CMSC 417

Computer Networks

Prof. Ashok K Agrawala

Set 8

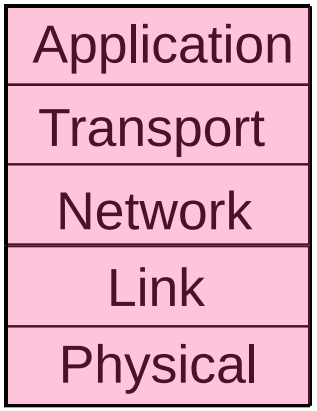
Network Security

- Cryptography
- Symmetric-Key Algorithms
- Public-Key Algorithms
- Digital Signatures
- Management of Public Keys
- Communication Security
- Authentication Protocols
- Email Security
- Web Security
- Social Issues

Revised: August 2011

Network Security

Security concerns a variety of threats and defenses across all layers



Network Security (1)

Some different adversaries and security threats

- Different threats require different defenses

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

Cryptography

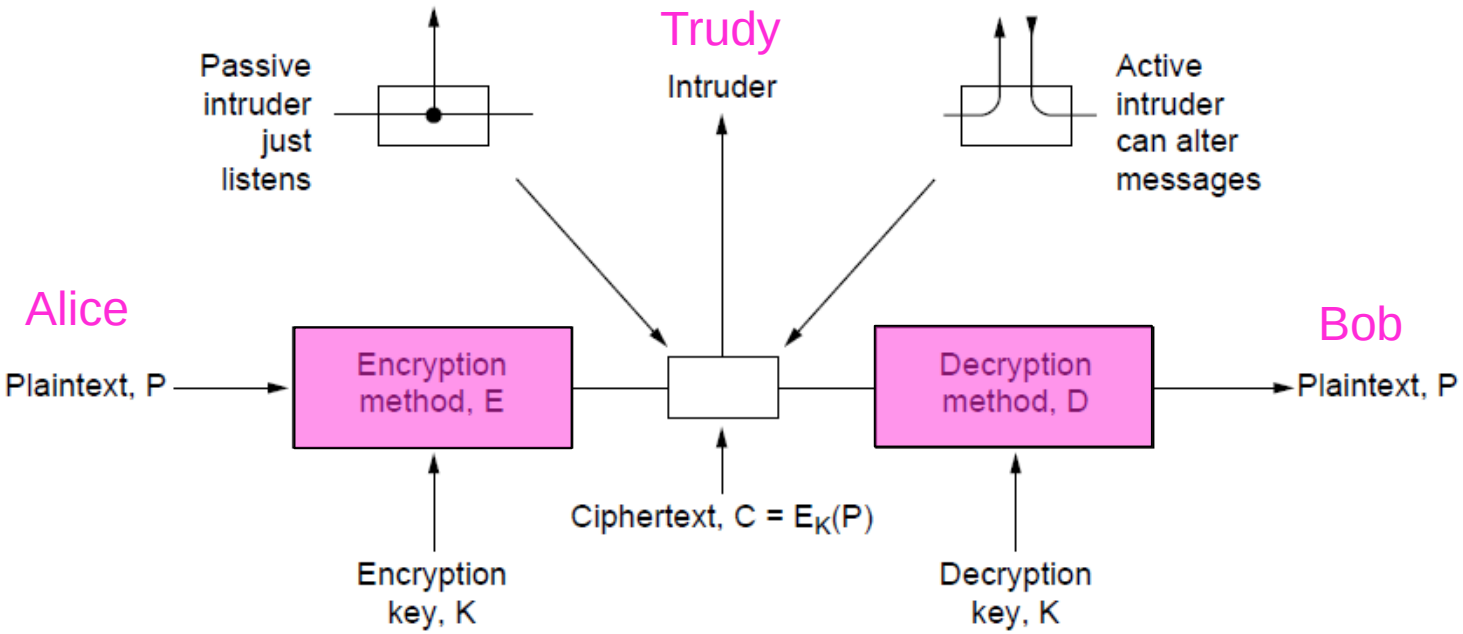
Cryptography is a fundamental building block for security mechanisms.

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

Introduction

The encryption model (for a symmetric-key cipher)

- Kerckhoff's principle: Algorithms (E, D) are public; only the keys (K) are secret



Substitution Ciphers

Substitution ciphers replace each group of letters in the message with another group of letters to disguise it

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

Simple single-letter substitution cipher

Transposition Ciphers

Transposition ciphers reorder letters to disguise

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

← Key gives column order

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Column 5 6 7 8

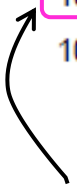
Simple column transposition cipher

One-Time Pads (1)

Simple scheme for perfect secrecy:

- XOR message with secret pad to encrypt, decrypt
- Pad is as long as the message and can't be reused!
  - It is a "one-time" pad to guarantee secrecy

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

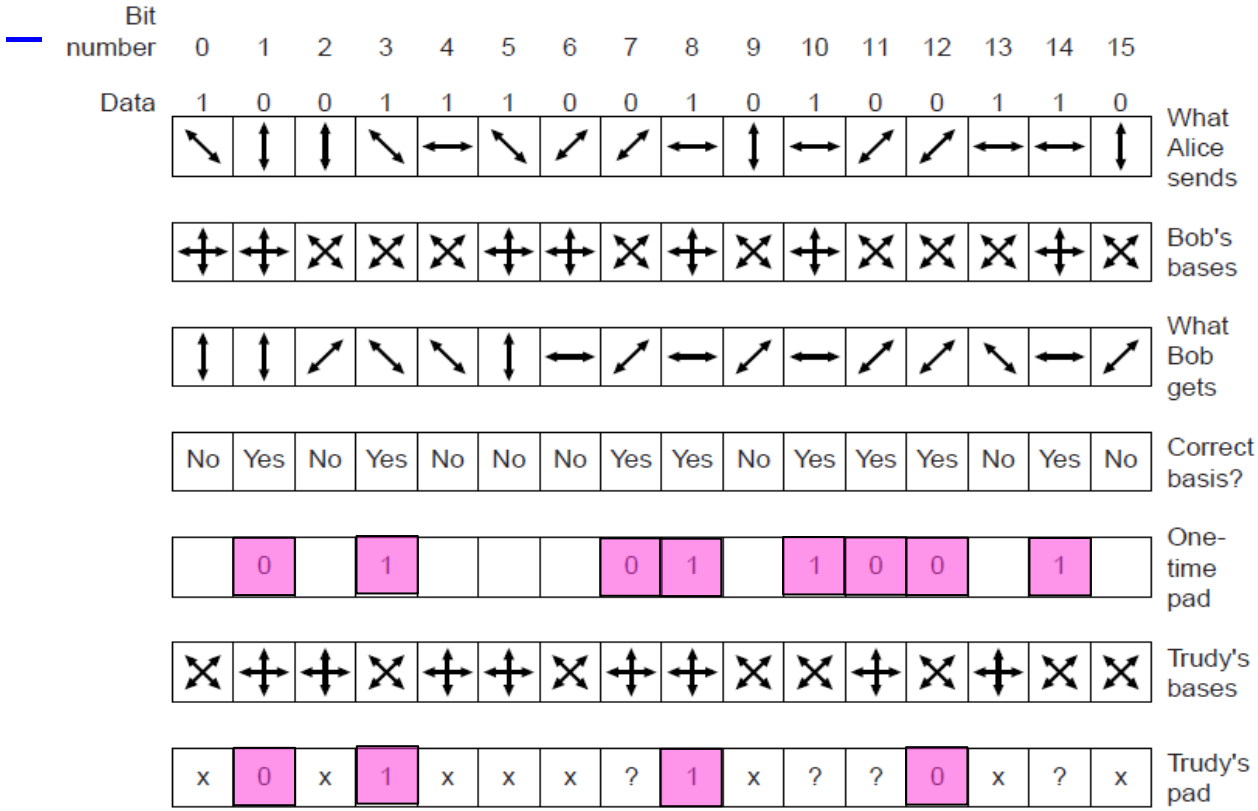


Different secret pad decrypts to the wrong plaintext

One-Time Pads (2)

Alice sending Bob a one-time pad with quantum crypto.

