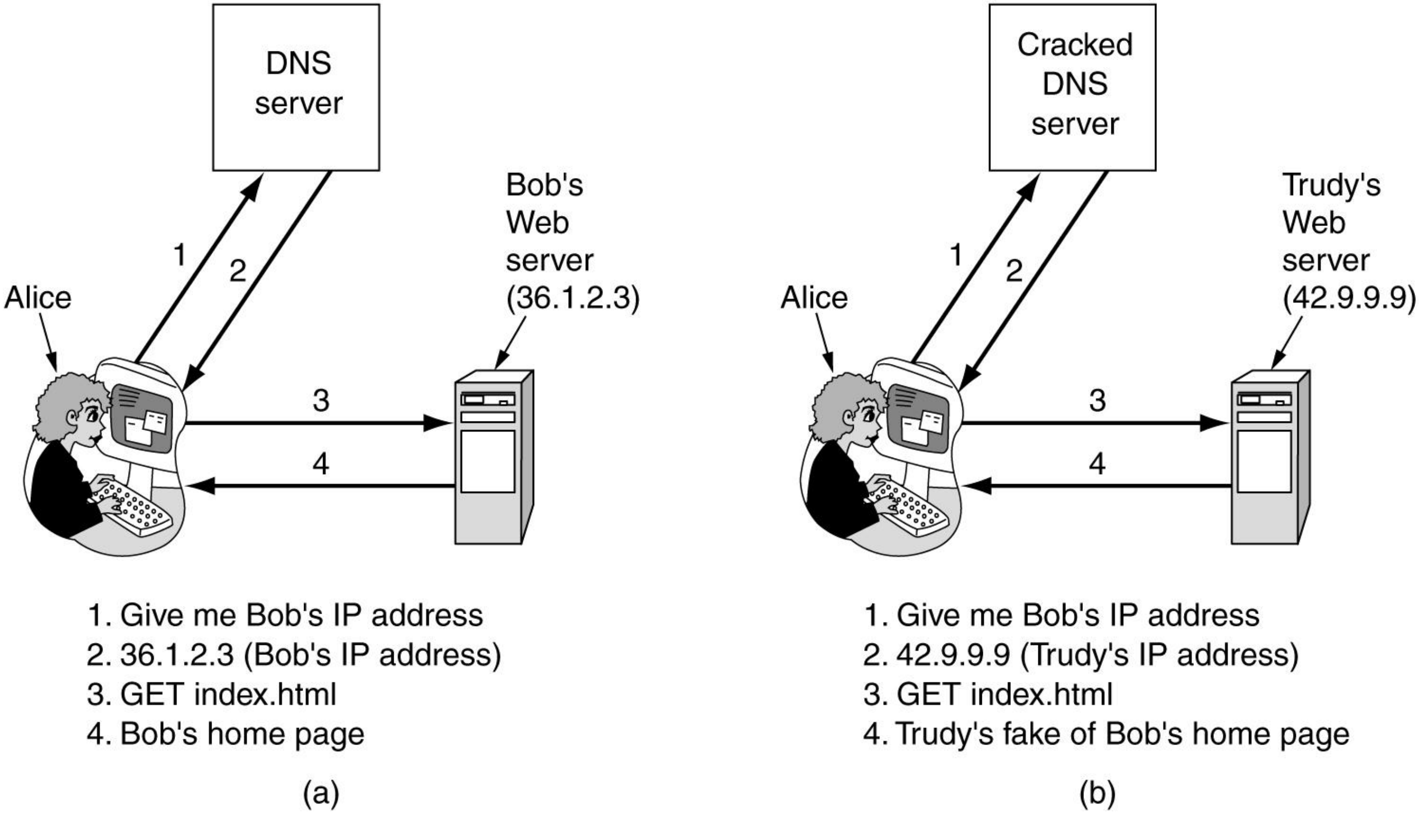


A PGP message.

