# NETWORK SECURITY

# Cryptography

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

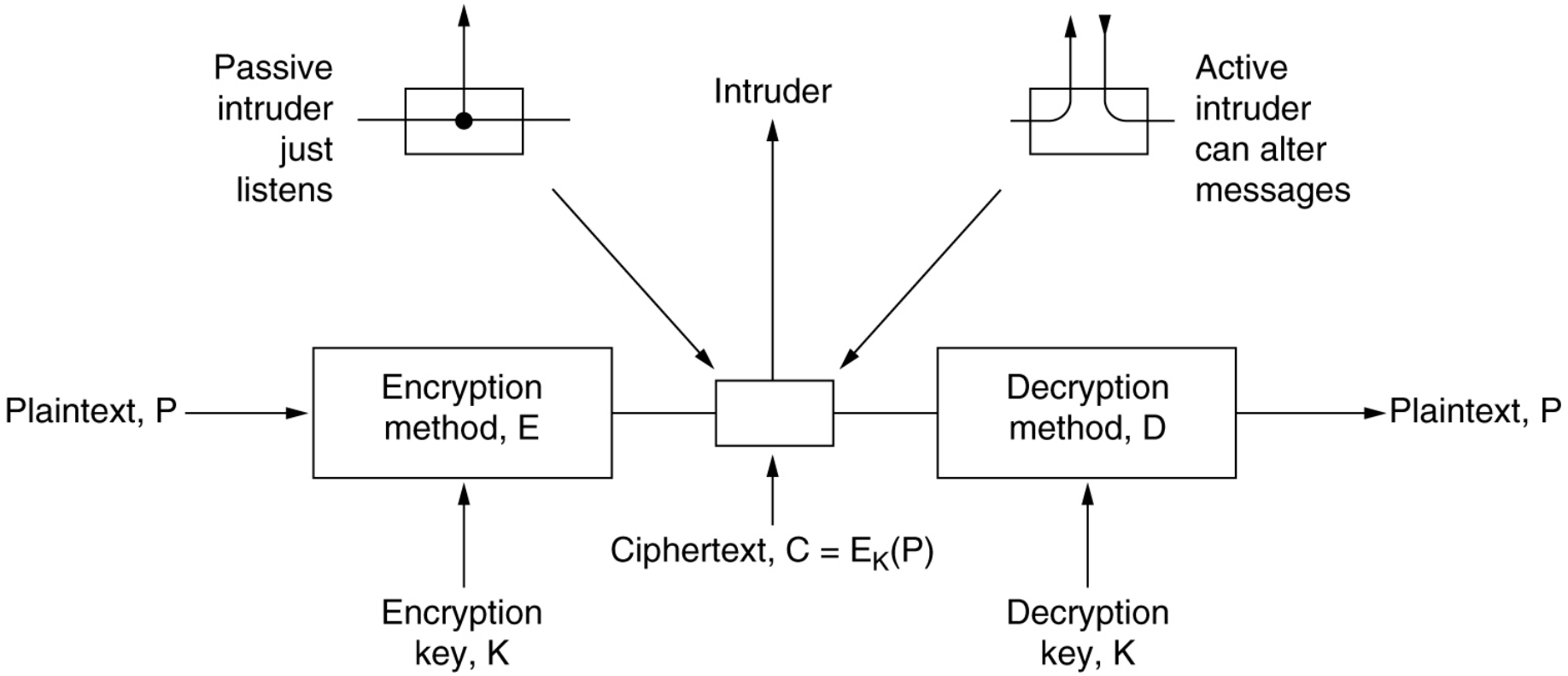
# Need for Security

- 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 |

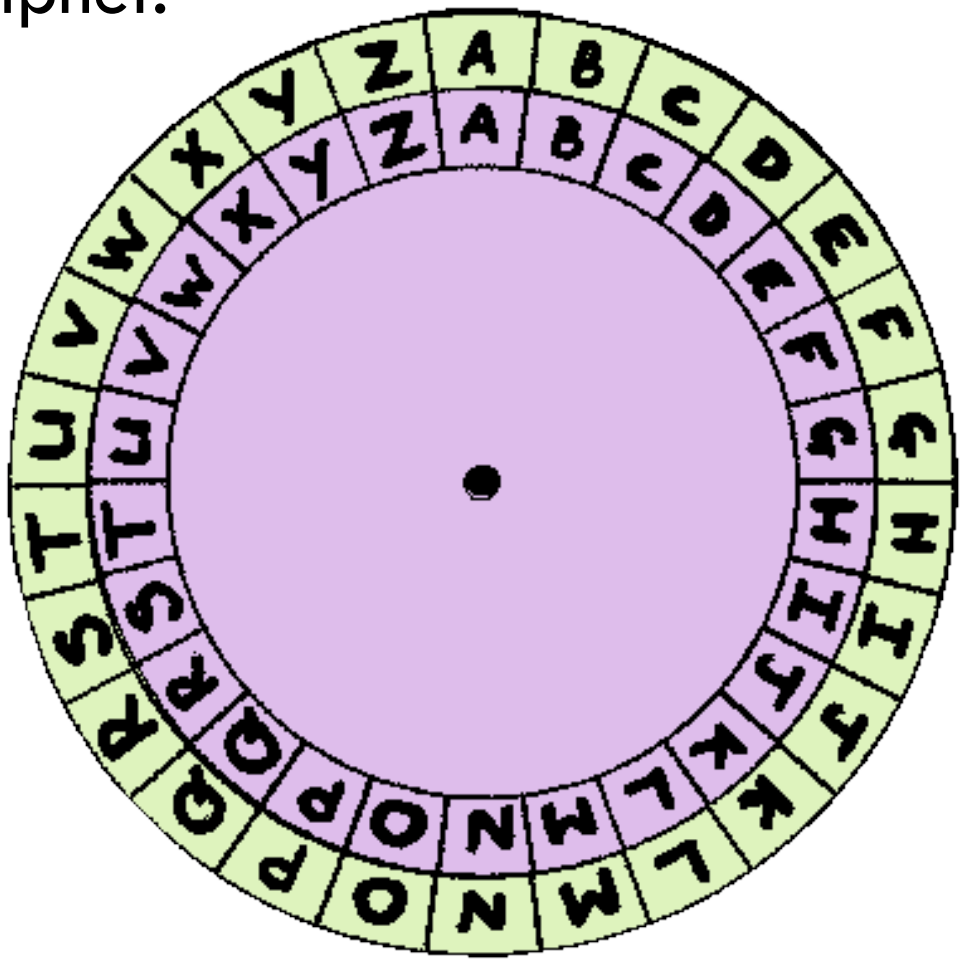
# An Introduction to Cryptography

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



# Ciphers

- Caesar's Cipher.