- Bob's guesses yield bits; Trudy misses some



Fundamental Cryptographic Principles

1. Messages must contain some redundancy
   - All encrypted messages decrypt to something
   - Redundancy lets receiver recognize a valid message
   - But redundancy helps attackers break the design

2. Some method is needed to foil replay attacks
   - Without a way to check if messages are fresh then old messages can be copied and resent
   - For example, add a date stamp to messages

Symmetric-Key Algorithms

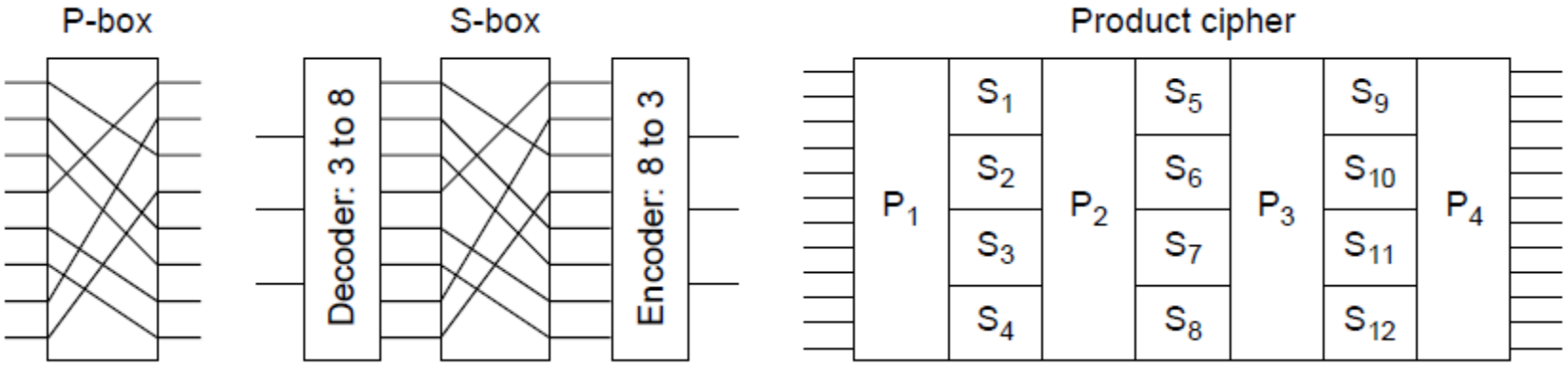
Encryption in which the parties share a secret key

- DES – Data Encryption Standard »
- AES – Advanced Encryption Standard »
- Cipher modes »
- Other ciphers »
- Cryptanalysis »

Symmetric-Key Algorithms (1)

Use the same secret key to encrypt and decrypt; block ciphers operate a block at a time

- Product cipher combines transpositions/substitutions



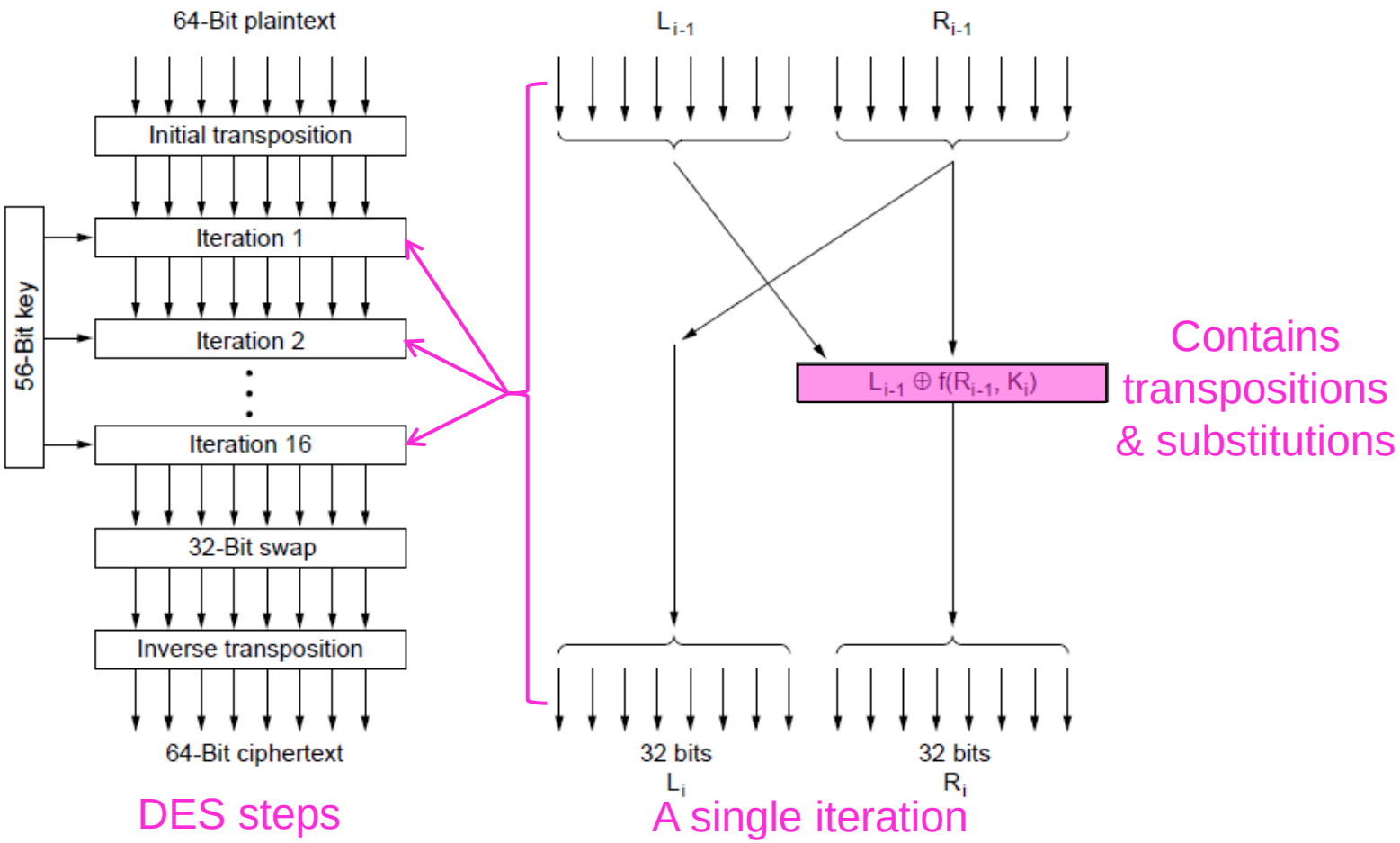
Permutation (transposition) box

Substitution box

Product with multiple P- and S-boxes

Data Encryption Standard (1)