Web Security

- Threats
- Secure Naming
- SSL – The Secure Sockets Layer
- Mobile Code Security

Secure Naming



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

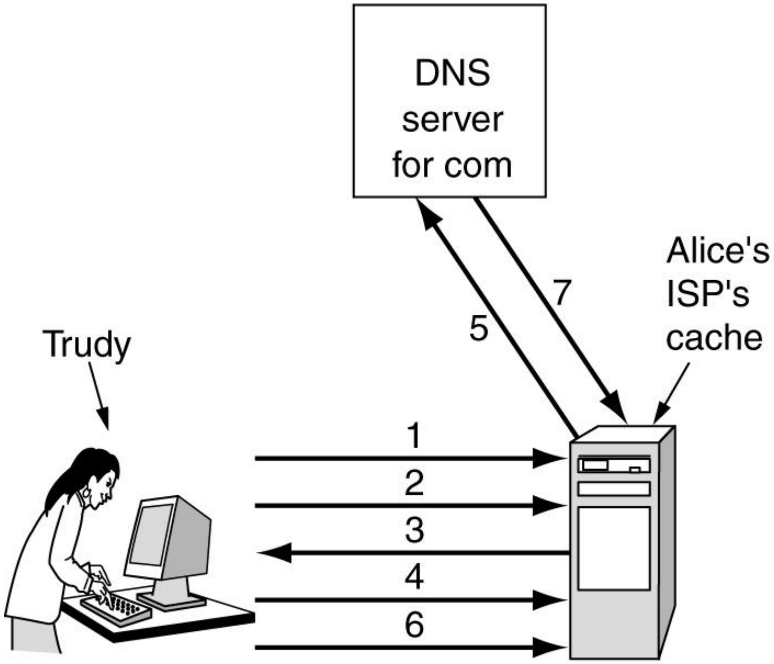
(a)

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)

(a) Normal situation. (b) An attack based on breaking into DNS and modifying Bob's record.

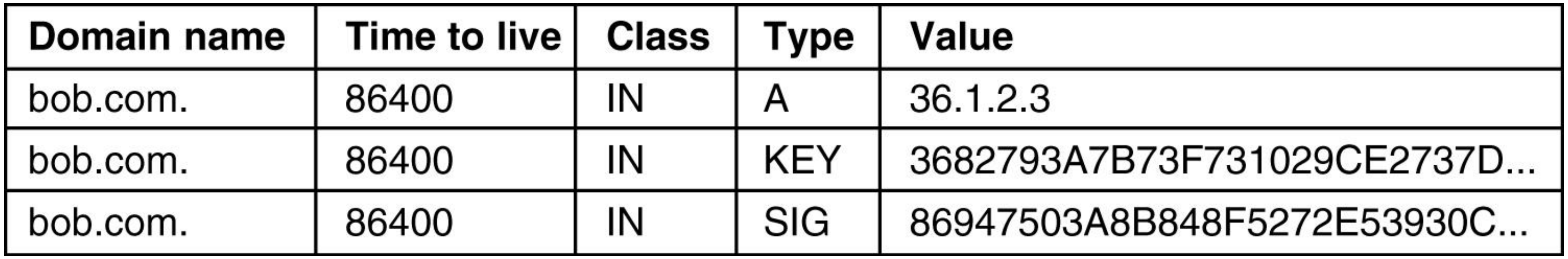
Secure Naming (2)



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.

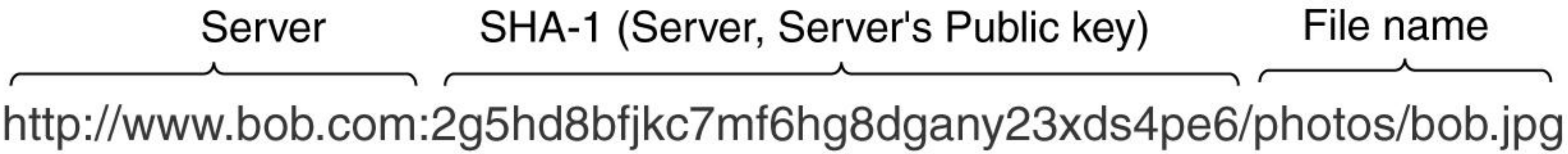
Secure DNS



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 has of the *A* and *KEY* records to verify their authenticity.