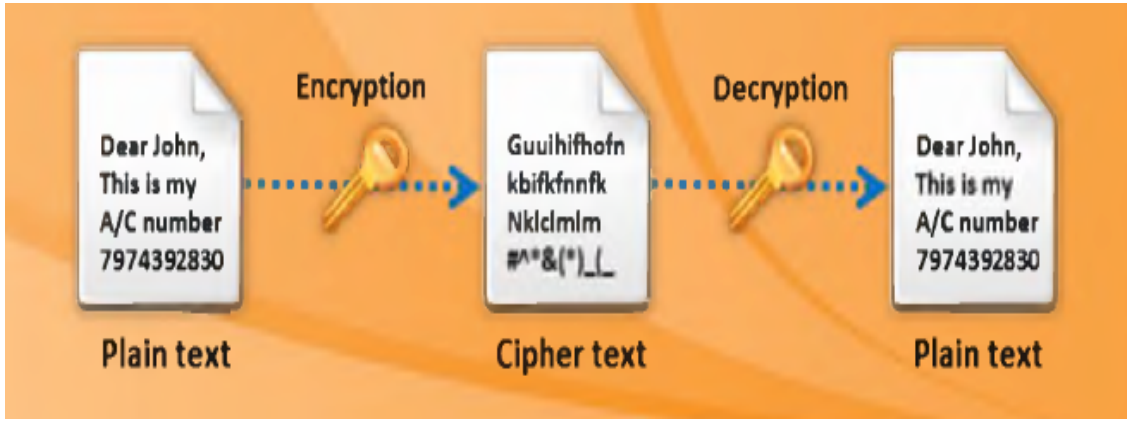


# One-Time Pads

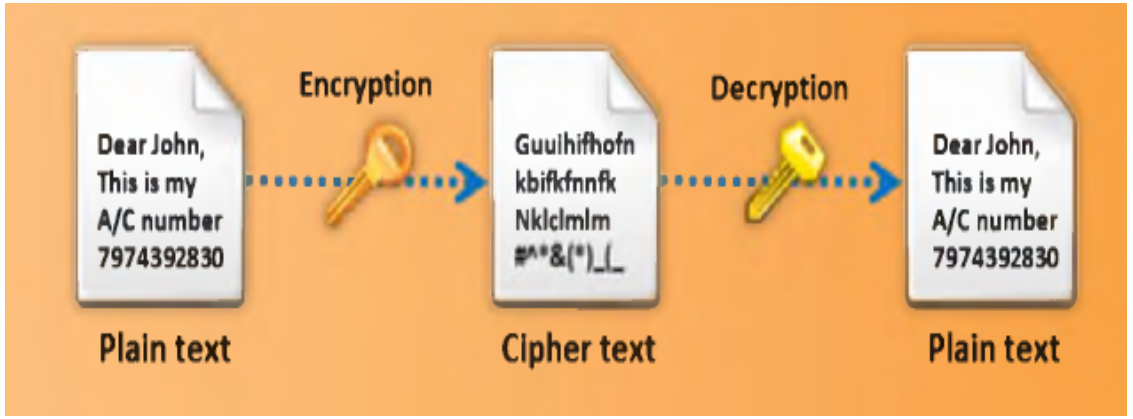
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Message 1: | 1001001 | 0100000 | 1101100 | 1101111 | 1110110 | 1100101 | 0100000 | 1111001 | 1101111 | 1110101 | 0101110 |
| Pad 1: | 1010010 | 1001011 | 1110010 | 1010101 | 1010010 | 1100011 | 0001011 | 0101010 | 1010111 | 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 |