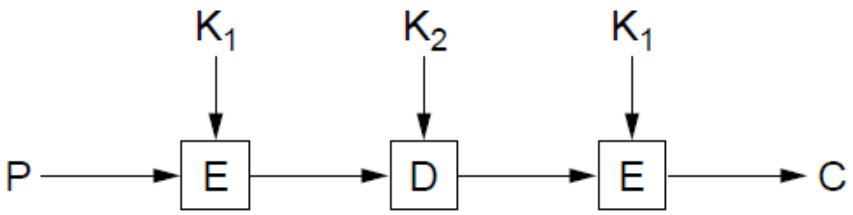
DES encryption was widely used (but no longer



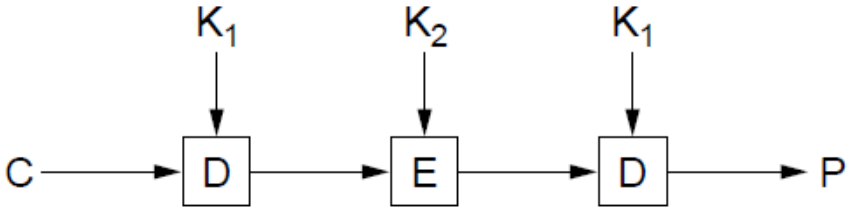
Data Encryption Standard (2)

Triple encryption ("3DES") with two 56-bit keys

- Gives an adequate key strength of 112 bits
- Setting $K_1 = K_2$ allows for compatibility with DES



Triple DES encryption



Triple DES decryption

Advanced Encryption Standard (1)

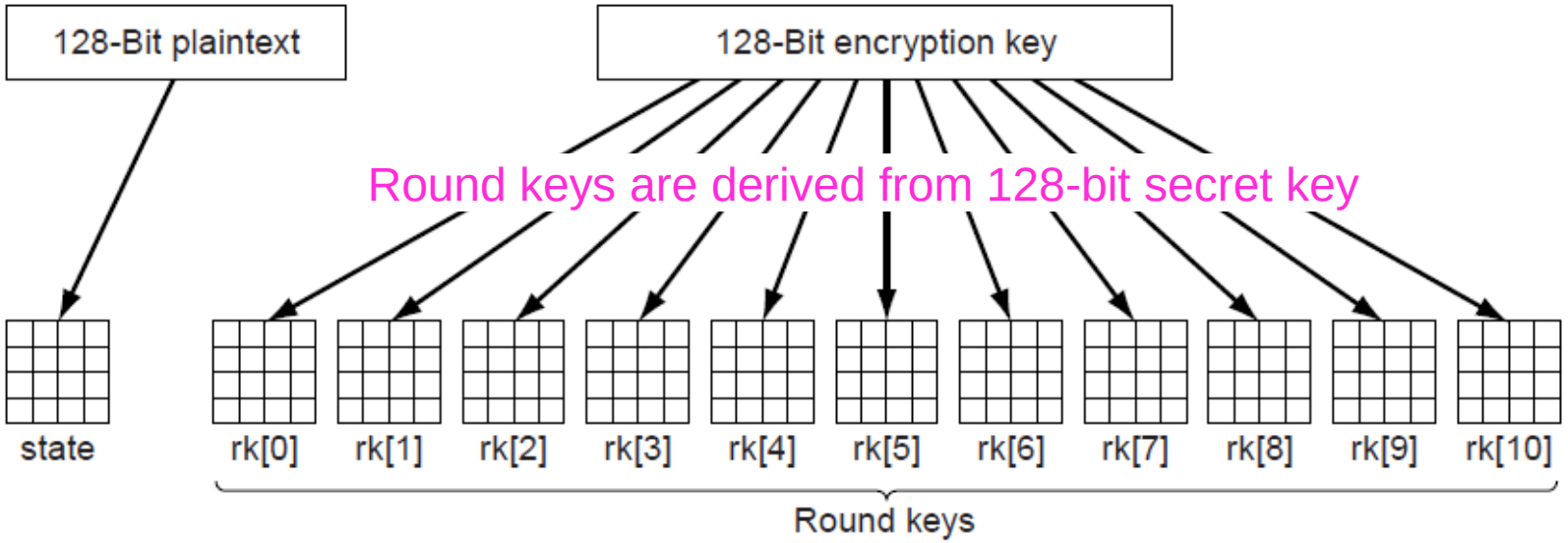
AES is the successor to DES:

- Symmetric block cipher, key lengths up to 256 bits
- Openly designed by public competition (1997-2000)
- Available for use by everyone
- Built as software (e.g., C) or hardware (e.g., x86)
- Winner was Rijndael cipher
- Now a widely used standard

Advanced Encryption Standard (2)

AES uses 10 rounds for 128-bit block and 128-bit key

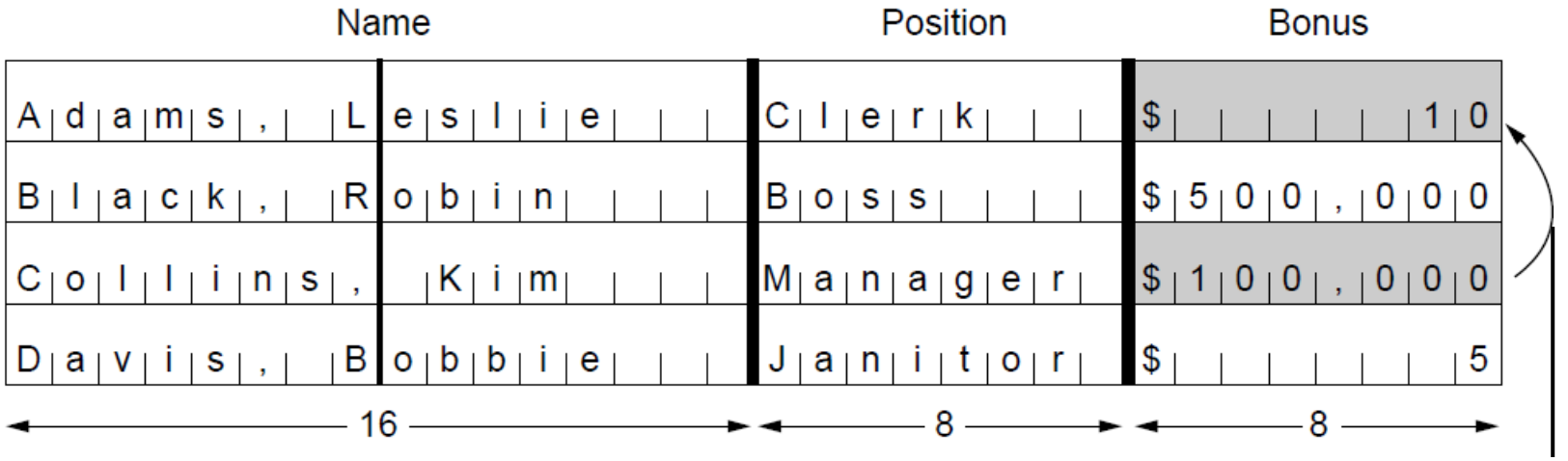
- Each round uses a key derived from 128-bit key
- Each round has a mix of substitutions and rotations
- All steps are reversible to allow for decryption



Cipher Modes (1)

Cipher modes set how long messages are encrypted

- Encrypting each block independently, called ECB (Electronic Code Book) mode, is vulnerable to shifts



