Lecture 9:
Security

Prof. Shervin Shirmohammadi

Need for Security

- Some people who cause security problems and why

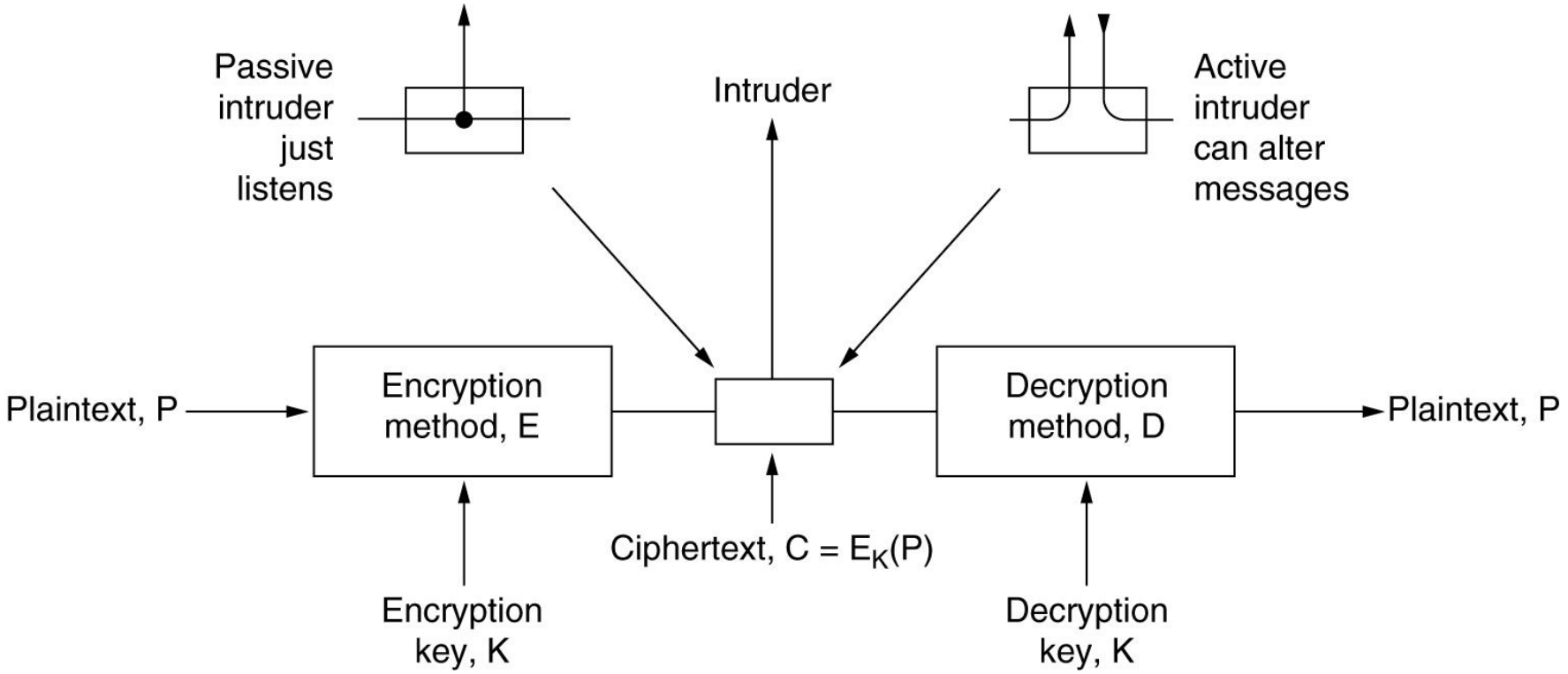
Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	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

Security Requirements

- Confidentiality: data should be accessible to authorized parties only.
- Integrity: data can only be modified by authorized parties.
- Authenticity: receiver should be able to verify the identity of sender.

An Introduction to Cryptography

- The encryption model for a symmetric-key cipher.



Passive Attacks

- Eavesdropping on transmissions to obtain information
- Release of message contents
  - Outsider learns content of transmission
- Traffic analysis
  - By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed
- Difficult to detect
- Can be prevented

Active Attacks

- Masquerade
  - Pretending to be a different entity
- Replay
- Modification of messages
- Denial of Service
- More easy to detect
  - Detection may lead to deterrent
- Hard to prevent

Substitution Ciphers

- Two types of Ciphers: substitution; transposition
- **Substitution**: Replace each symbol with another symbol
- A substitution cipher:
  - 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
  - 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
  - attack → QZZQEA
- Broken using statistical properties of the language.
  - English: e, t, o, a, n, i; th, in, er, re, an; the, ing, and, ion

Transposition Ciphers

- A **transposition** cipher:

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

One-Time Pads

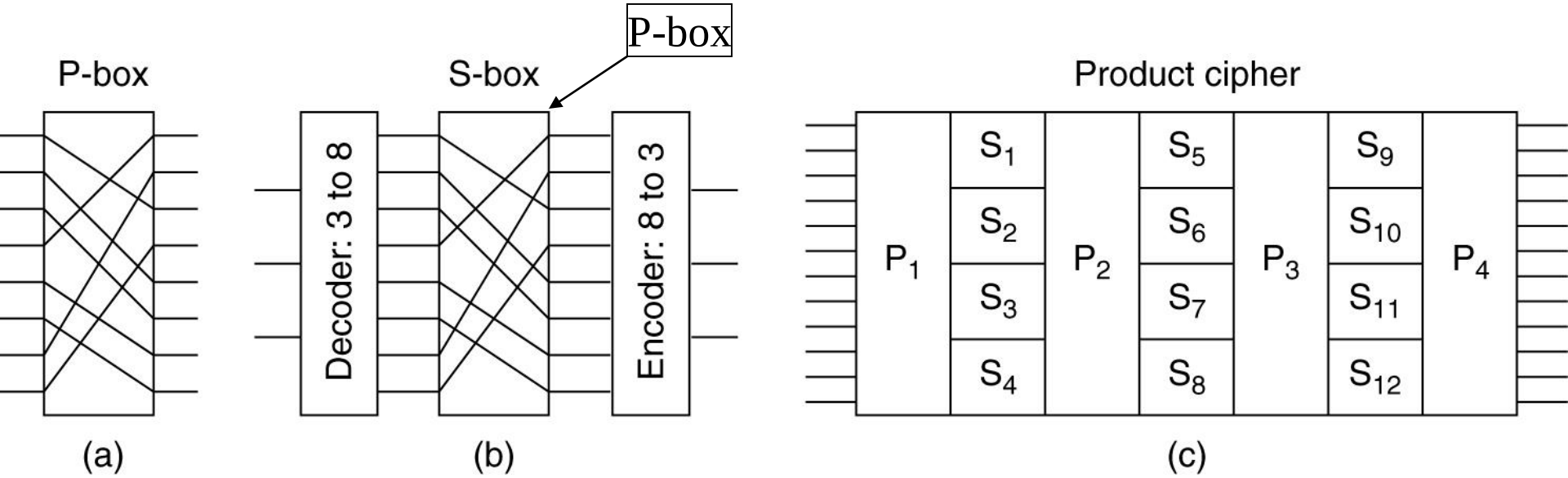
- Use a random series of bits (the key) with the same length of the message.
- XOR the message wit the key.

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

- Information theory: there is no information in the Ciphertext because any plaintext of the given length is a possible valid message.
- Is this a practical solution?

Product Ciphers

- Basic elements of product ciphers:
  - Permutation (P): changes the order of bits
  - Substitution (S): substitutes one pattern with another