# Types of Cryptography

- Symmetric




- Asymmetric

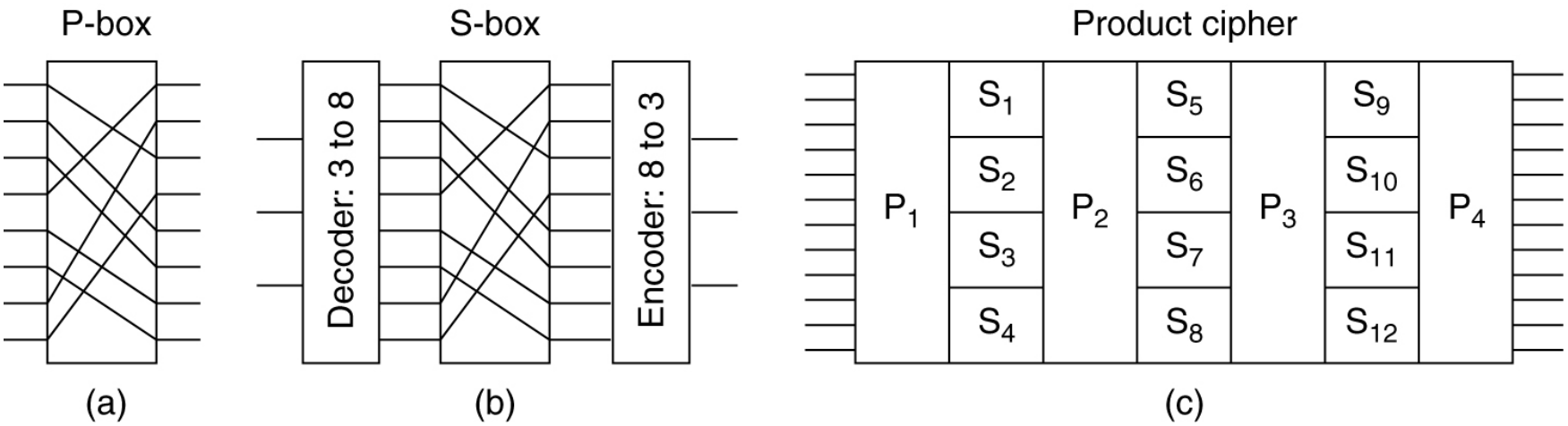


# Symmetric-Key Algorithms

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

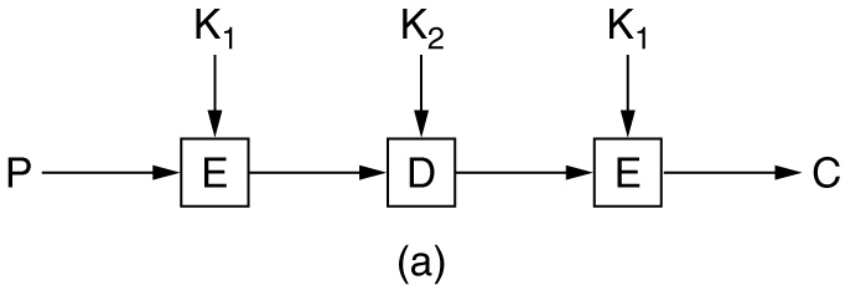
# Product Ciphers

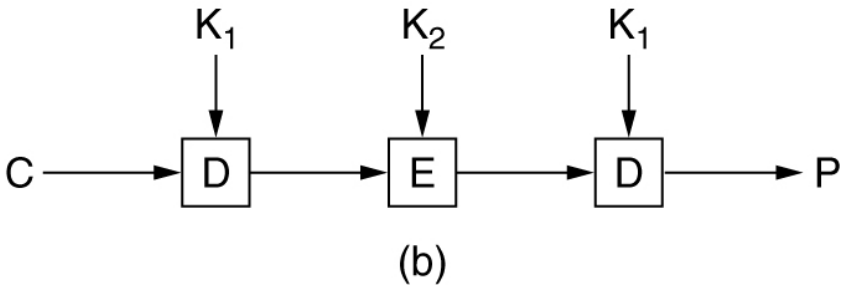
- Basic elements of product ciphers.
  (a) P-box.
  (b) S-box.
  (c) Product.



# 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.

# Cryptanalysis

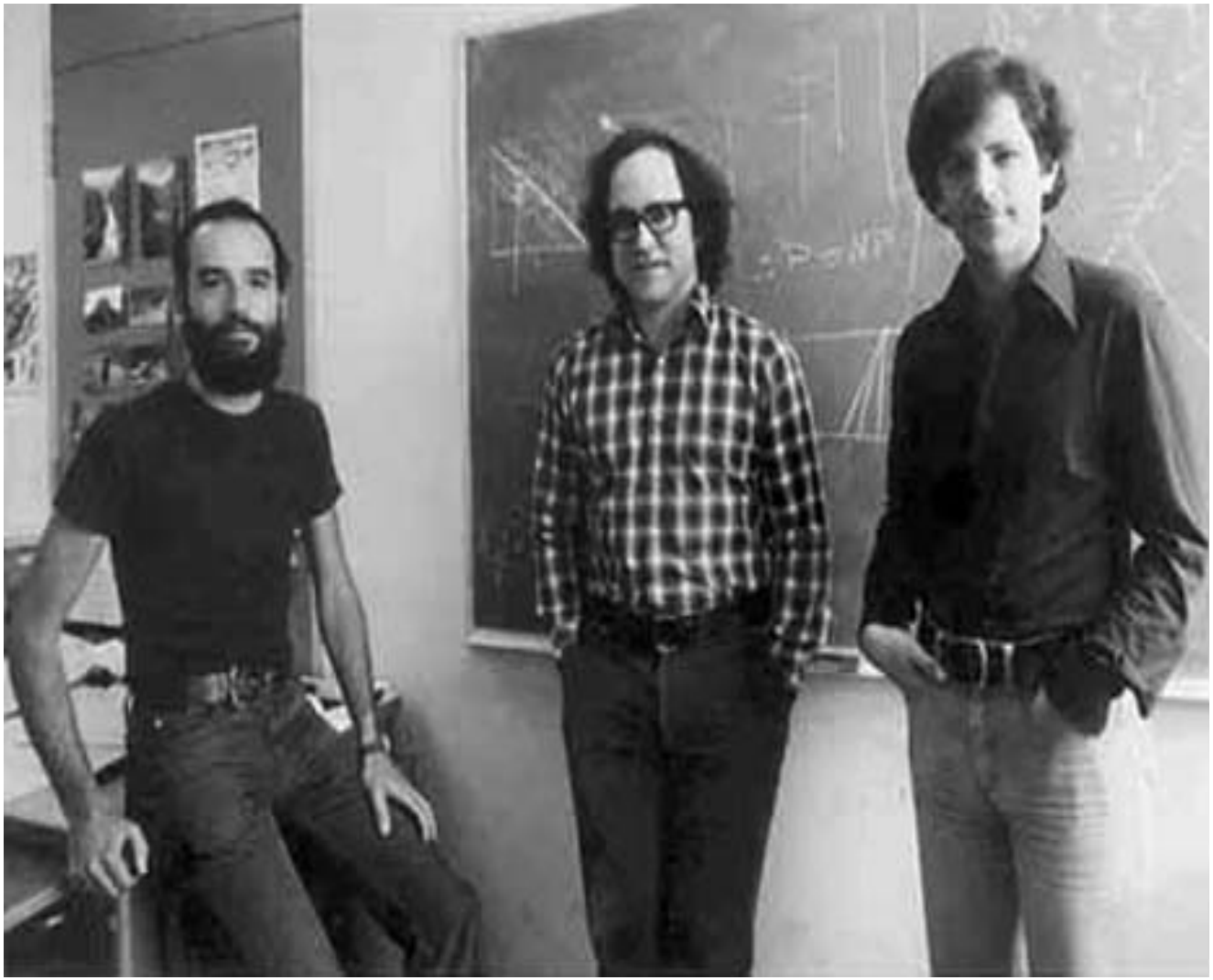
- Some common symmetric-key cryptographic algorithms.