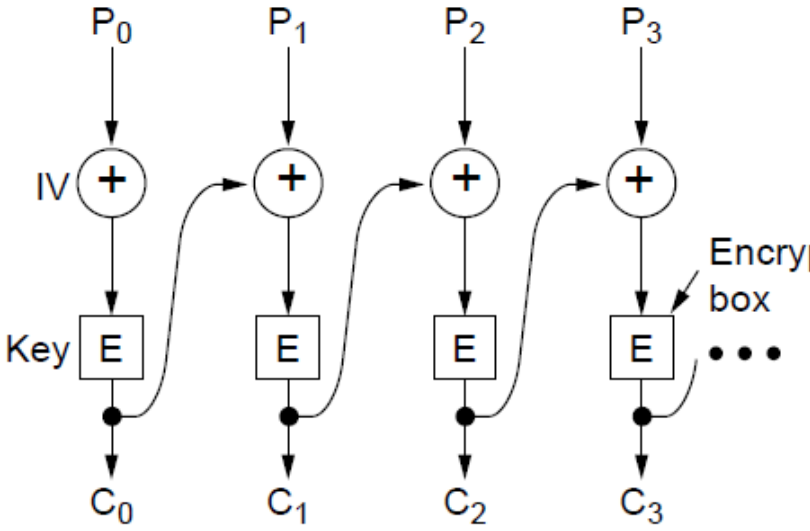
With ECB mode, switching encrypted blocks gives a different but valid message

Leslie gets a large bonus!

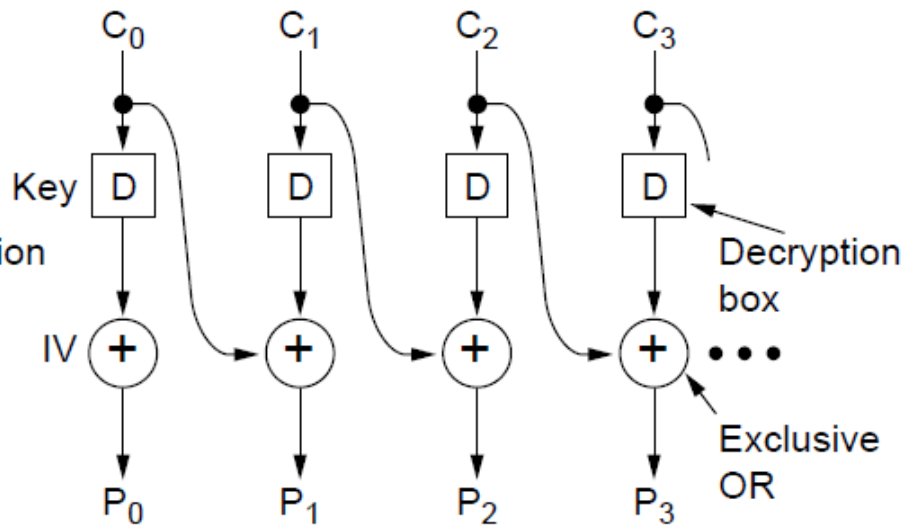
Cipher Modes (2)

CBC (Cipher Block Chaining) is a widely used mode

- Chains blocks together with XOR to prevent shifts
- Has a random IV (Initial Value) for different output



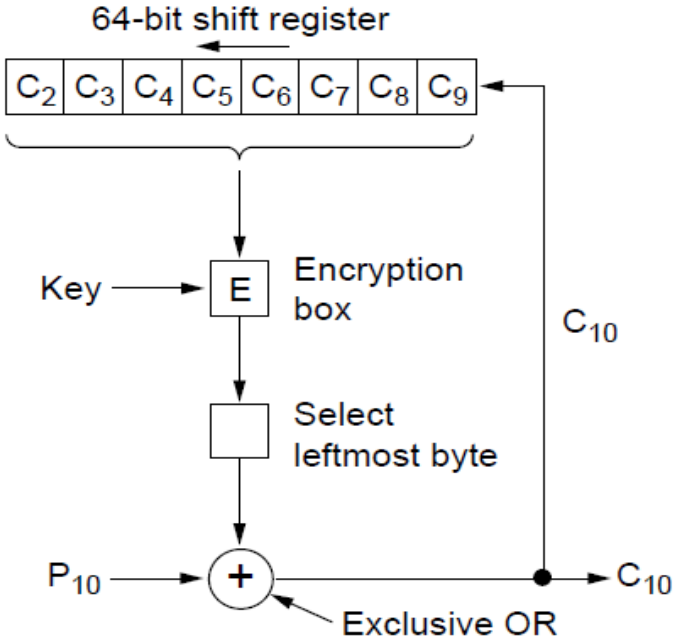
CBC mode encryption



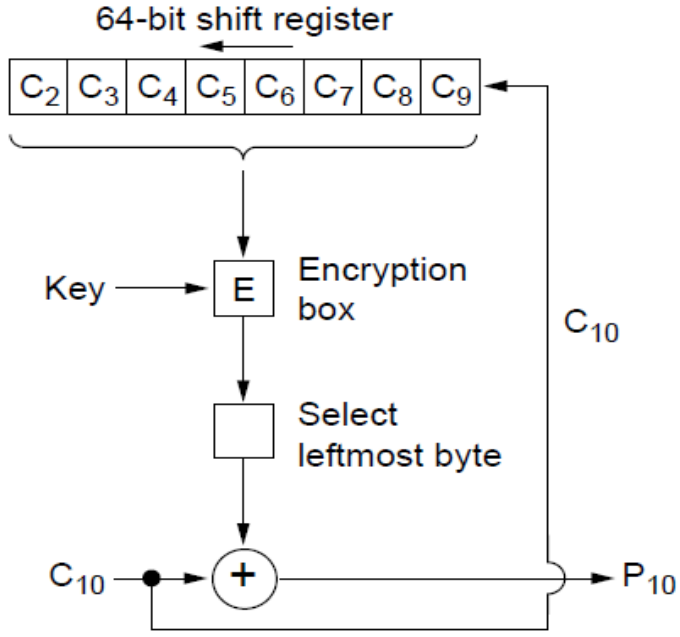
CBC mode decryption

Cipher Modes (3)

There are many other modes with pros / cons, e.g., cipher feedback mode is similar to CBC mode but can operate a byte (rather than a whole block) at