Self-Certifying Names

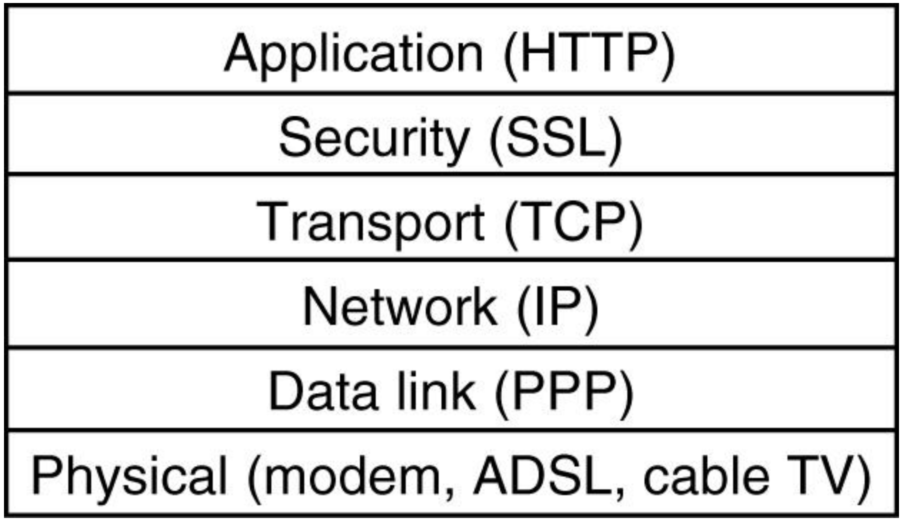


Server SHA-1 (Server, Server's Public key) File name

http://www.bob.com:2g5hd8bfjkc7mf6hg8dgany23xds4pe6/photos/bob.jpg

A self-certifying URL containing a hash of server's name and public key.

SSL—The Secure Sockets Layer



Application (HTTP)

Security (SSL)

Transport (TCP)