| 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

RSA

# Rivest Shamir Adleman Algorithm



# RSA Example

- P = 61 <= firs t prime number (destroy this after computing E and D)
- Q = 53 <= second prime number (destroy this after computing E and D)
- PQ = 3233 <= modulus (give this to others)
- E = 17 <= public exponent (give this to others)
- D = 2753 <= private exponent (keep this secret!)
- Your public key is (E,PQ).
- Your private key is D.

# RSA Encryption

- The encryption function is:

  encrypt(T) = (T^E) mod PQ

  = (T^17) mod 3233

Encrypt(123) = (123^17) mod 3233

=337587917446653715596592958817679803 mod 3233

= 855

# RSA Decryption

- The decryption function is:

  decrypt(C) = (C^D) mod P

  = (C^2753) mod 3233

Decrypt(855) = (855^2753) mod 3233

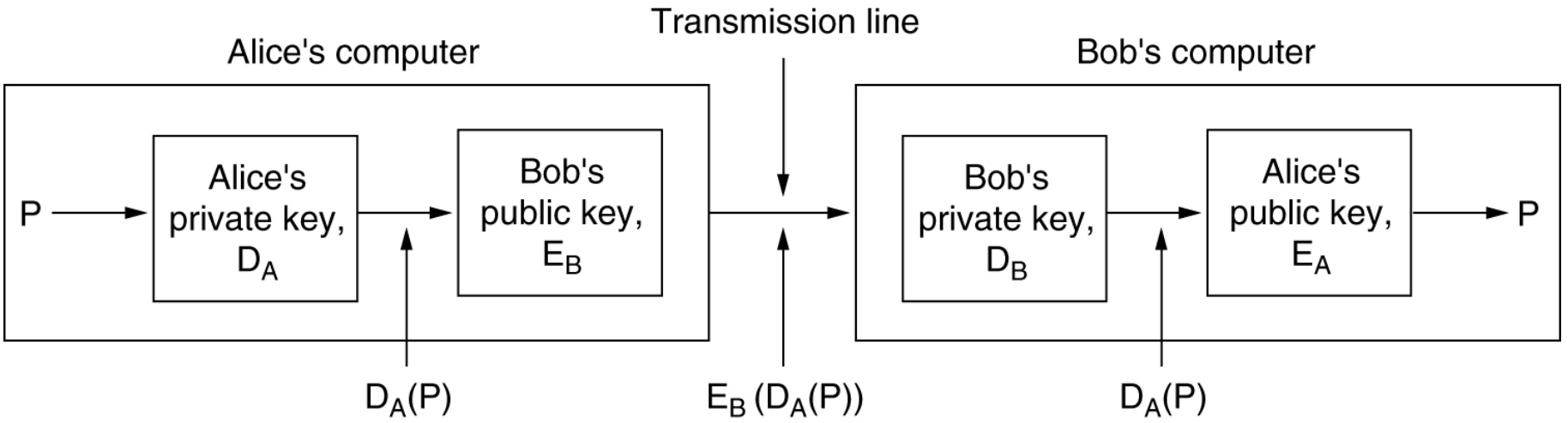
= 123

# Digital Signatures

- Symmetric-Key Signatures
- Public-Key Signatures
- Message Digests

# Public-Key Signatures

- Digital signatures using public-key cryptography.