Encryption

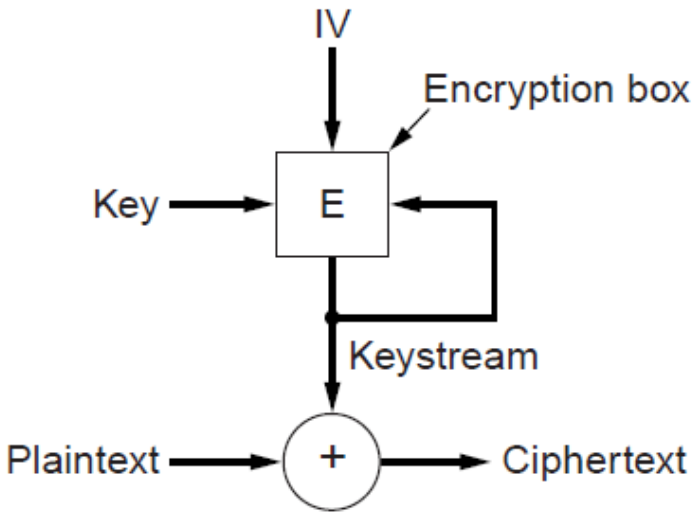


Decryption

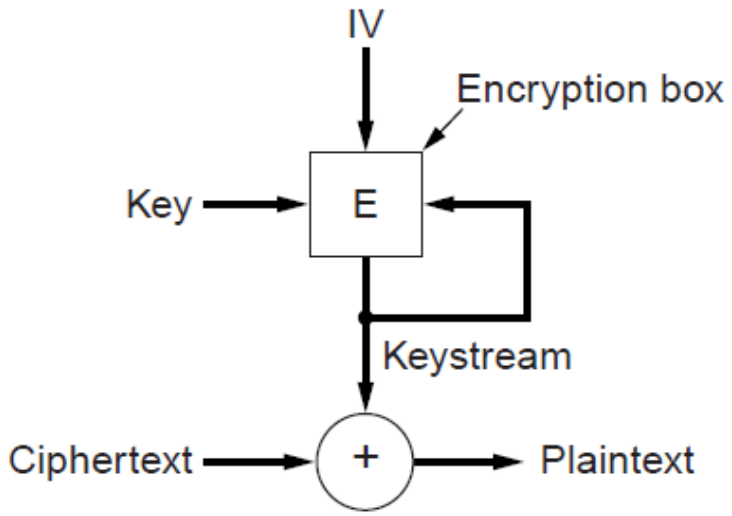
Cipher Modes (4)

A stream cipher uses the key and IV to generate a stream that is a one-time pad; can't reuse (key, IV) pair

- Doesn't amplify transmission errors like CBC mode



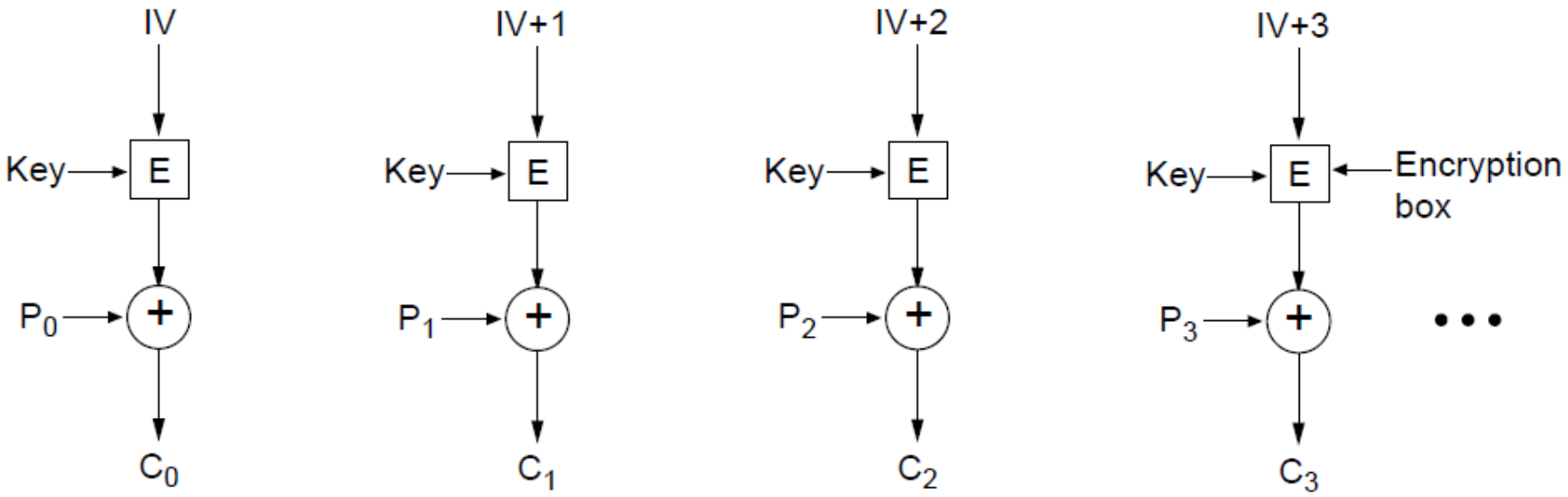
Encryption



Decryption

Cipher Modes (5)

Counter mode (encrypt a counter and XOR it with each message block) allows random access for



Encryption above; repeat the operation to decrypt

Other Ciphers

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

Encryption in which each party publishes a public part of their key and keep secret a private part of it

- RSA (by Rivest, Shamir, Adleman) »

Public-Key Algorithms (1)

Downsides of keys for symmetric-key designs:

- Key must be secret, yet be distributed to both parties
- For N users there are N^2 pairwise keys to manage

Public key schemes split the key into public and private parts that are mathematically related:

- Private part is not distributed; easy to keep secret
- Only one public key per user needs to be managed

Security depends on the chosen mathematical property

- Much slower than symmetric-key, e.g., 1000X
- So use it to set up per-session symmetric keys

RSA (1)

RSA is a widely used public-key encryption method whose security is based on the difficulty of factoring large numbers

Key generation:

- Choose two large primes, p and q
- Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
- Choose d to be relatively prime to z
- Find e such that $e \times d = 1 \bmod z$
- Public key is (e, n), and private key is (d, n)

Encryption (of k bit message, for numbers up to n):

- $\text{Cipher} = \text{Plain}^e \pmod n$

Decryption:

- $\text{Plain} = \text{Cipher}^d \pmod n$

RSA (2)

Small-scale example of RSA encryption

- For p=3, q=11 → n=33, z=20 → d=7, e=3

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

Encryption: $C = P^3 \bmod 33$

Decryption: $P = C^7 \bmod 33$

Digital Signatures

Lets receiver verify the message is authentic

- Symmetric-Key signatures »
- Public-Key signatures »
- Message digests »
- The birthday attack »

Digital Signatures (1)

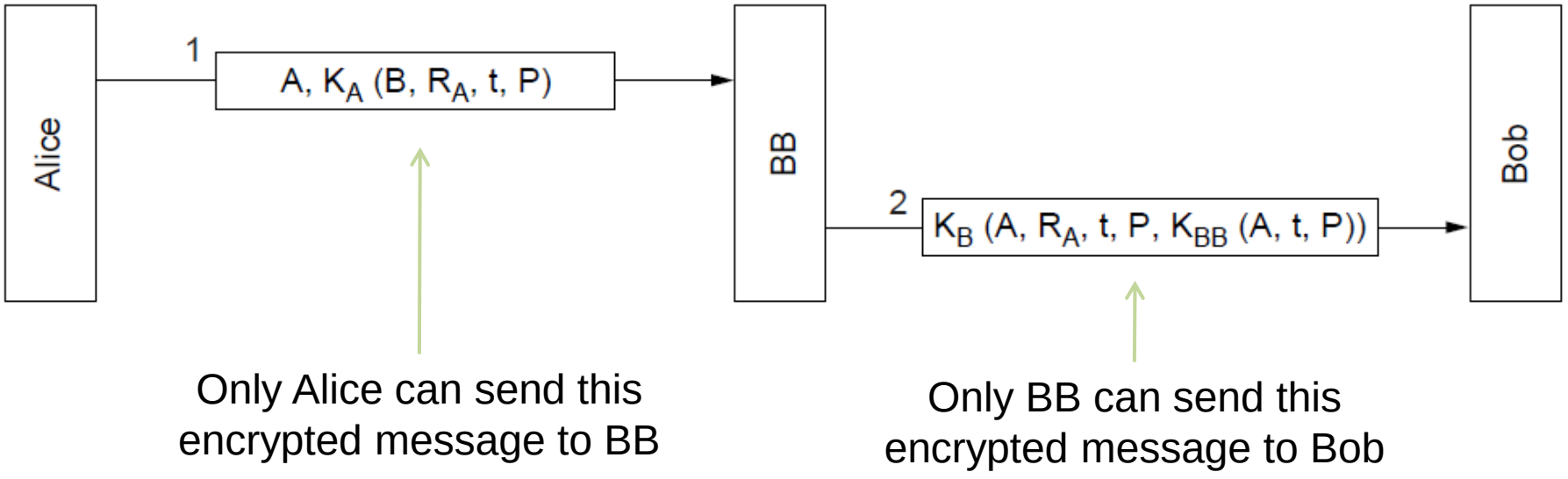
Requirements for a signature:

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

Symmetric-key Signatures

Alice and Bob each trust and share a key with Big Brother; Big Brother doesn't trust anyone

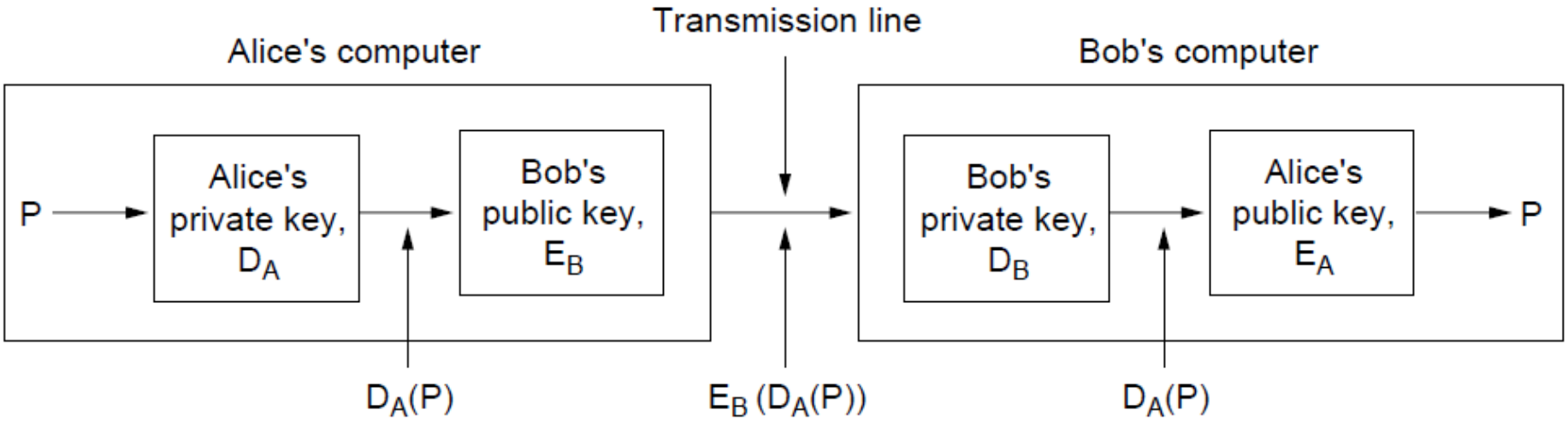
- A=Alice, B=Bob, P=message, R_A=random, t=time



Public-Key Signatures

No Big Brother and assumes encryption and decryption are inverses that can be applied in either order

- But relies on private key kept and secret



Message Digests (1)

Message Digest (MD) converts arbitrary-size message (P) into a fixed-size identifier MD(P) with properties:

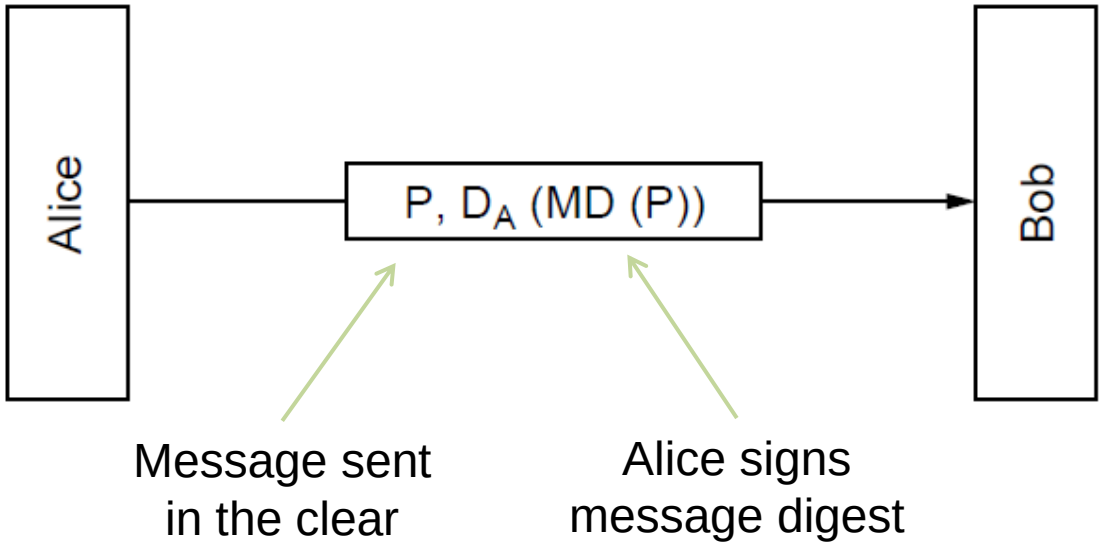
- Given P, easy to compute MD(P).
- Given MD(P), effectively impossible to find P.
- Given P no one can find P′ so that MD(P′) = MD(P).
- Changing 1 bit of P produces very different MD.

Message digests (also called cryptographic hash) can "stand for" messages in protocols, e.g., authentication

- Example: SHA-1 160-bit hash, widely used
- Example: MD5 128-bit hash – now known broken

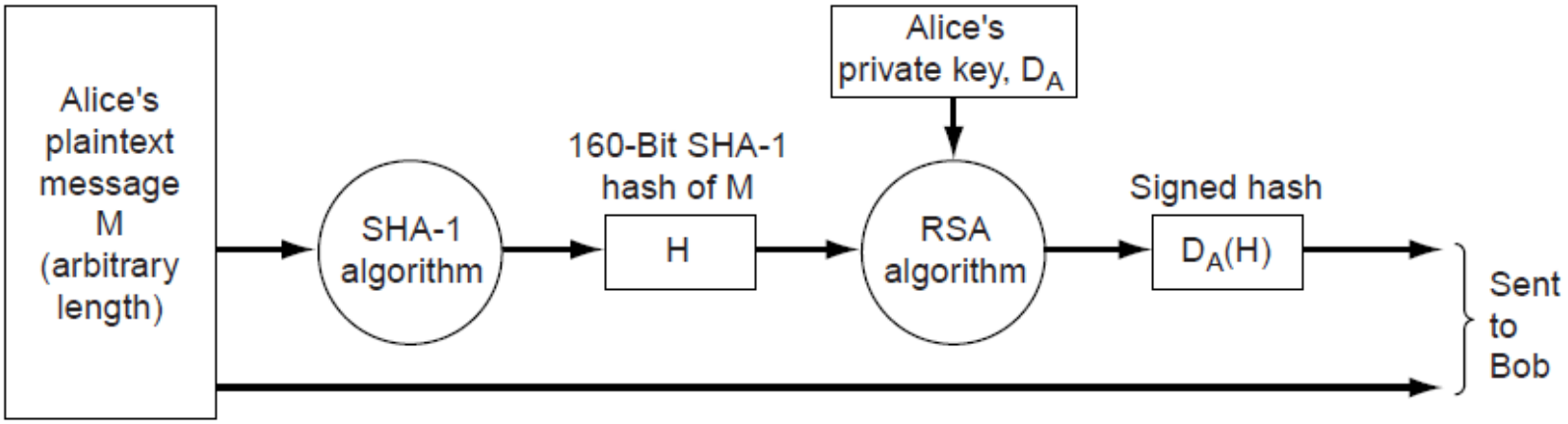
Message Digests (2)