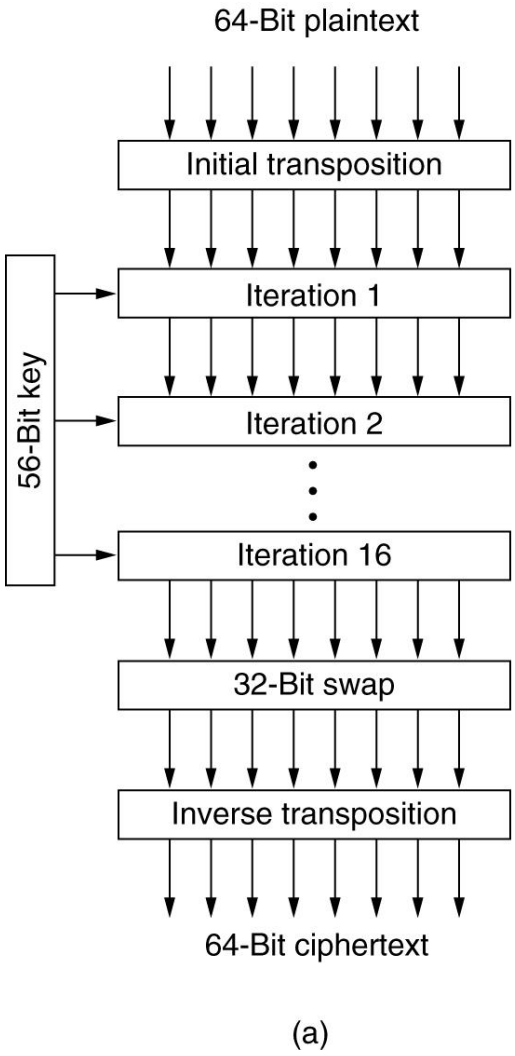
(a) P-box. (b) S-box. (c) Product

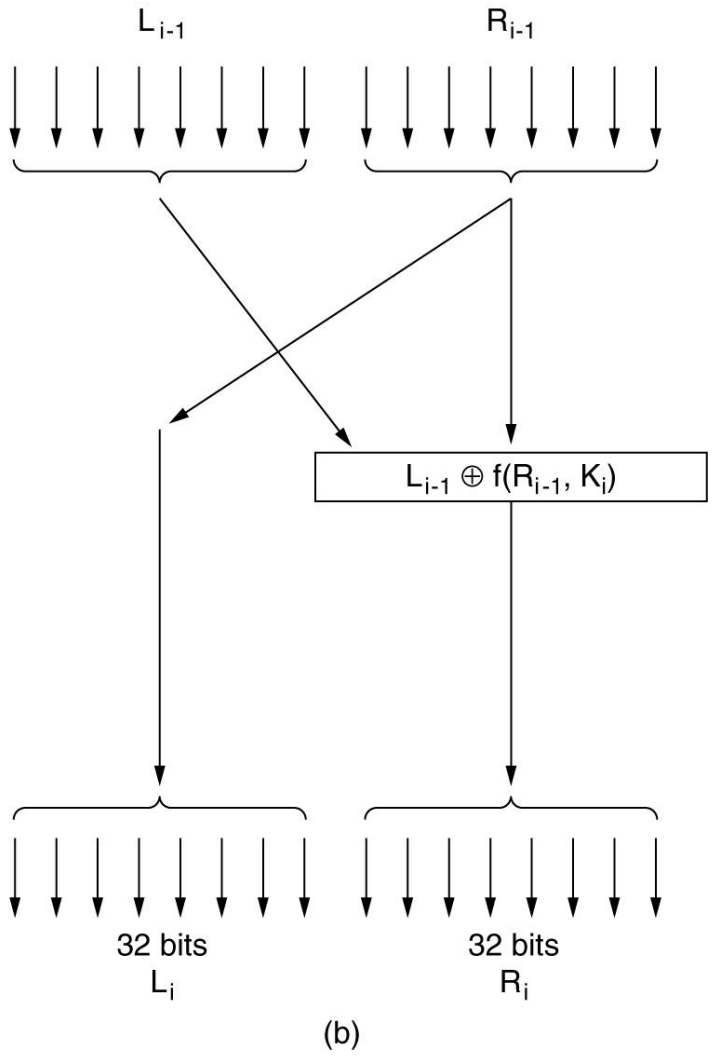
Symmetric-Key Algorithms

- Uses a shared secret key between the sender and the receiver.
- DES – The Data Encryption Standard
- AES – The Advanced Encryption Standard
- Each technique comes with a number of different Cipher Modes for specific situations.

Data Encryption Standard

- 1977 standard of NSA.
- Uses 56-bit keys.
- Takes in 64-bit plaintext segments.





(a) General outline (b) details of one iteration

DES problems

- 56-bit key too short; these days it can be broken by a sub-million dollar machine in under 1 day.
- NSA (National Security Agency) suspected of incorporating "secret design" to easily break DES for itself.

Table 21.1 Average Time Required for Exhaustive Key Search

Age of universe $\approx$ 20 billion years = 2×10^{10} years

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years

Advanced Encryption Standard (AES)

- 1997 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.

- A winner was chosen in 2001.

Rijndael

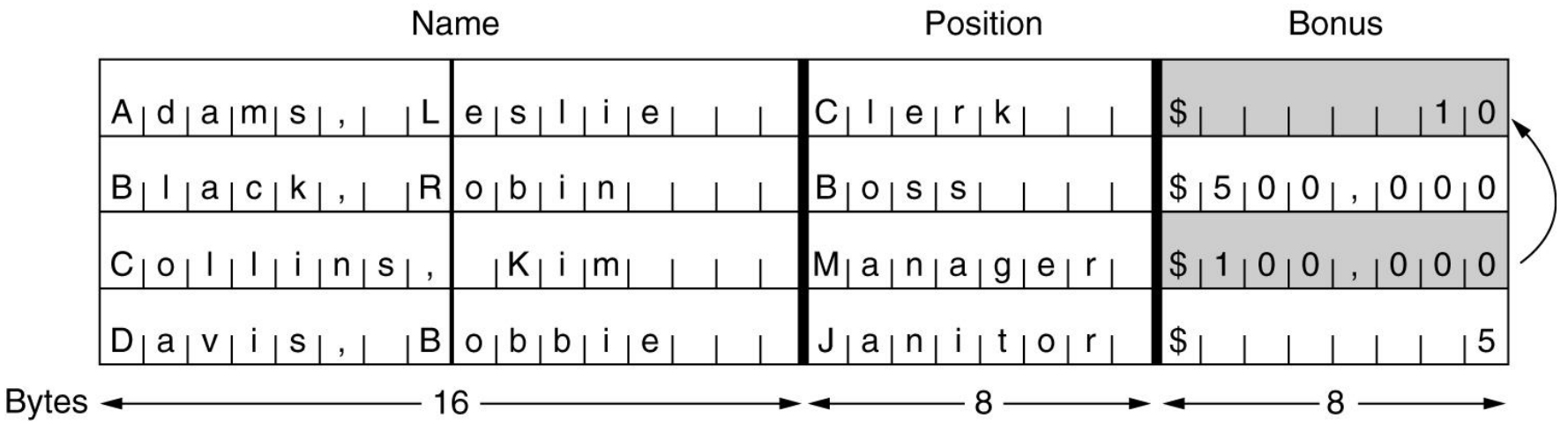
Winner:

Rijndael.

```
#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 */
}
```

Electronic Code Book Mode

- Cipher Modes add more security for specific situations.
- The plaintext of a file encrypted as 16 DES blocks:

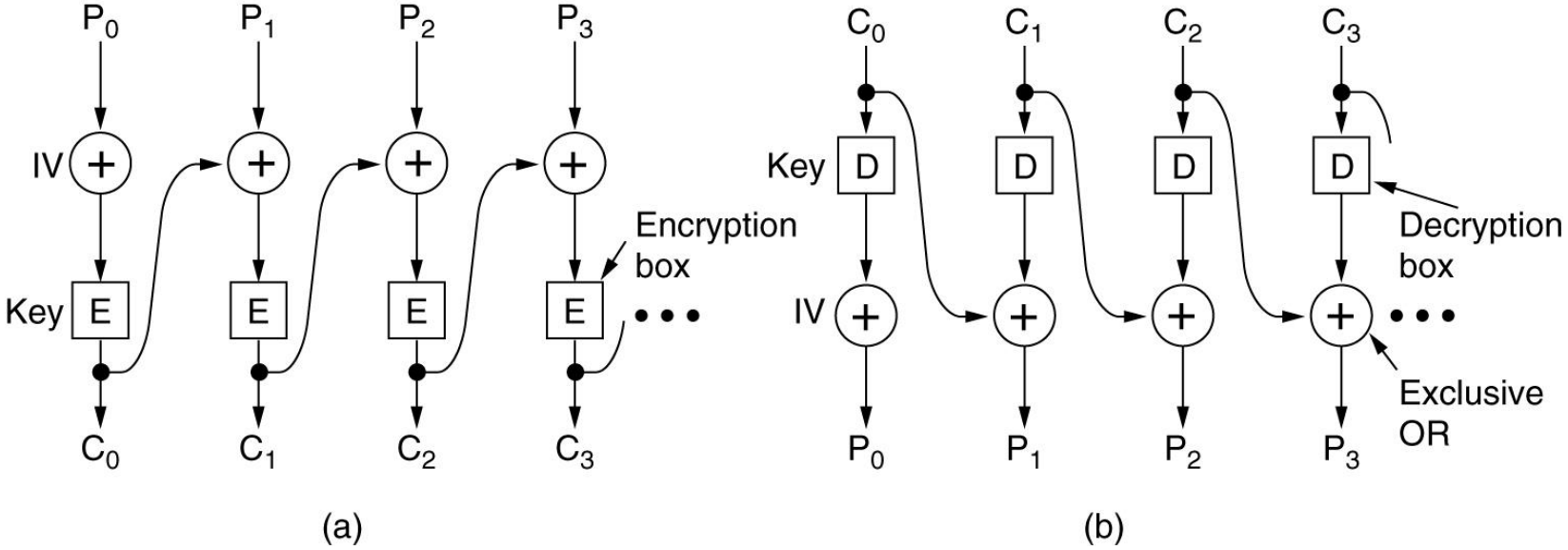


- Con: one can switch parts of ciphertext undetectably.

Cipher Block Chaining Mode

- Cipher block chaining.

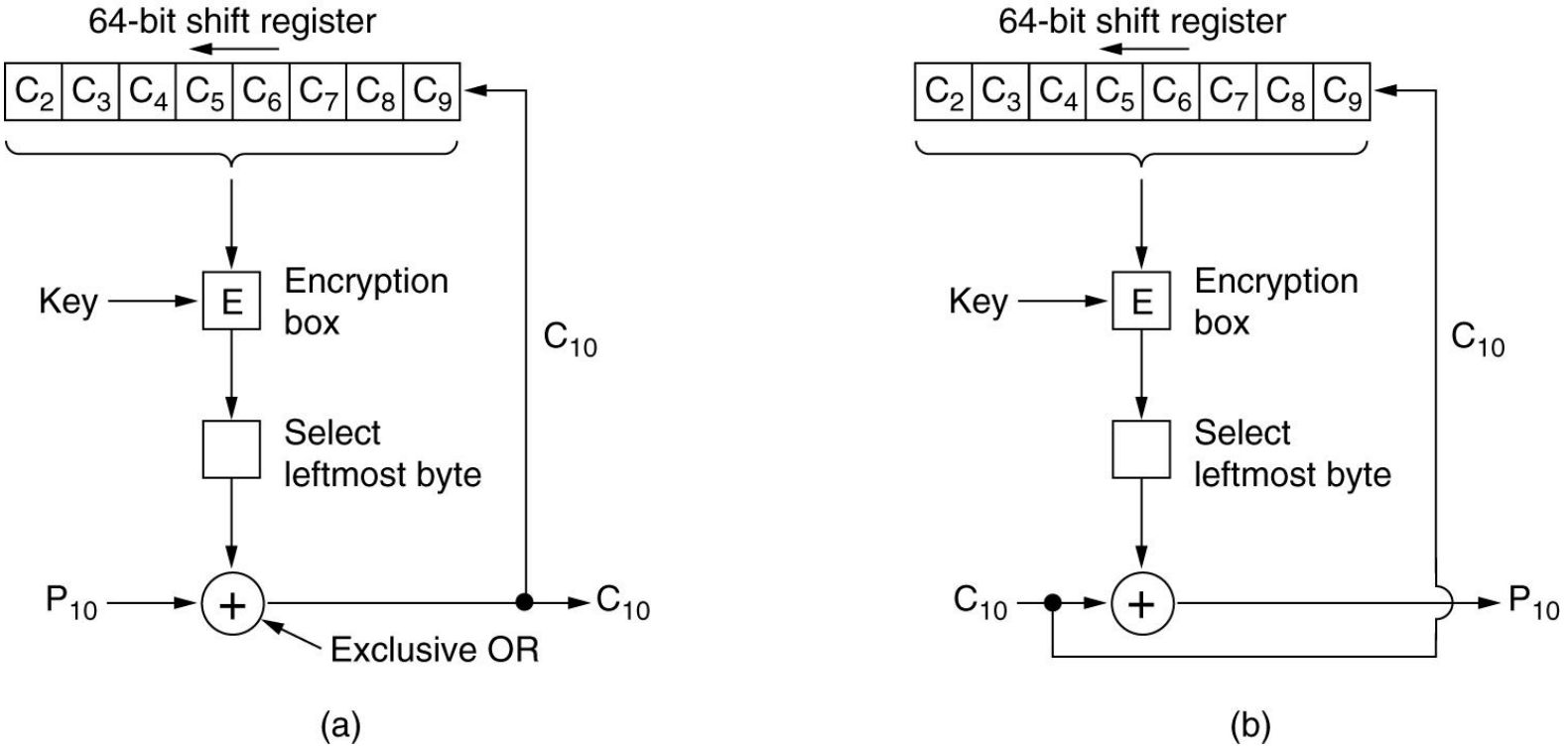
  (a) Encryption. (b) Decryption.