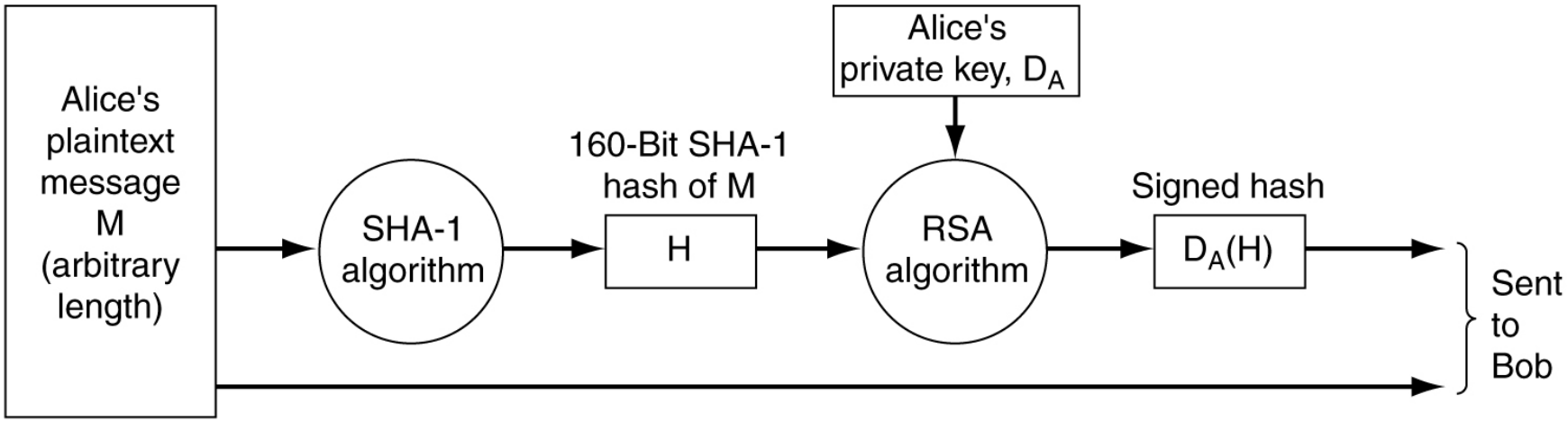


# Hashing

- MD5 Message Digest 5
- SHA1 – Secure Hashing Algorithm 160bit

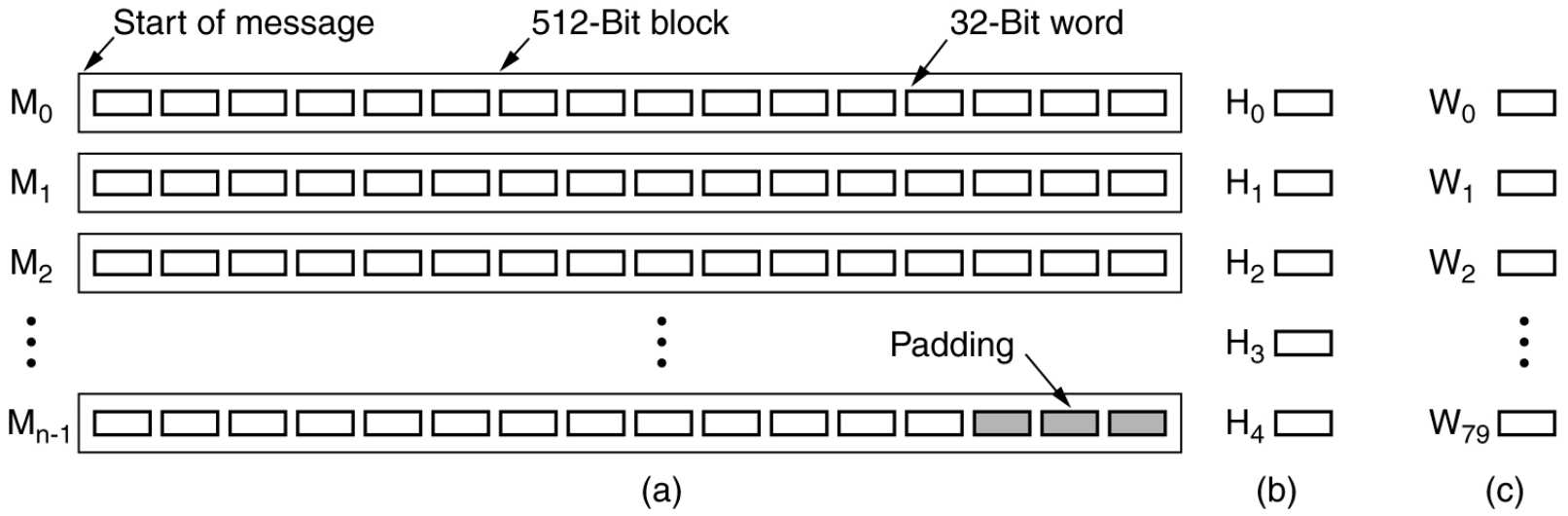
# SHA-1

- 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.

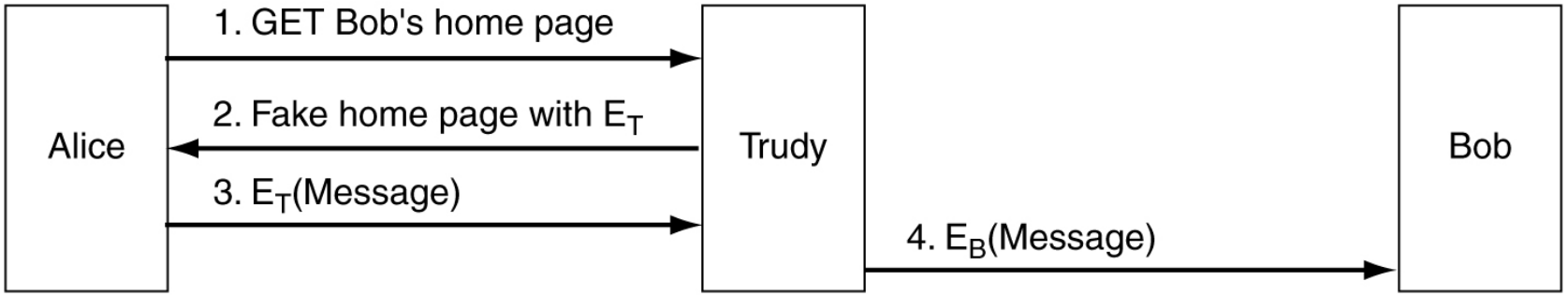


# Management of Public Keys

- Certificates
- X.509
- Public Key Infrastructures

# Problems with Public-Key Encryption

- A way for Trudy to subvert public-key encryption.



# Certificates

- A possible certificate and its signed hash.