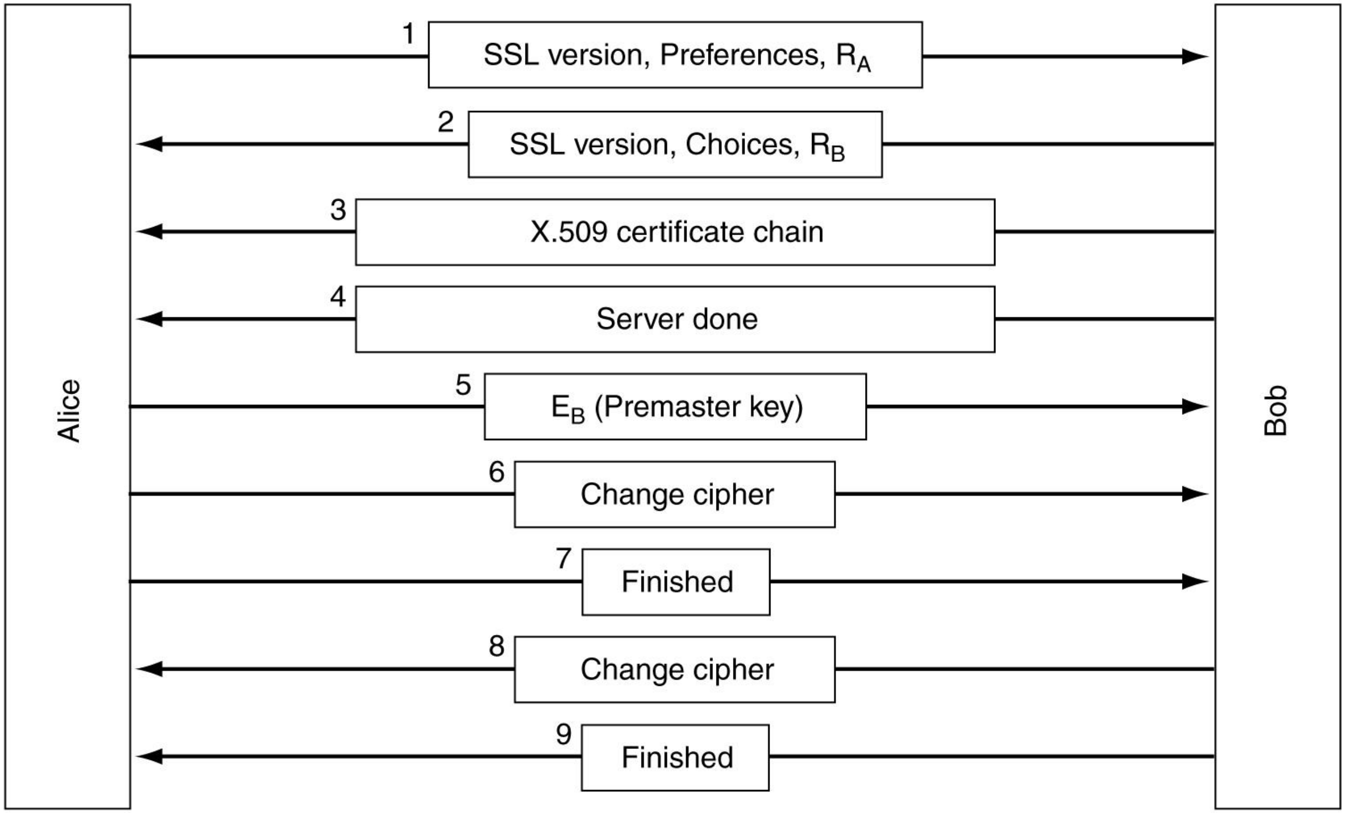
Network (IP)

Data link (PPP)

Physical (modem, ADSL, cable TV)