- Con: need to wait for complete C0 (typically 64-bit) before decryption can occur

Cipher Feedback Mode

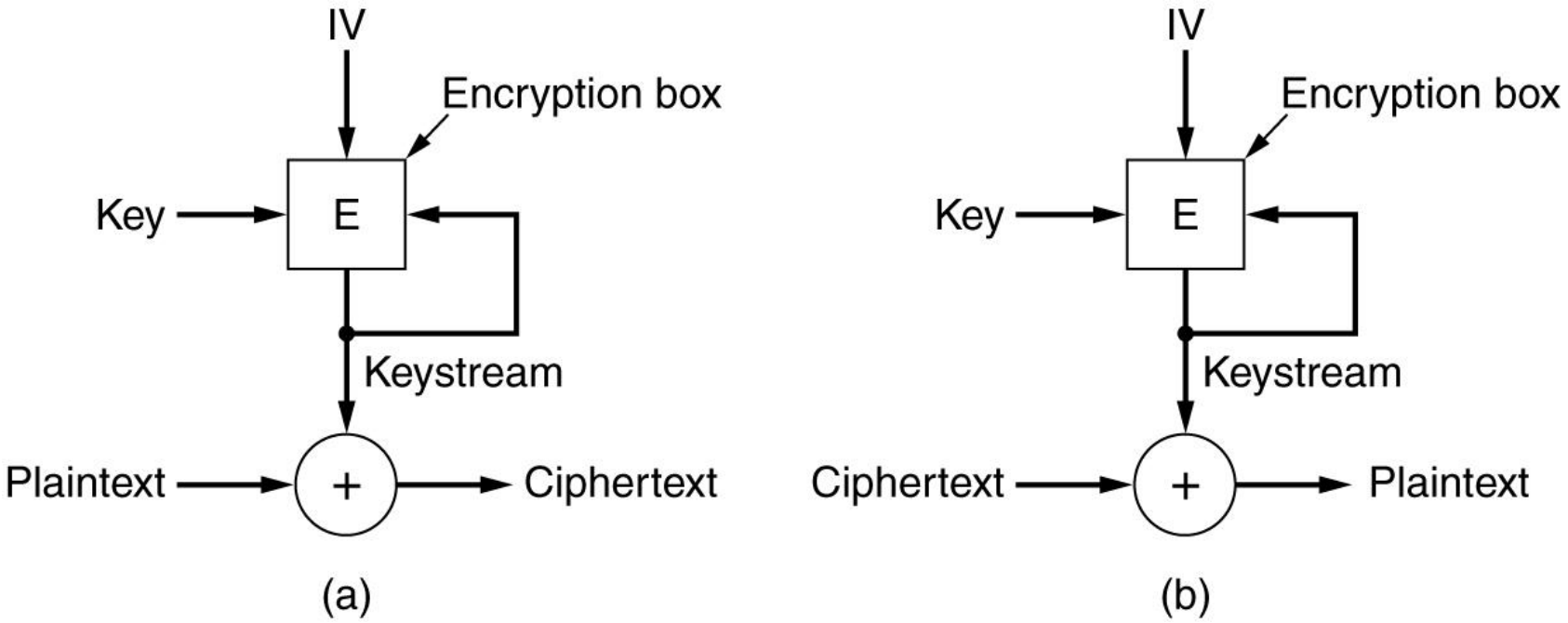
- (a) Encryption. (b) Decryption.



- Con: 1 bit error will lead to an 8-byte transmission error

Stream Cipher Mode & Counter Mode

- Stream Cipher Mode: (a) Encryption. (b) Decryption.



- Counter Mode: allows for Random Access - the ability to decrypt a specific part of the message.

Popular Implementations

- Some common symmetric-key cryptographic algorithms.

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

Public-Key Algorithms

- Also known as asymmetric algorithm.
- Uses a pair of keys, one public and one private.
- The idea is to give away your public key!
- Encrypt your messages using your recipient's public key; and only that recipient can decrypt it using its private key.
- Public-key algorithm can be used for both authentication and confidentiality; although differently for each.
- Main disadvantage: slow processing.

Rivest Shamir Adleman (RSA)

- Choose 2 large primes: p and q
- n = p × q and z=(p-1) ×(q-1)
- Choose a number d relatively prime to z
- Find e such that e × d = 1 mod z.
- $C = P^e \pmod n$ and $P = C^d \pmod n$
- Security is based on the difficulty of factoring large numbers (factoring a 500-digit number requires 10^{25} years on a computer with a 1 microsecond instruction time).

RSA

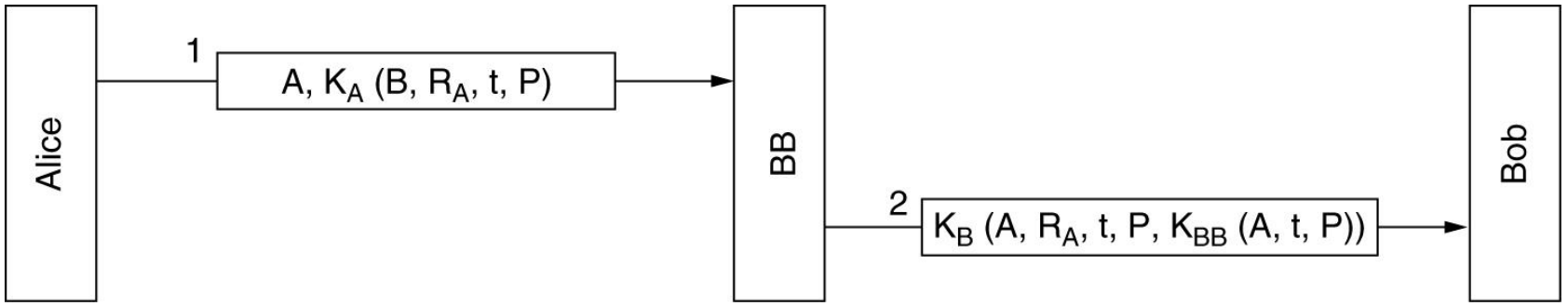
- How to provide:
  - authentication?
  - confidentiality?

Digital Signatures

- Similar to a signature on a document, a digital signature validates the authenticity of its signee.
- Upon receiving such digital signature, one should be able to prove, in a court of law, that the document is indeed signed by the person indicated by his/her signature.
- Can be accomplished using:
  - Symmetric-Key Signatures
  - Asymmetric-Key Signatures
  - Message Digests

Symmetric-Key Signatures

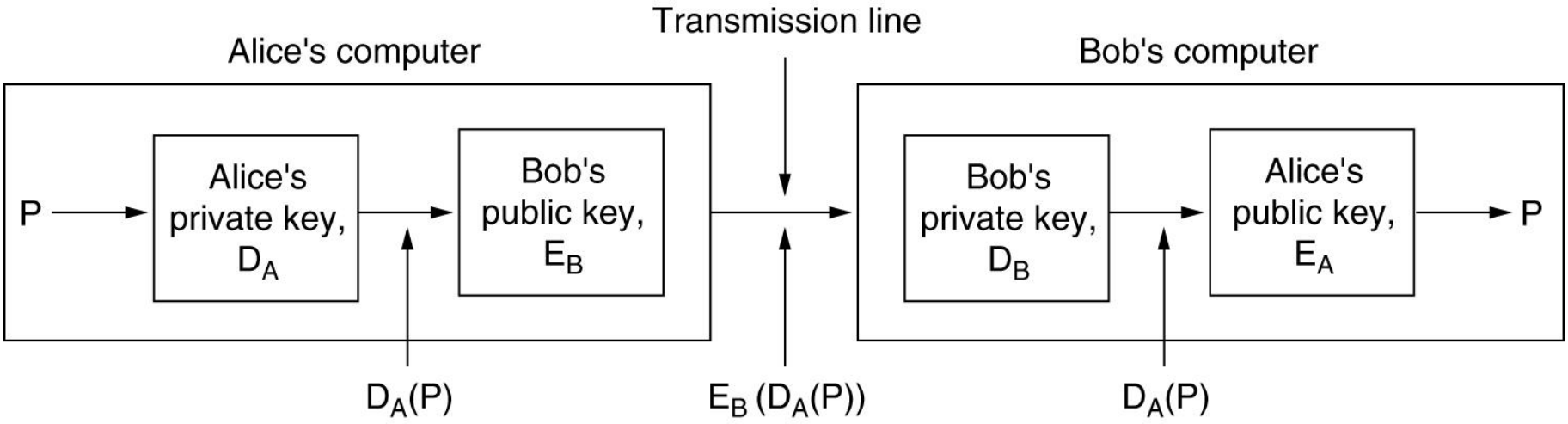
- Need a central authority (The Big Brother).
- Digital signatures with Big Brother:



- A: Alice, B: Bob, K: key, t: timestamp, R: random number.
- Drawbacks?
- Ways to cheat?

Public-Key Signatures

- Digital signatures using public-key cryptography.
- This example also provides confidentiality.