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

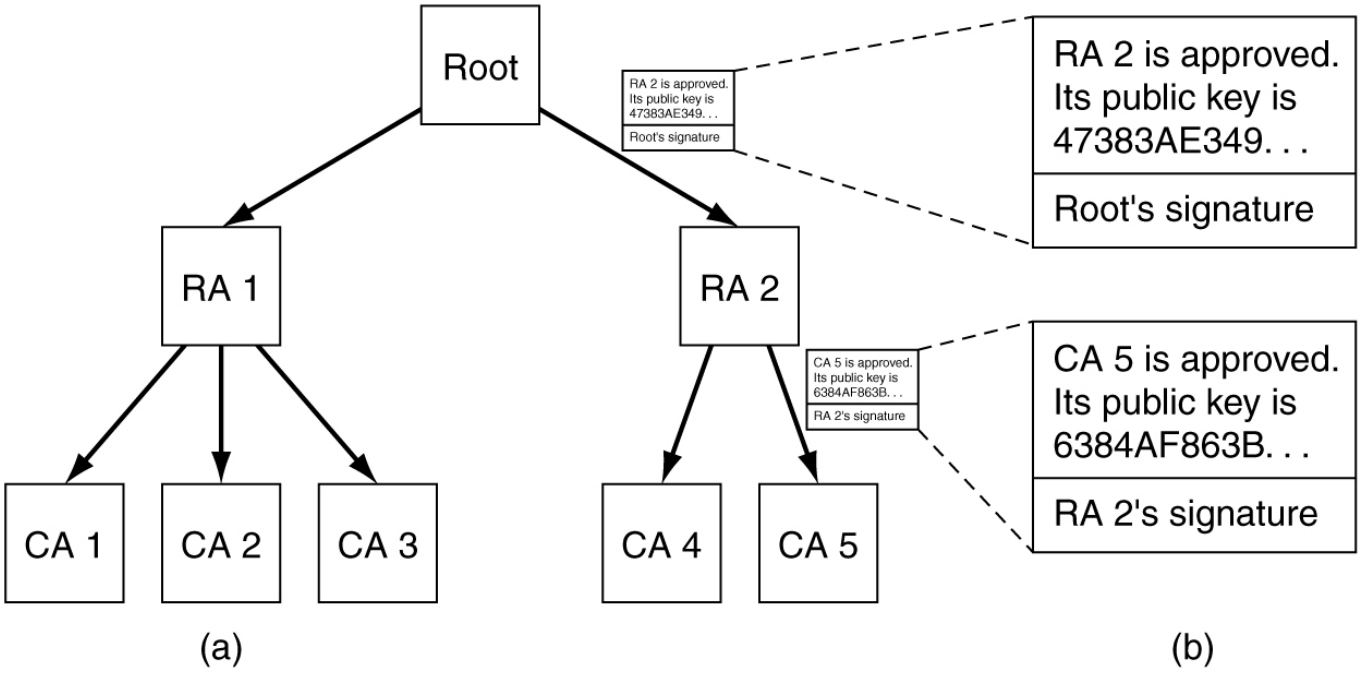
# X.509

- 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) |

# Public-Key Infrastructures

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

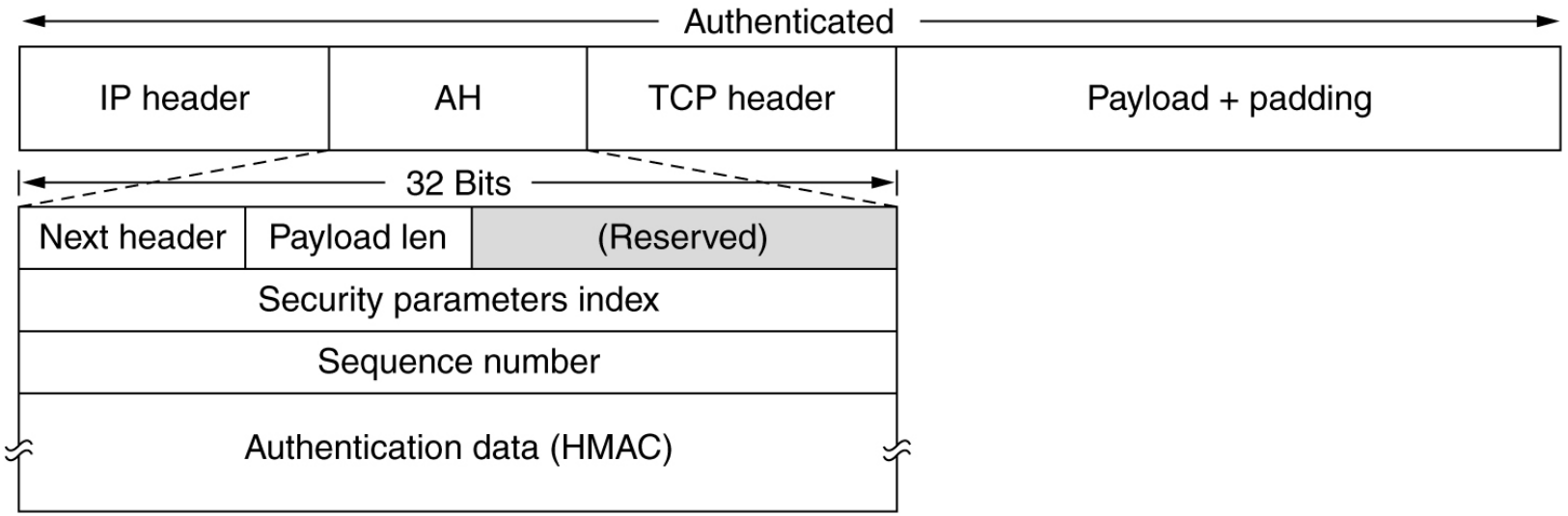


# Communication Security

- IPsec
- Firewalls
- Virtual Private Networks