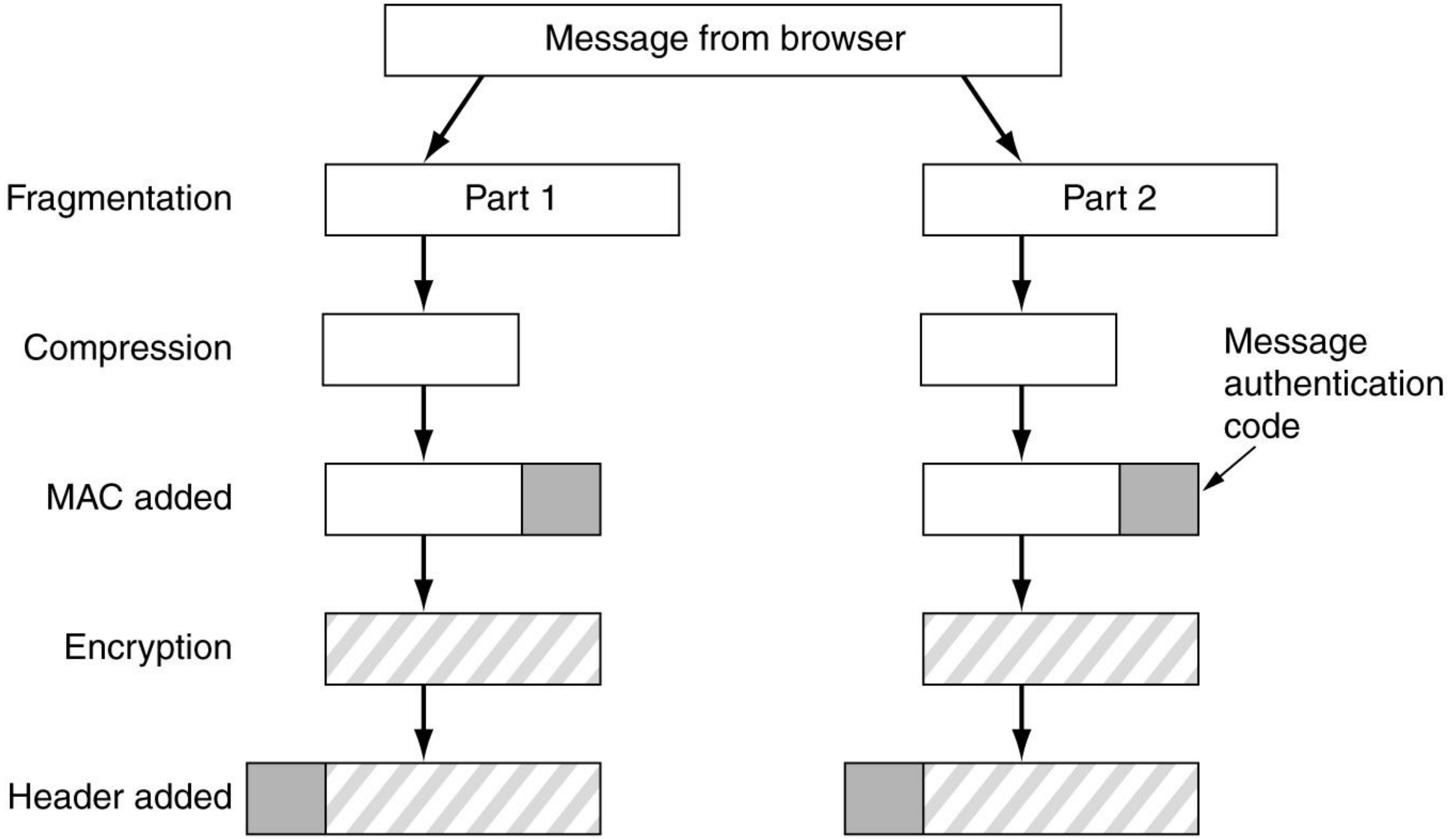
Layers (and protocols) for a home user browsing with SSL.

SSL (2)



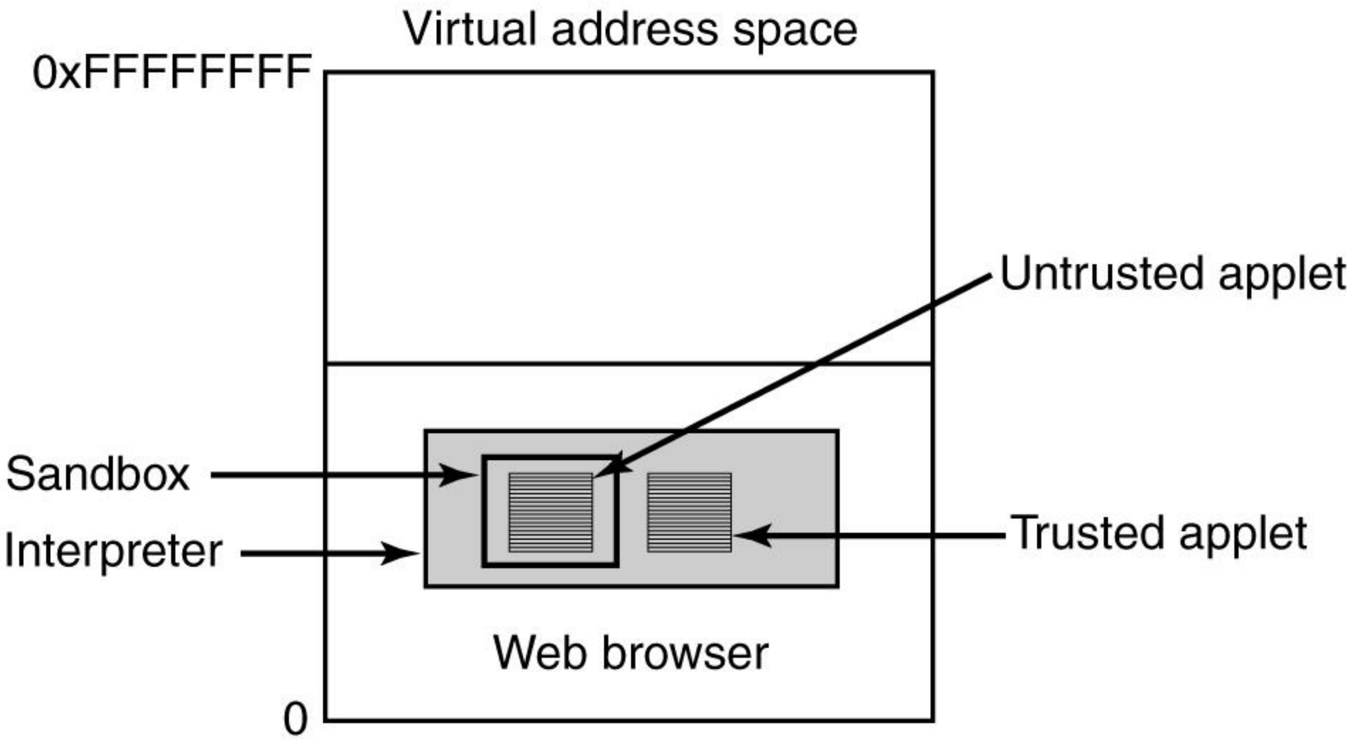
A simplified version of the SSL connection establishment subprotocol.