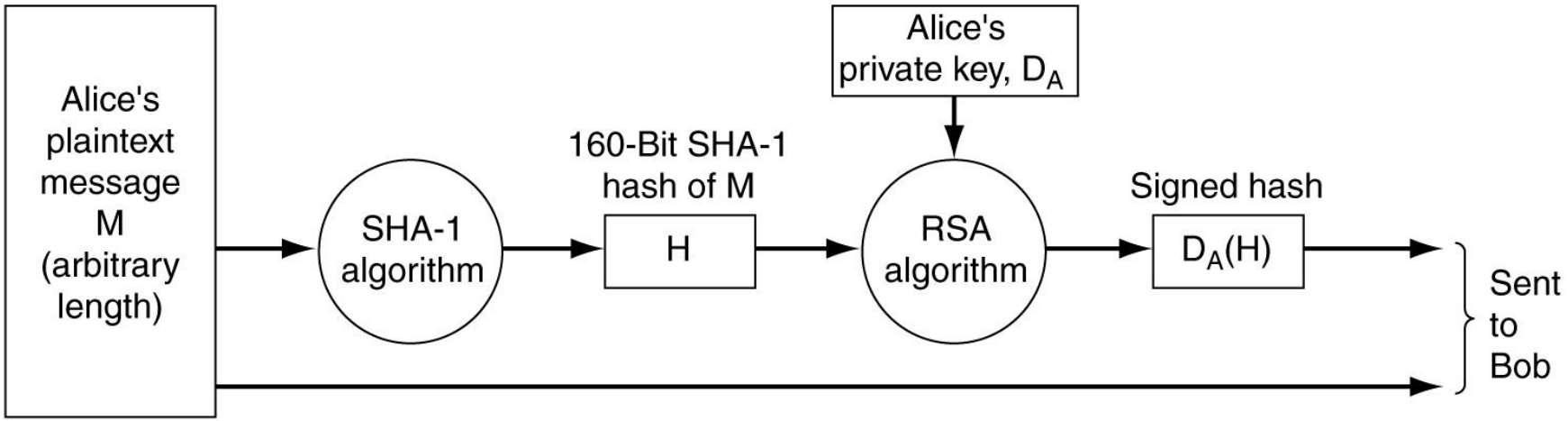
- Problem?

Message Digests

- Creates a unique, fixed-sized, one-way digest using the message. ① ② ③
- MD5: takes 512 bit blocks and gives a 128-bit digest
  - Essentially a hash converter.
- Digital signatures using message digests and public-key encryption:

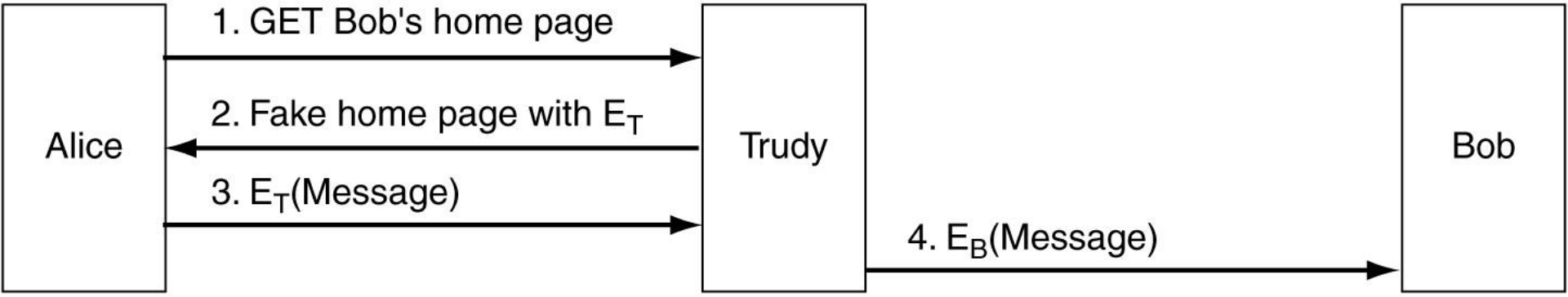
SHA-1

- SHA: Secure Hash Algorithm
- Takes 512 bit blocks and gives a 160-bit digest
- Use of SHA-1 and RSA for signing non-secret messages.



Cheating Public-Key Encryption

- Man-in-the-middle attack:
- A way for Trudy to subvert public-key encryption:



PK Management: Certificates

- Who to get the certificate from?
  - Certificate Authority (CA)
- A possible certificate and its signed hash Issued by a CA

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

Providers

- 2018 providers

Provider	Market share
IdenTrust	39.7%
Comodo	34.9%
DigiCert	12.3%
GoDaddy	7.2%
GlobalSign	3.5%
Certum	0.7%
Actalis	0.3%
Entrust	0.3%
Secom	0.3%
Let's Encrypt	0.2%
Trustwave	0.1%
WISeKey Group	0.1%
StartCom	0.1%
Network Solutions	0.1%

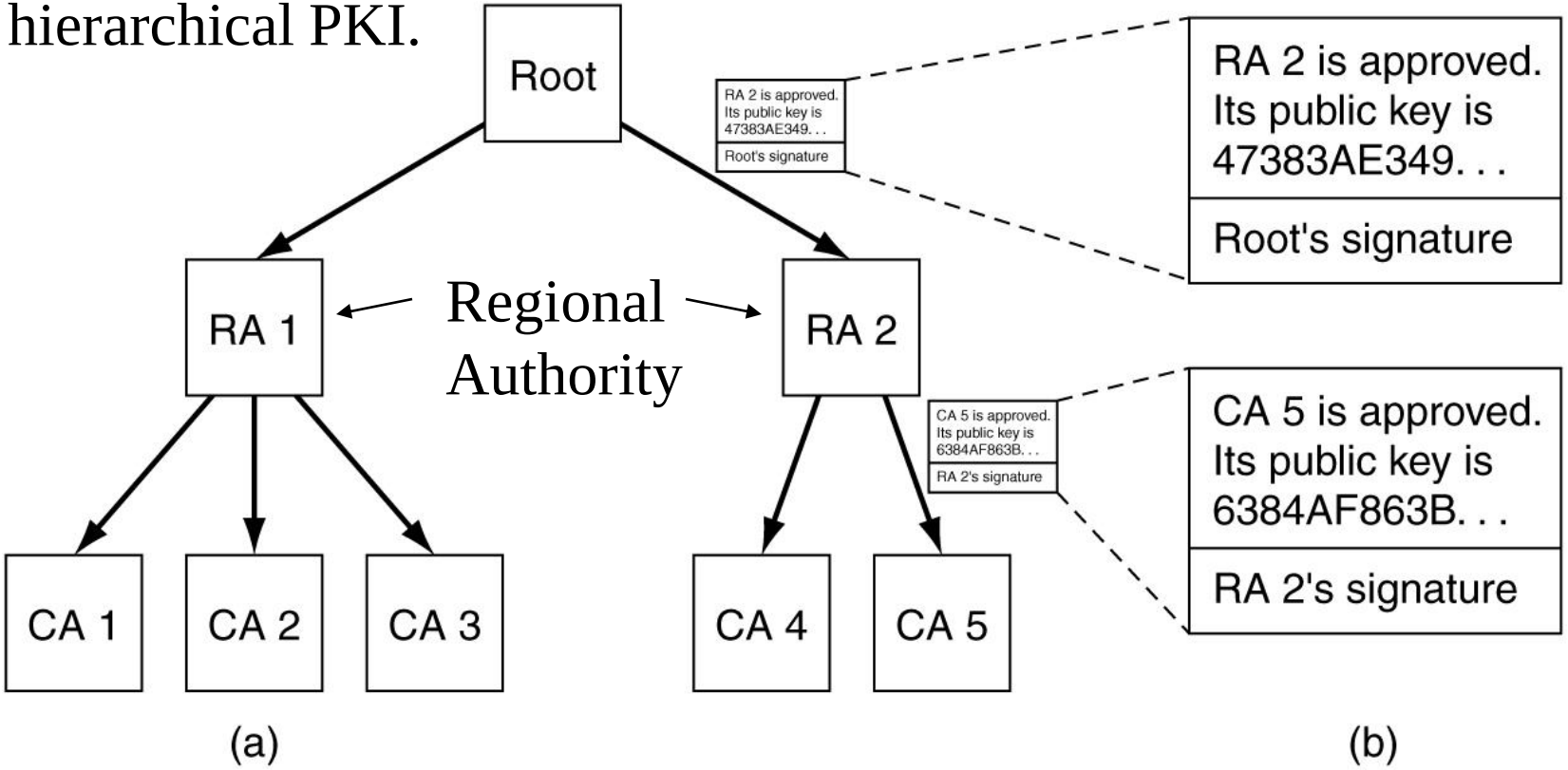
PK Management: X.509

- What format to use for the certificate?
  - Most common format: **ITU X.509**
- The basic fields of an X.509 certificate:

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)

PK Management: Public-Key Infrastructures

- Obviously we can't have one server for the CA for the whole planet
  - Scalability problems
- Solution: use multiple servers, but make sure there is a hierarchical infrastructure to maintain integrity and reliability.
- A hierarchical PKI.



Steganography

- The science of hiding messages.
- Greek for "covered writing".