Public-key signature for message authenticity but not confidentiality with a message digest



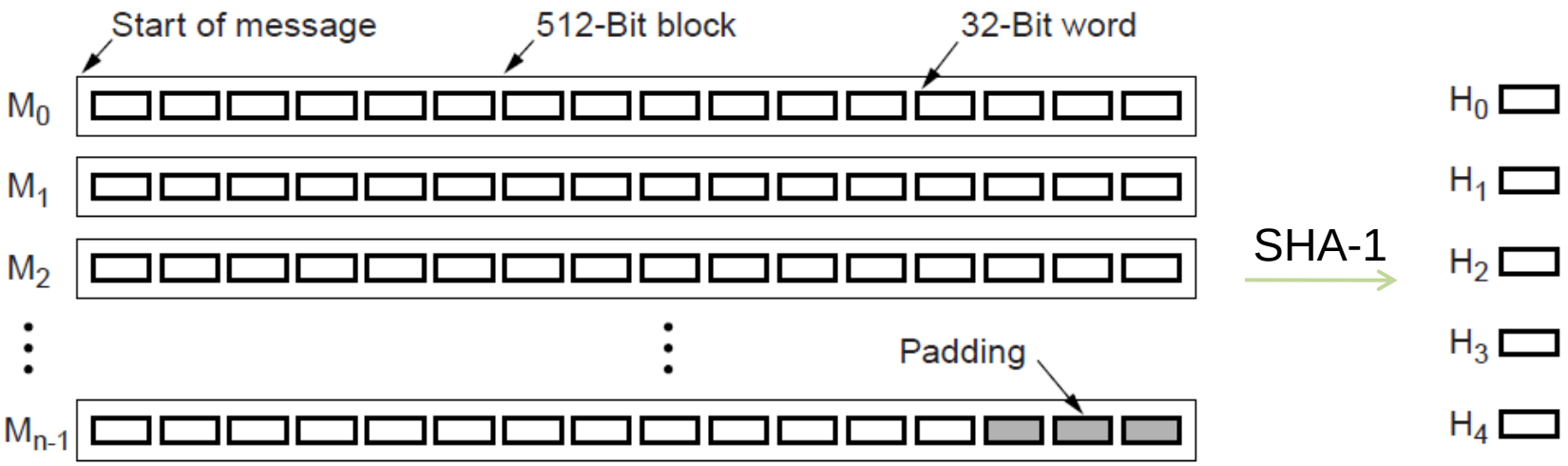
Message Digests (3)

In more detail: example of using SHA-1 message digest and RSA public key for signing nonsecret messages



Message Digests (4)

SHA-1 digests the message 512 bits at a time to build a 160-bit hash as five 32-bit components



Message in 512-bit blocks

Five 32-bit hashes output

Birthday Attack

How hard is it to find a message P′ that has the same message digest as P?

- Such a collision will allow P′ to be substituted for P!

Analysis:

- N bit hash has 2^N possible values
- Expect to test 2^N messages given P to find P′
- But expect only $2^{N/2}$ messages to find a collision
- This is the birthday attack

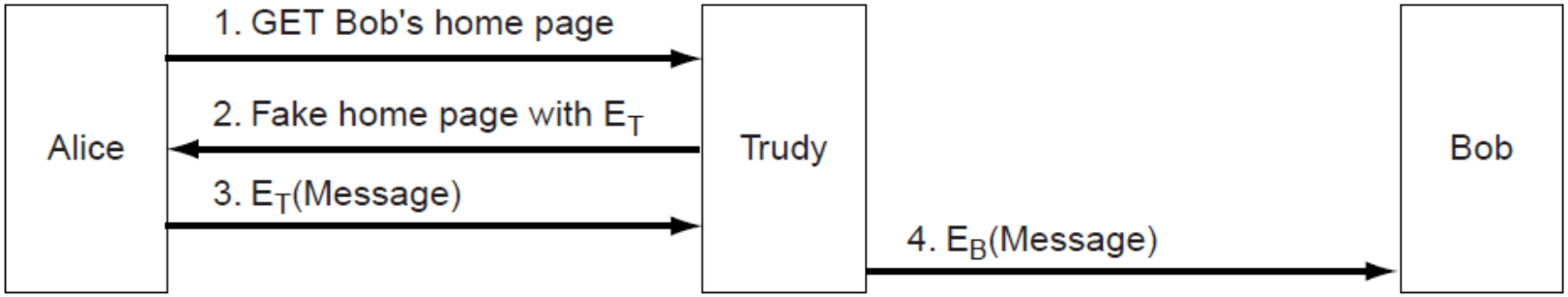
Management of Public Keys

We need a trusted way to distribute public keys

- Certificates »
- X.509, the certificate standard »
- Public Key infrastructures »

Management of Public Keys (1)

Trudy can subvert encryption if she can fake Bob's public key; Alice and Bob will not necessarily know



Trudy replaces E_B with E_T and acts as a "man in the middle"

Certificates

CA (Certification Authority) issues signed statements about public keys; users trust CA and it can be

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

X.509

X.509 is the standard for widely used certificates

- Ex: used with SSL for secure Web browsing

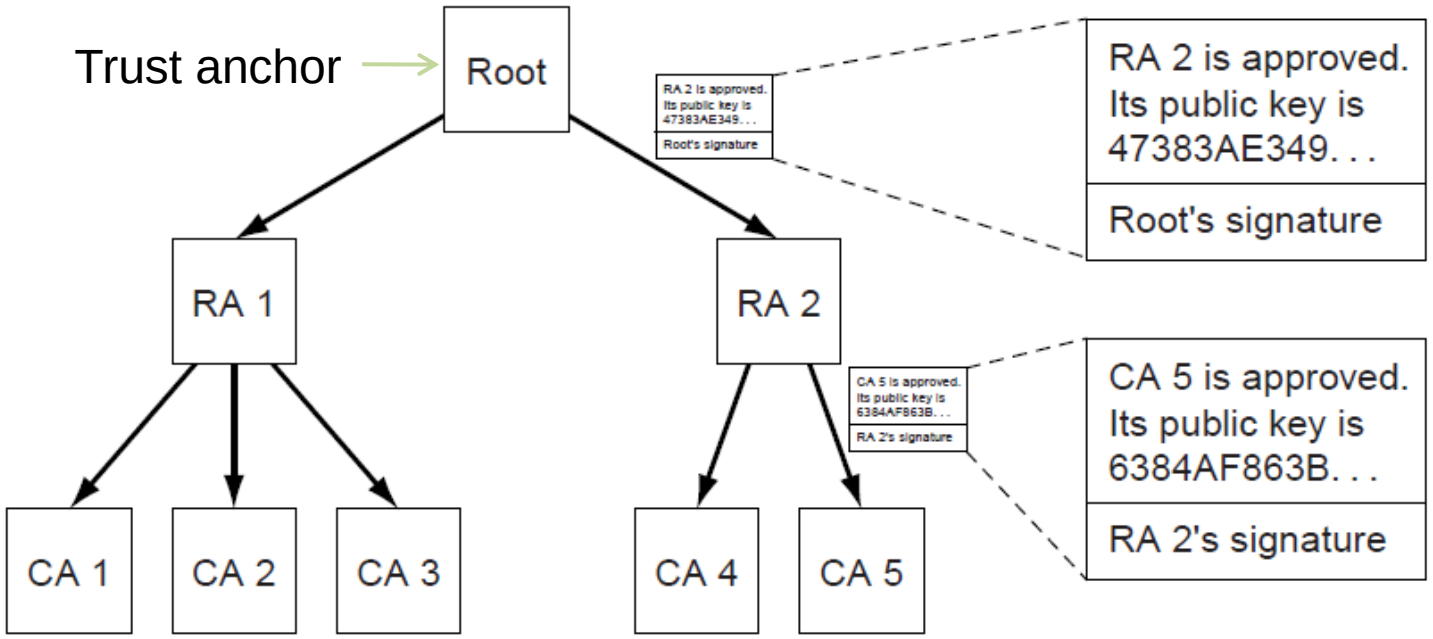
Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The 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)