SSL (3)



Data transmission using SSL.

Java Applet Security

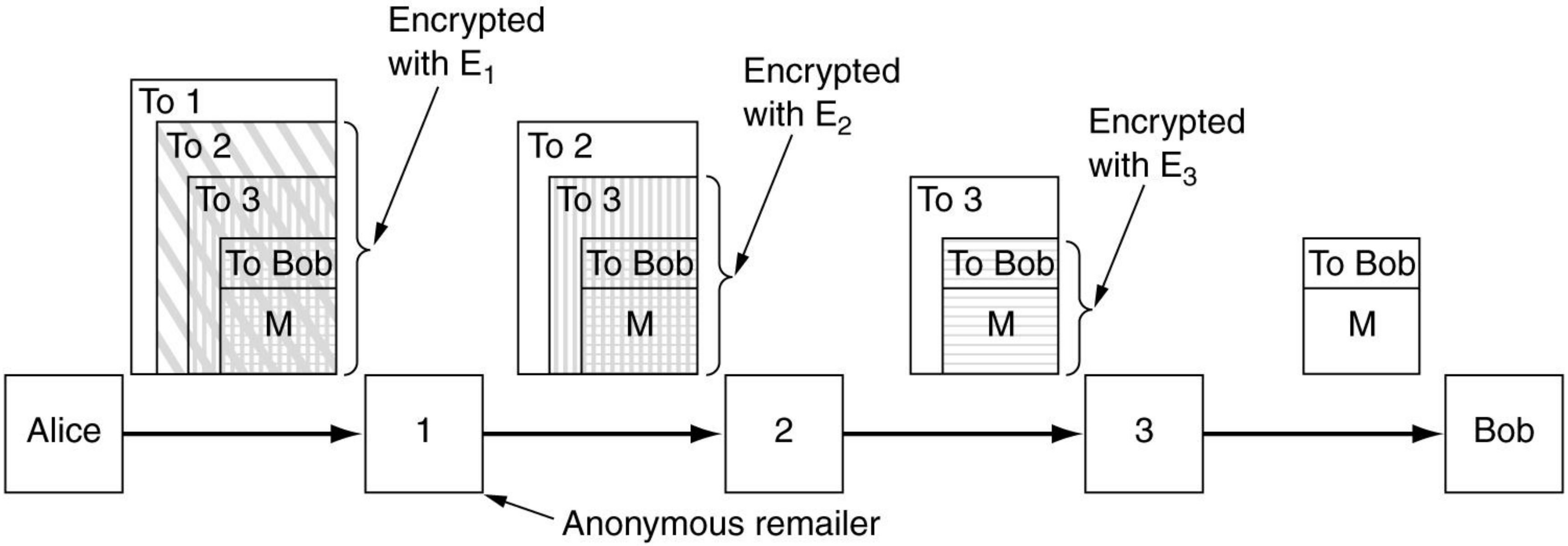


Applets inserted into a Java Virtual Machine interpreter inside the browser.