- Web Security

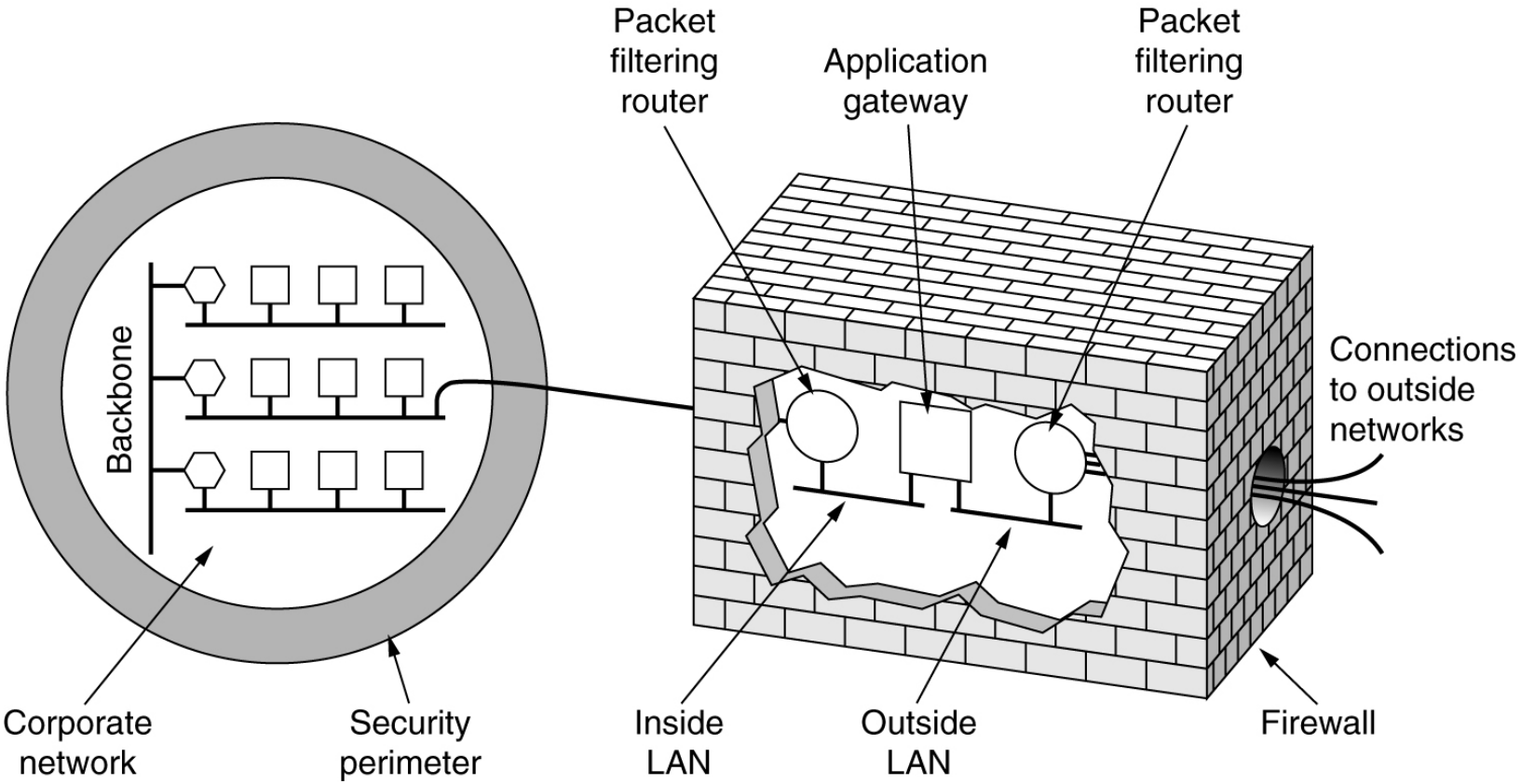
# IPsec

- The IPsec authentication header in transport mode for IPv4.



# Firewalls

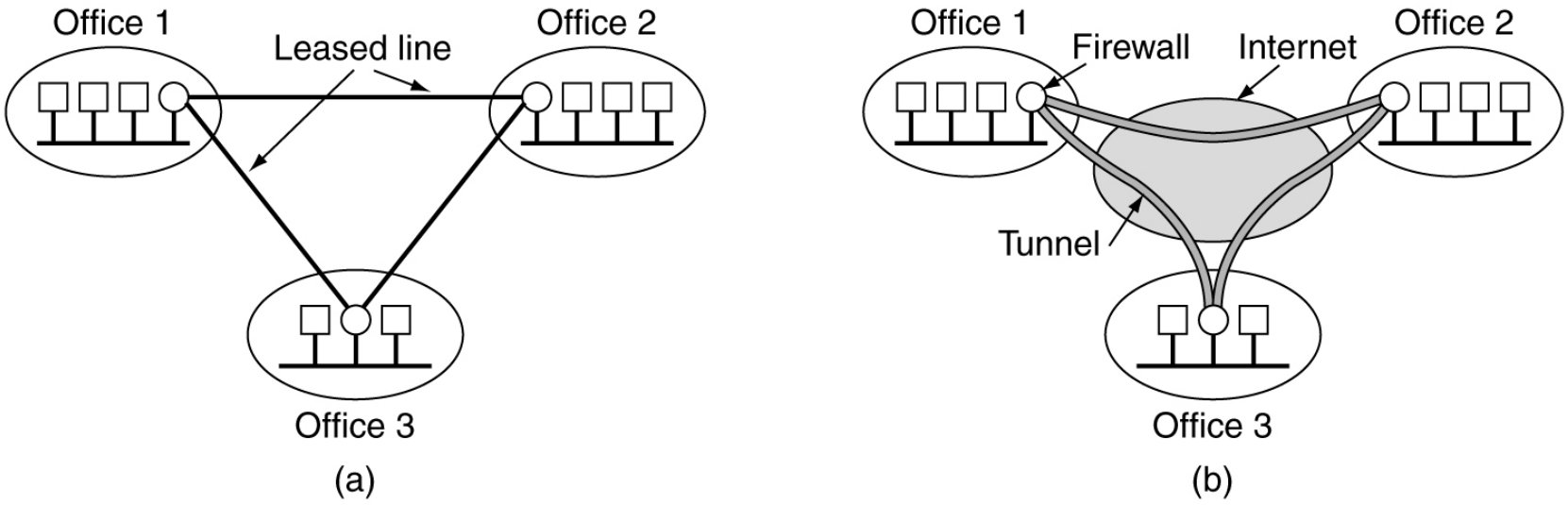
- A firewall consisting of two packet filters and an application gateway.



# Virtual Private Networks

(a) A leased-line private network.

(b) A virtual private network.