3rd March

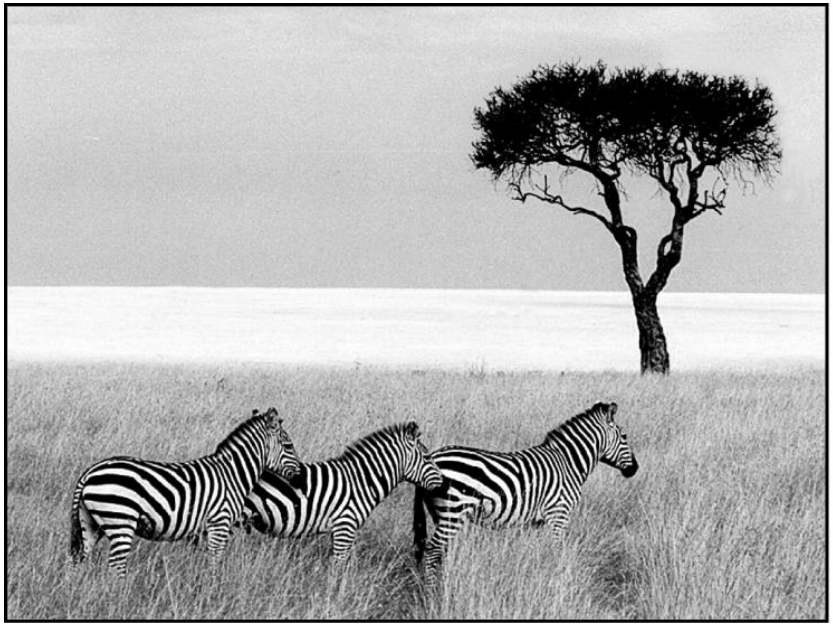
Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

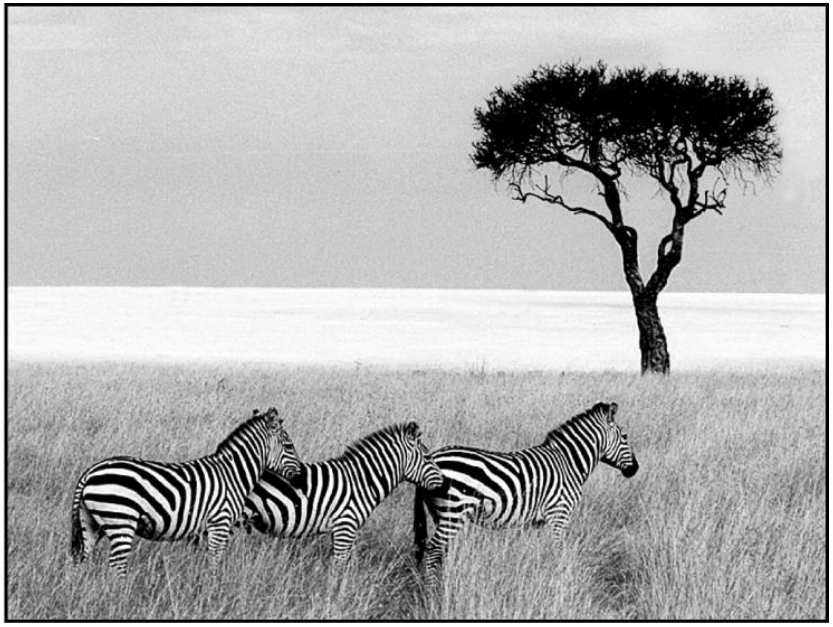
Sincerely yours,

Figure 2.8 A Puzzle for Inspector Morse
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Steganography Example



a



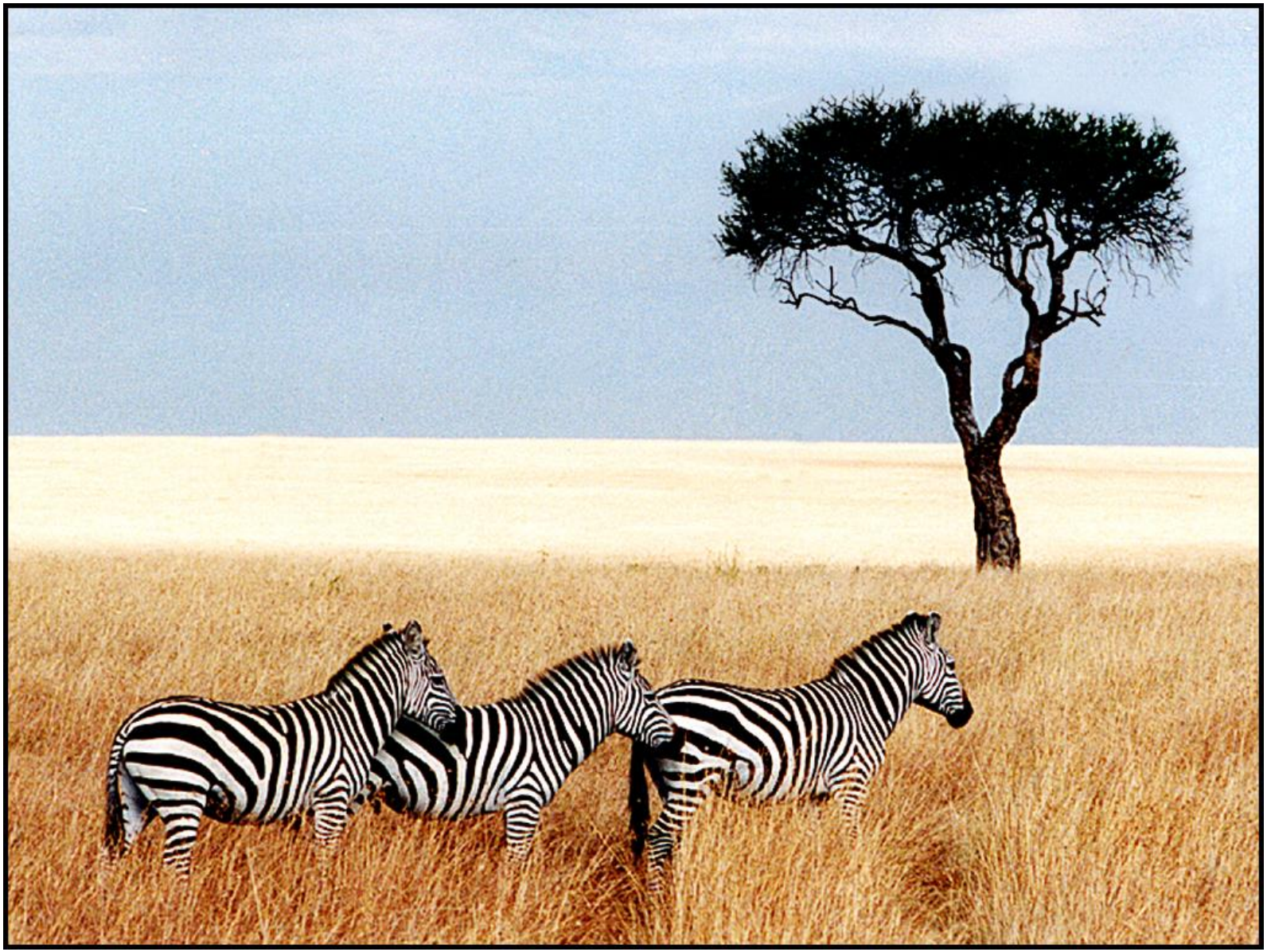
b

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

Steganography (original picture)

Size:

2,359,352 B



Steganography (encoded picture)

Size:

2,359,352 B

Contains full text of:

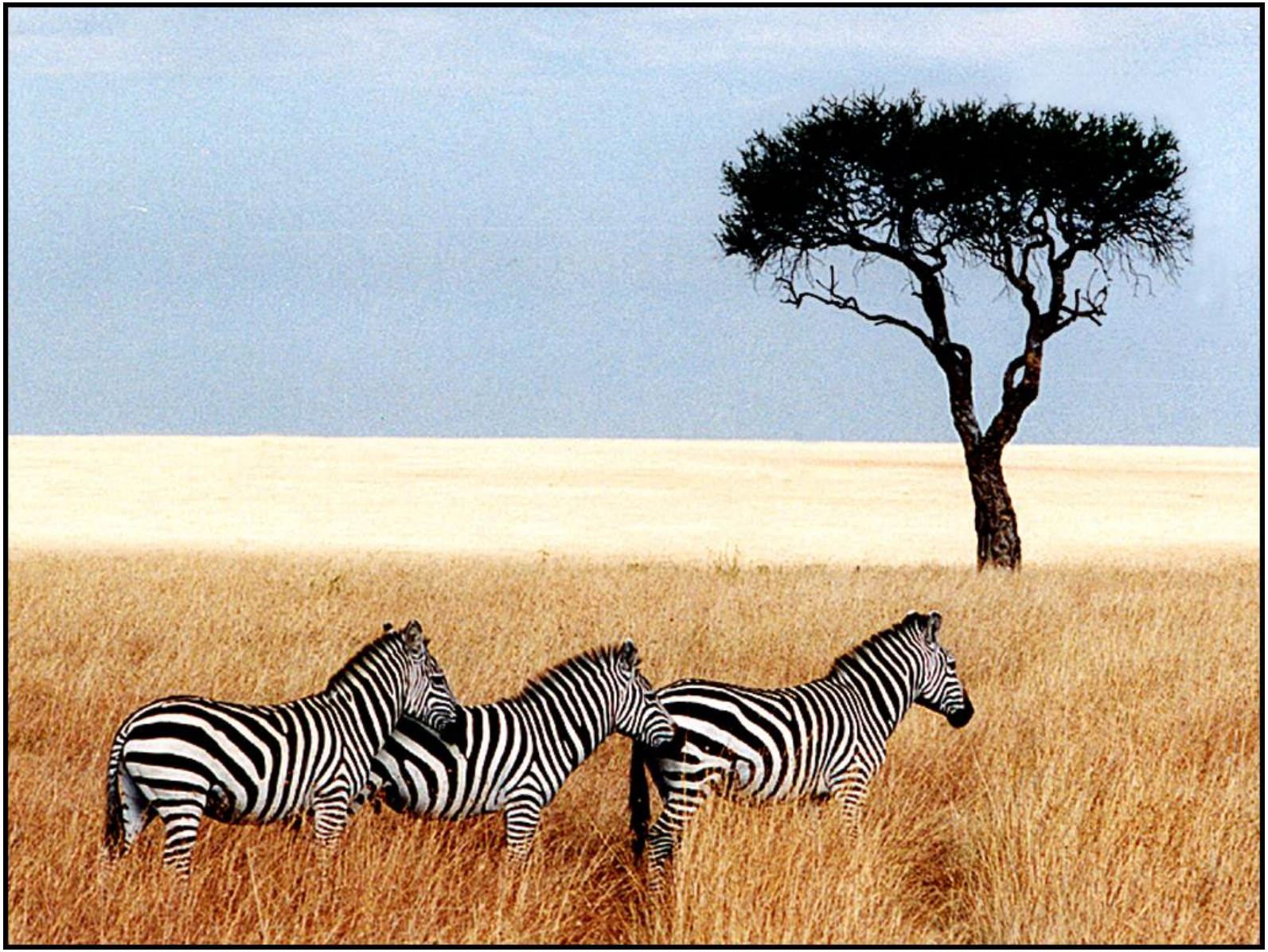
Hamlet,

King Lear,

Macbeth,

The Merchant of Venice,

Julius Caesar.