Social Issues

- Privacy
- Freedom of Speech
- Copyright

Anonymous Remailers



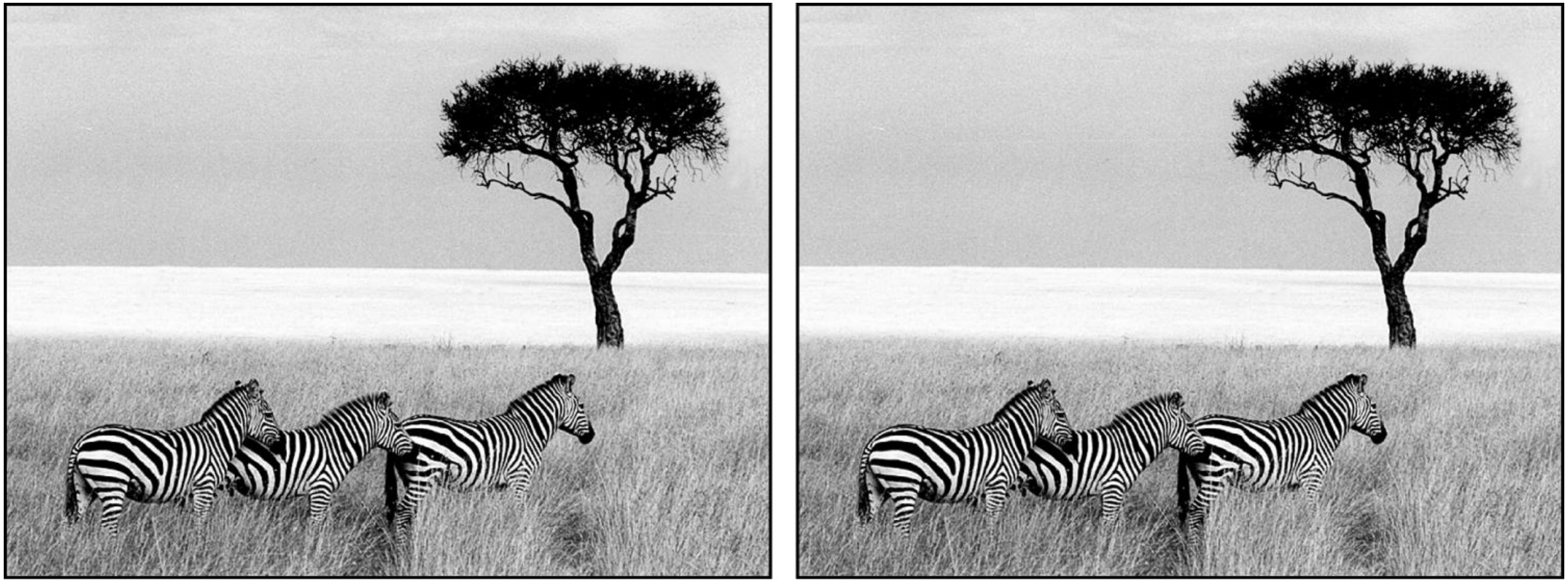
Users who wish anonymity chain requests through multiple anonymous remailers.

Freedom of Speech

Possibly banned material:

1. Material inappropriate for children or teenagers.
2. Hate aimed at various ethnic, religious, sexual, or other groups.
3. Information about democracy and democratic values.
4. Accounts of historical events contradicting the government's version.
5. Manuals for picking locks, building weapons, encrypting messages, etc.

Steganography



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