# Web Security

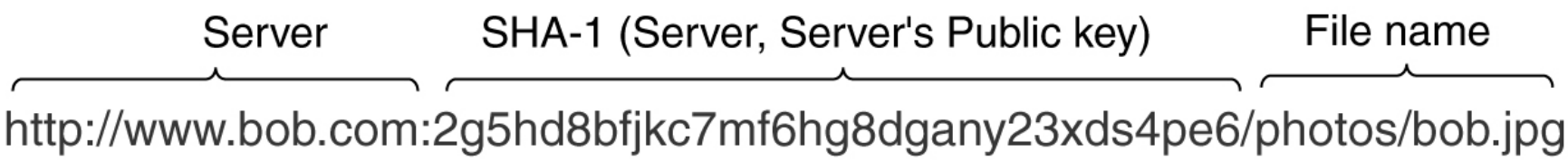
- Threats
- Secure Naming
- SSL – The Secure Sockets Layer
- Mobile Code Security

# 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.

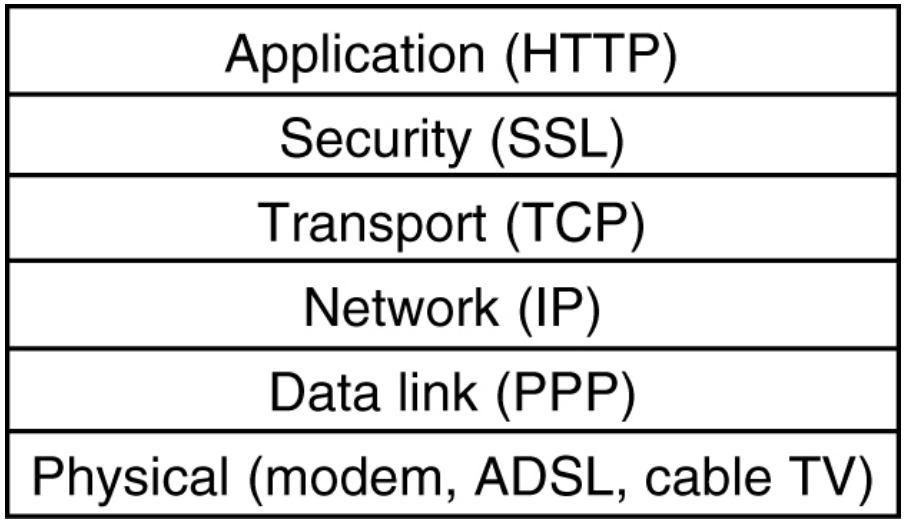
# Self-Certifying Names



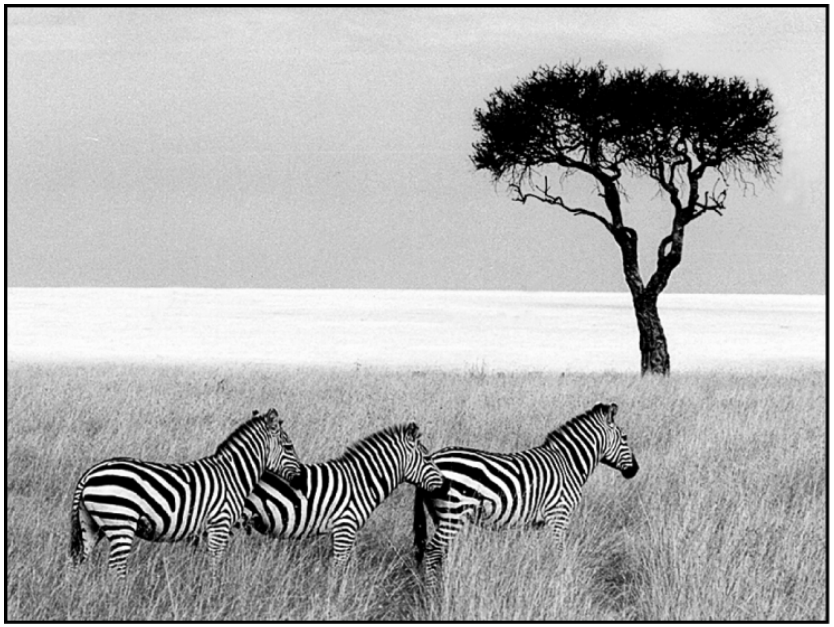

- A self-certifying URL containing a hash of server's name and public key.

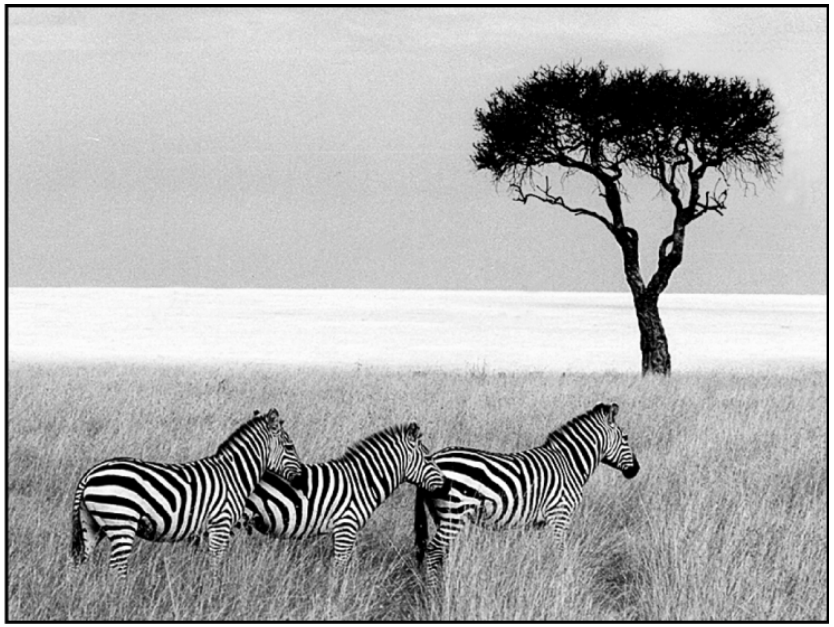
# SSL—The Secure Sockets Layer

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



# Steganography





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