Network Security

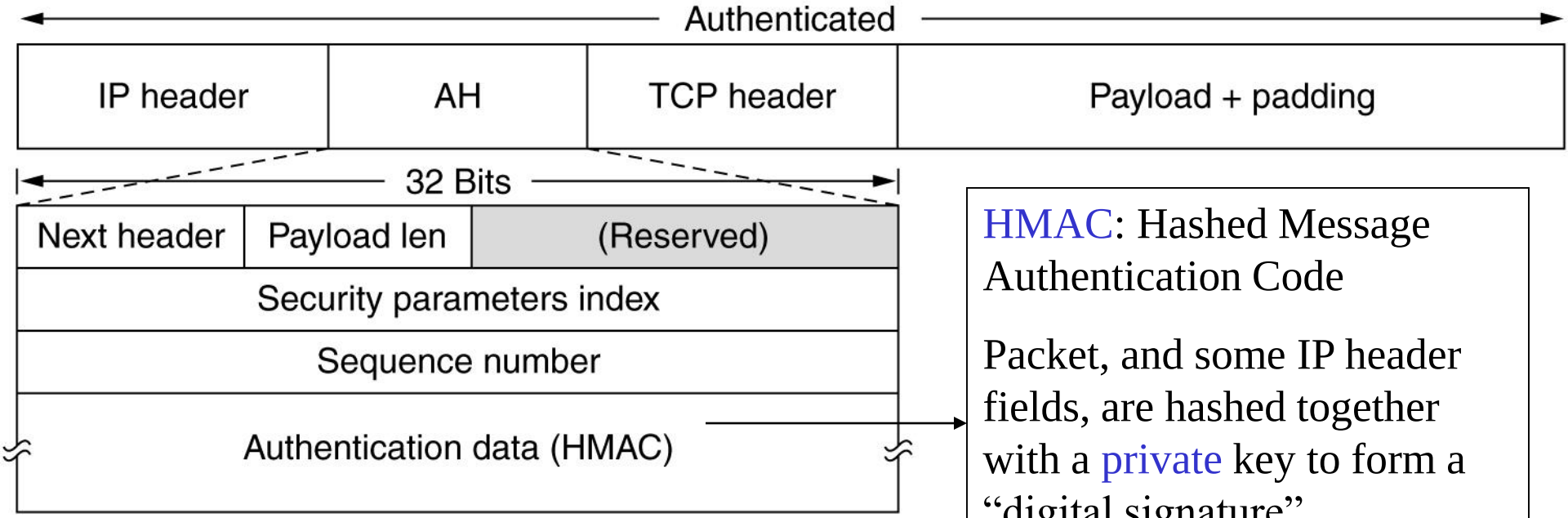
- Why secure communications?
  - 1999, Swedish hacker breaks into Hotmail, exposing the emails of any user ID.
  - Russian hacker breaks into an e-commerce site, stealing 300,000 credit card numbers. Upon not being taken seriously by the site on his $100,000 ransom request, he exposes the numbers in public, causing millions of dollars in damages.
  - 23-year old California student fakes an email from Emulex Corporation reporting they have a huge quarterly loss and the CEO is resigning. After selling his stocks, he sends the email causing a 60% drop in the stock price and $2billion stockholder loss within the hour, making a quarter million dollars himself before being arrested.
  - …
- IPsec
  - Secure IP, providing authentication and/or encryption at the networking level.
- SSL (Secure Socket Layer)
  - Provides security at the transport layer.
- Firewall
  - Protecting networks from unwanted access
- VPN (Virtual Private Network)
  - Using the “normal” Internet for secure communication between private subnets.

IPsec

- A protocol used to enhance IP with security.
- Establishes a simplex *connection*, known as Security Association (SA).
  - Unlike normal IP, that is connectionless.
  - It's a simplex connection, so we'd need two SAs for a full-duplex secure connection.
- Provides Authentication Header (AH), and Encapsulating Security Payload (ESP).
- AH is used for authentication, ESP is used for authentication and confidentiality.
- Used in transport mode (host-to-host), or tunnel mode (gateway-to-gateway).

IPsec AH

- The IPsec authentication header in transport mode for IPv4.

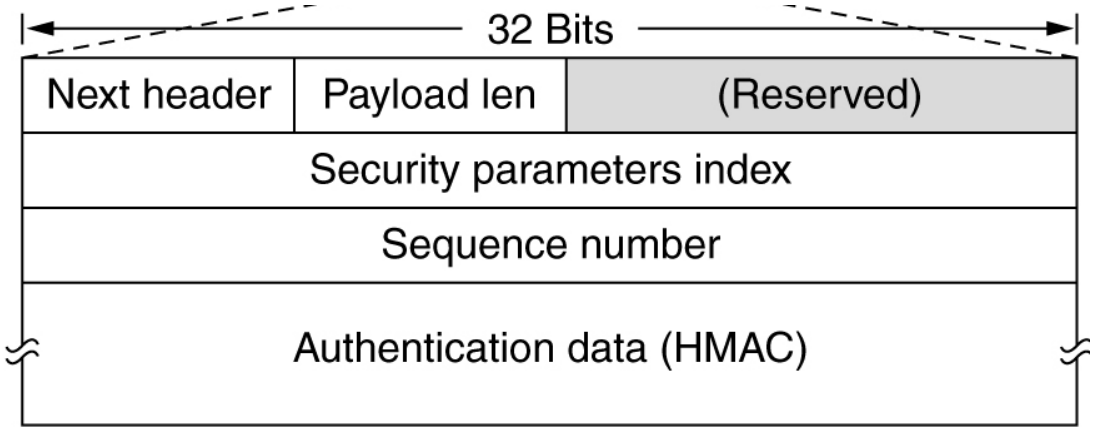


HMAC: Hashed Message Authentication Code

Packet, and some IP header fields, are hashed together with a private key to form a "digital signature".

- How to let the receiver know that this packet is an IPsec packet?
  - Set the *protocol* field in the IP header to be IPsec (value 51)

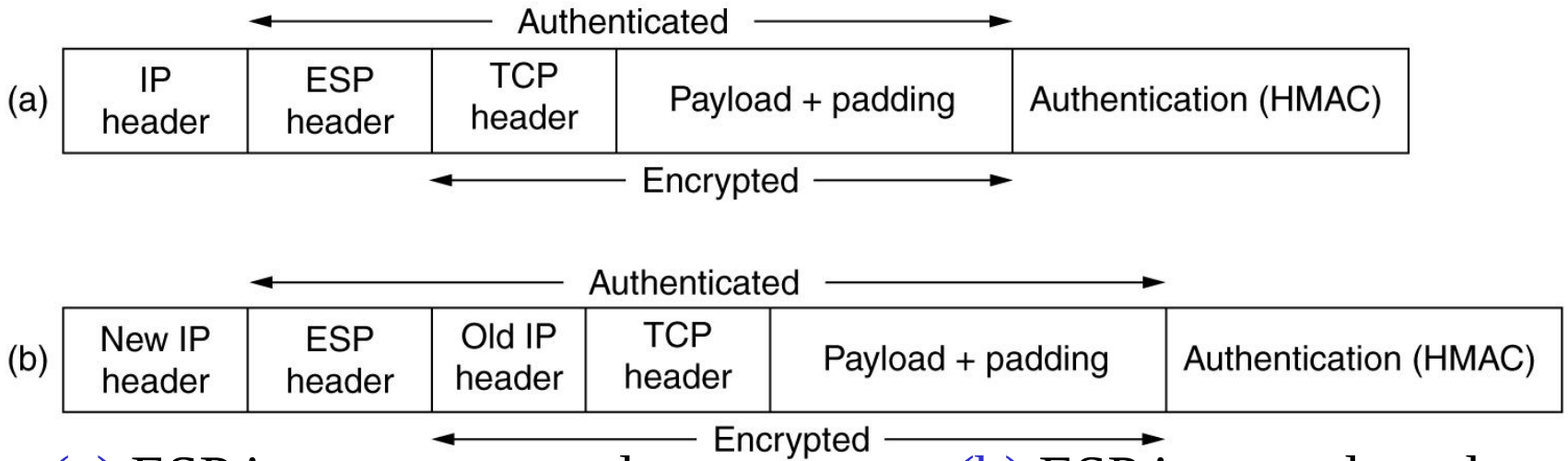
AH fields



- Next Header: the actual "protocol" field in the IP header that was replaced with 51.
- Payload Length: length of AH (in counts of 32-bits)
- Security parameters index: connection identifier, indicates the connection that this packet belongs to.
  - Each connection has its own key. Therefore the receiver knows, from this identifier, which key to use.
- Sequence number: used not for ordering (like TCP) but to prevent replay attacks!
  - Wrap-around is not allowed.

IPsec ESP

- Used for both authentication and confidentiality.
- ESP header has fields similar to the AH header, plus some more for encryption purposes.
- HMAC is a trailer (rather than a header) due to easier hardware implementation (like Ethernet's CRC).



(a) ESP in transport mode. (Host to host)

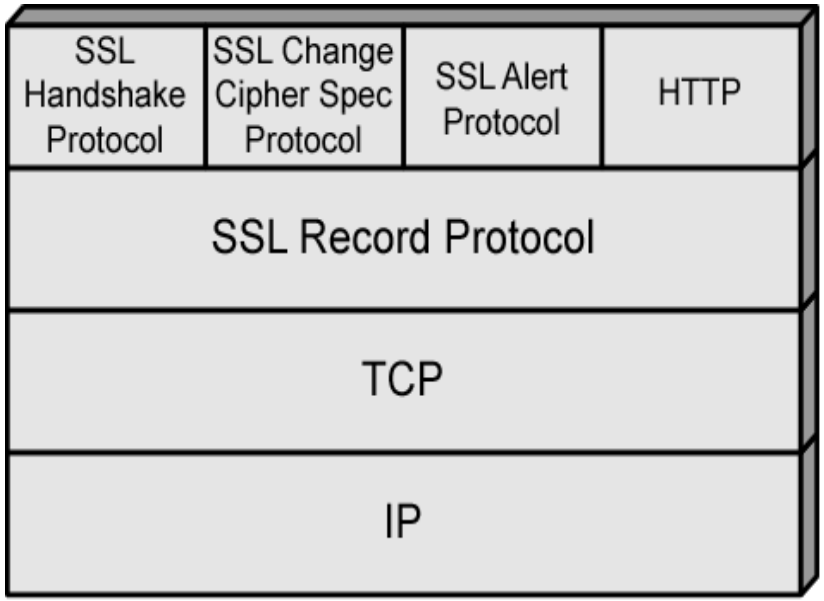
(b) ESP in tunnel mode. (gateway to gateway)

Transport Layer Security (TLS)

- History:
  - Secure Socket Layer (SSL) originally proposed by Netscape corporation in 1995.
  - IETF took over in 1996, coming up with Transport Layer Security (TLS) defined in RFC 2246.
  - Last version of SSL (SSL 3.0) was deprecated in 2015.
- Set of protocols that rely exclusively on TCP.
- Current applications: HTTPS, SSH, SFTP, …
- Two implementation options:
  - Part of underlying protocol suite
    - Transparent to applications
  - Embedded in specific packages
    - E.g. Chrome and Microsoft Edge and most Web servers

SSL Architecture

- SSL uses TCP to provide reliable end-to-end secure service
- Two layers of protocols
  - Record Protocol provides basic security services to various higher-layer protocols
  - Three higher-layer protocols
    - Handshake Protocol
    - Change Cipher Spec Protocol
    - Alert Protocol



SSL Connection and Session

- Connection
  - Transport that provides suitable type of service
  - Peer-to-peer
  - Transient
  - Every connection associated with one session
- Session
  - Association between client and server
  - Created by Handshake Protocol
  - Define set of cryptographic security parameters
  - Used to avoid negotiation of new security parameters for each connection
- Maybe multiple secure connections between parties
- May be multiple simultaneous sessions between parties
  - Not used often in practice

Handshake Protocol

- Used to establish a session between the two parties.
- Authenticates parties, and negotiates encryption and MAC algorithm and cryptographic keys
- Used before any SSL connection is established application data sent.
- Consists of 4 phases (see next slides).

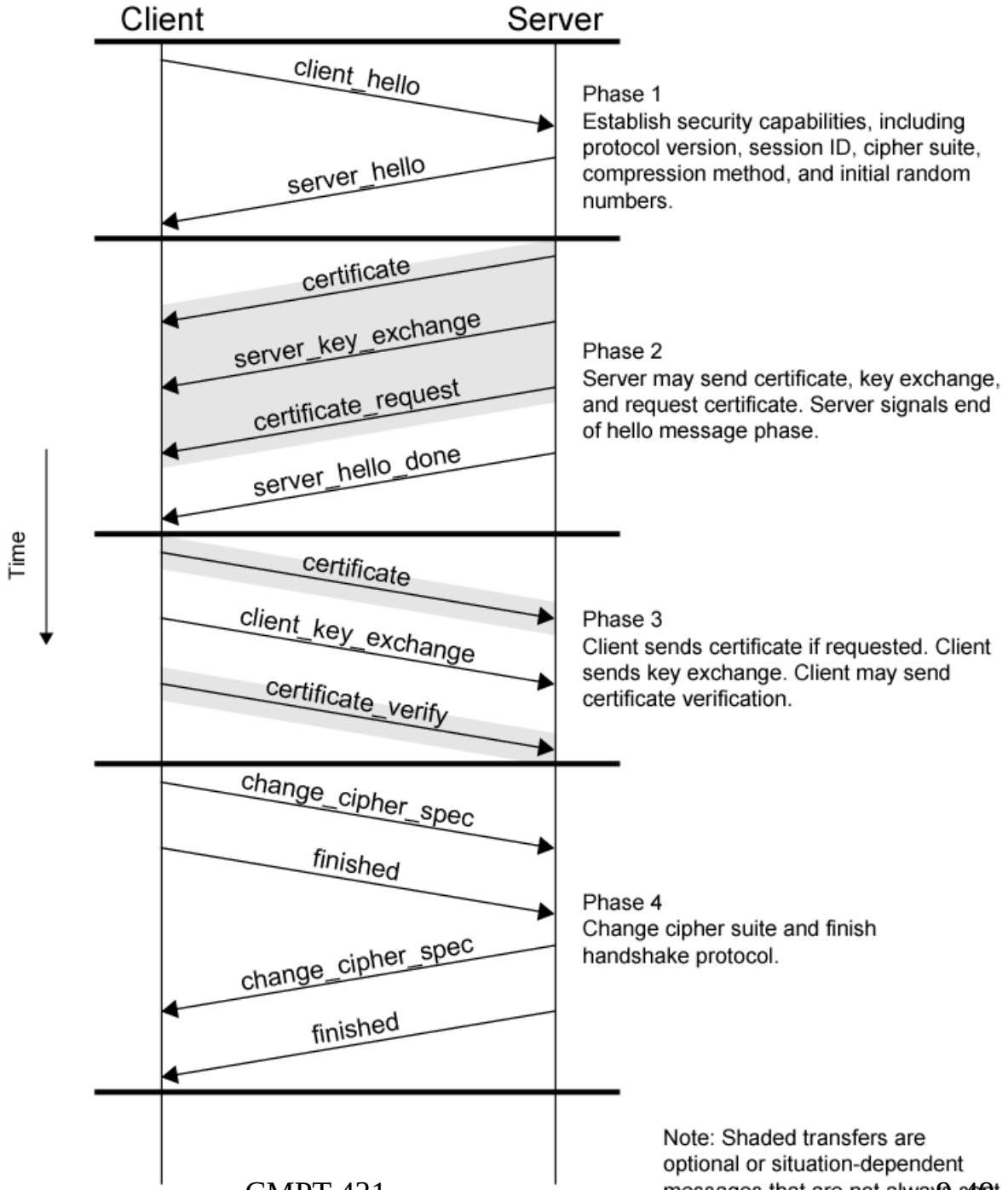
Phase 1 Initiate Connection

- Client sends hello message with the following info:
  - Version
    - Highest SSL version understood by client
  - Random
    - Client-generated random structure used during key excahnge.
    - Used during key exchange to prevent replay attacks
  - Session ID
    - Variable-length
    - Nonzero indicates client wishes to update existing connection or create new connection on session
    - Zero indicates client wishes to establish new connection on new session
  - CipherSuite
    - List of cryptographic algorithms supported by client
    - Each element defines key exchange algorithm and CipherSpec
  - Compression Method
    - Compression methods client supports
- Server responds with hello with the same parameters as above.

Phase 2, 3, and 4

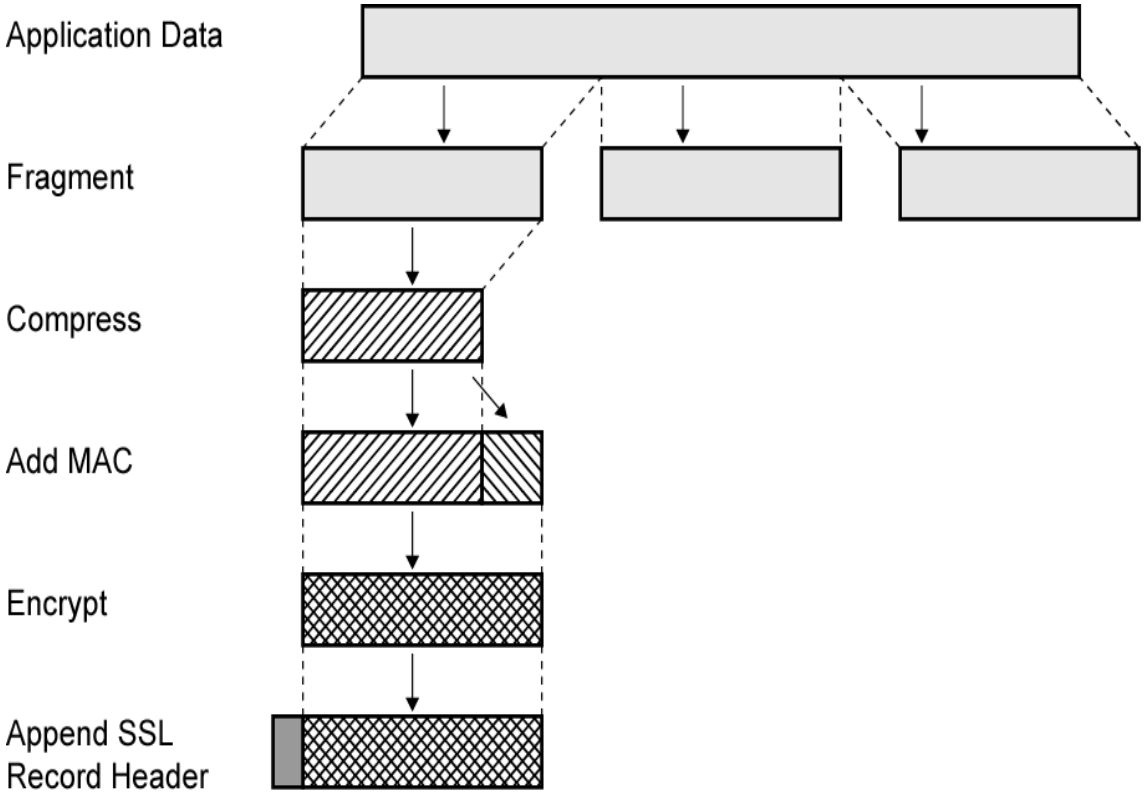
- Phase 2 depends on underlying encryption scheme
  - Key exchange by the server
  - Certificate sent by server
- Final message in Phase 2 is server_done
  - Required
- Phase 3
  - Upon receipt of server_done, client verifies certificate if required and check server_hello parameters
  - Client sends messages to server, depending on underlying public-key scheme
- Phase 4
  - Parties exchange change_cipher_spec message to confirm cipher specs, and signal finish to finish the handshake.

Handshake Protocol Action



SSL Record Protocol

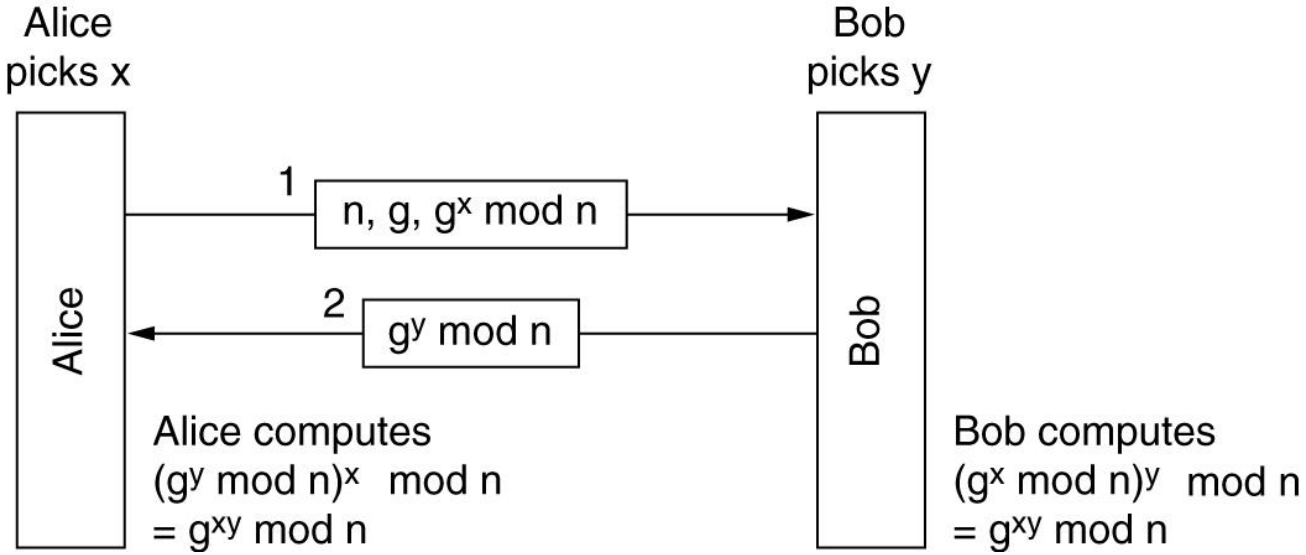
- Used for
  - Confidentiality
    - Uses shared secret key exchanged during handshake for encryption
  - Authentication
    - Uses shared secret key exchanged during handshake to create Message Authentication Code (MAC)
- Each upper-layer message fragmented into 16 Kbytes (16384 bytes) or less.
- Compression optionally applied



Change Cipher Spec Protocol and Alert Protocol

- Change Cipher Spec Protocol
  - A Single message consisting of a single byte. If it's 1, the pending state is copied into the current sate
  - used to change the cipher spec on a given connection.
- Alert Protocol
  - A Two-byte message:
  - First byte warning (1) or fatal (2)
    - If fatal, SSL immediately terminates connection
    - Other connections on session may continue
    - No new connections on session
  - Second byte indicates specific alert

The Diffie-Hellman Key Exchange



Alice picks: x=3, n=11, g=25

Alice sends: 11, 25, $(25^3 \bmod 11)=5$

Bob picks: y=4

Bob sends: $(25^4 \bmod 11)=4$

Alice ends up with: $4^3 \bmod 11 = \boxed{9}$

Bob ends up with: $5^4 \bmod 11 = \boxed{9}$

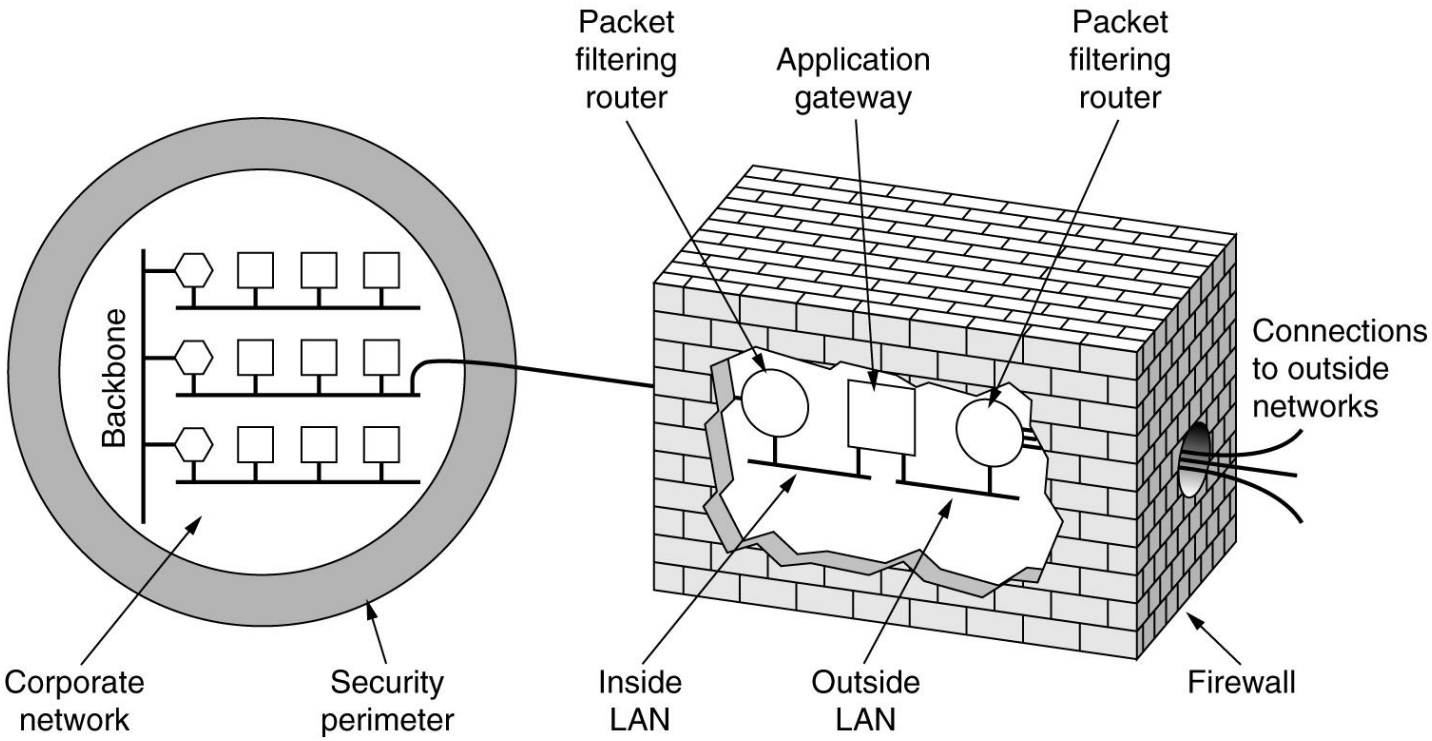
Remember:

$a^x \bmod b = c$

has an infinite number of answers for x

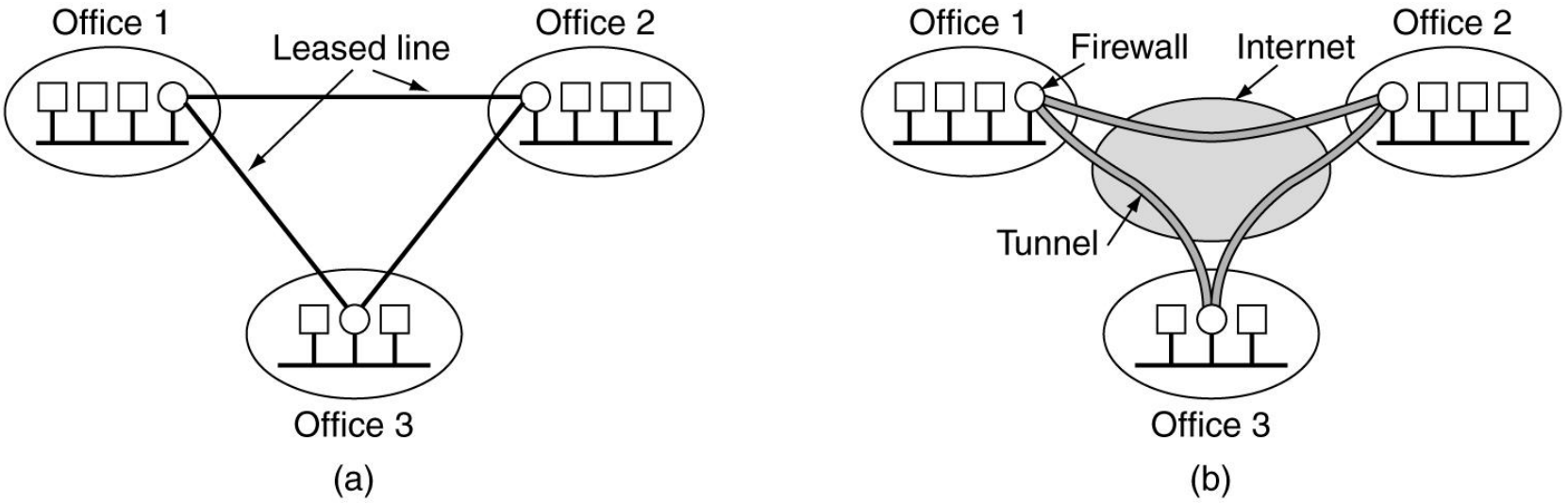
Firewall

- Prevents unwanted access to a subnetwork.
- Typically Consists of a packet filter and an application gateway.
  - **Packet filter**: filters packet based on IP, TCP, or UDP specs, including port numbers allowed, policies for incoming/outgoing packets, hosts allowed, …
  - **Application gateway**: filters application data (e.g., catching spam in email).



VPN: Virtual Private Network

- Many organizations are distributed geographically.
- Problem: how to send information between its subnetworks in a seamless manner?
- Solution 1: lease private lines (disadvantage of this approach?)
- Solution 2: use the regular Internet connections with VPN
- A natural implementation: use IPsec with firewalls at each subnet.



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