Basic fields in X.509 certificates

Public Key Infrastructures (PKIs)

PKI is a system for managing public keys using CAs

- Scales with hierarchy, may have multiple roots
- Also need CRLs (Certificate Revocation Lists)



Hierarchical PKI

Chain of certificates for CA 5

Communication Security

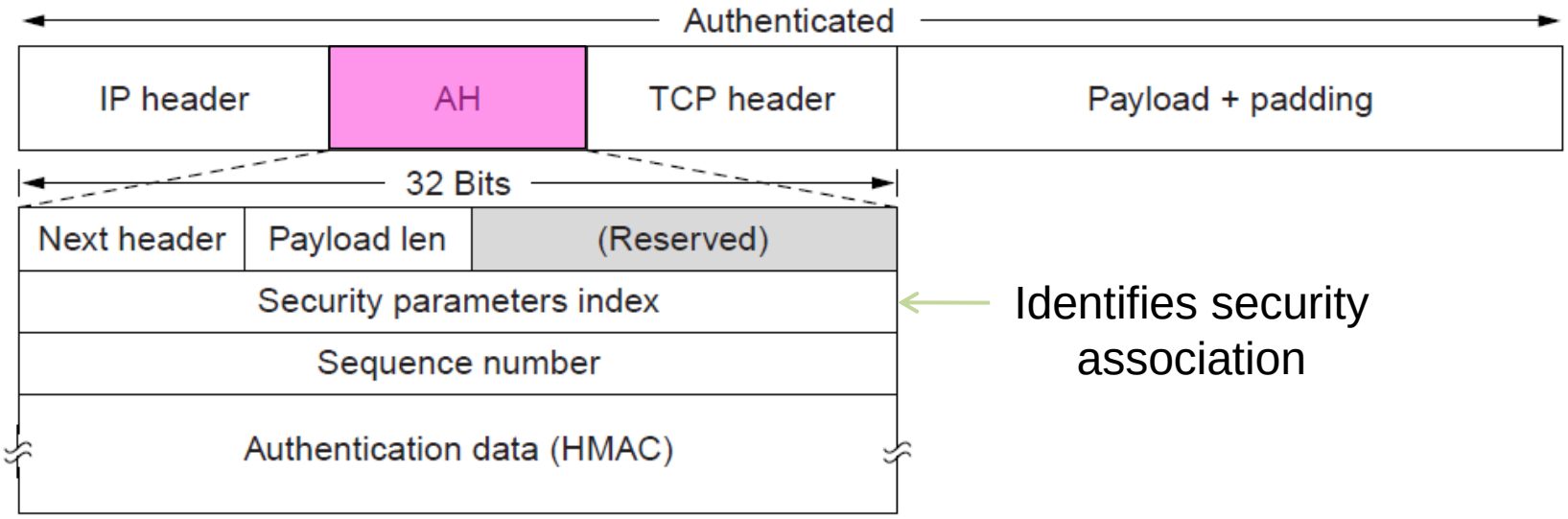
Applications of security to network protocols

- IPsec (IP security) »
- Firewalls »
- Virtual private networks »
- Wireless security »

IPsec (1)

IPsec adds confidentiality and authentication to IP

- Secret keys are set up for packets between endpoints called security associations
- Adds AH header; inserted after IP in transport mode

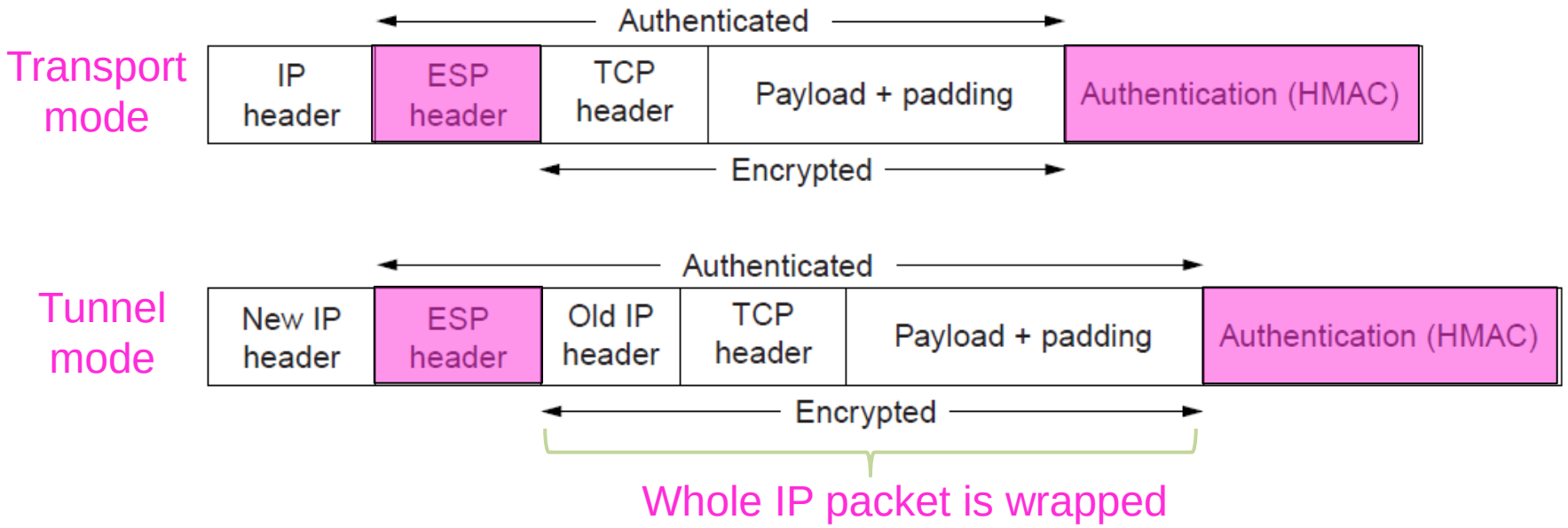


AH (Authentication Header) provides integrity and anti-replay

IPsec (2)

ESP (Encapsulating Security Payload) provides secrecy and integrity; expands on AH

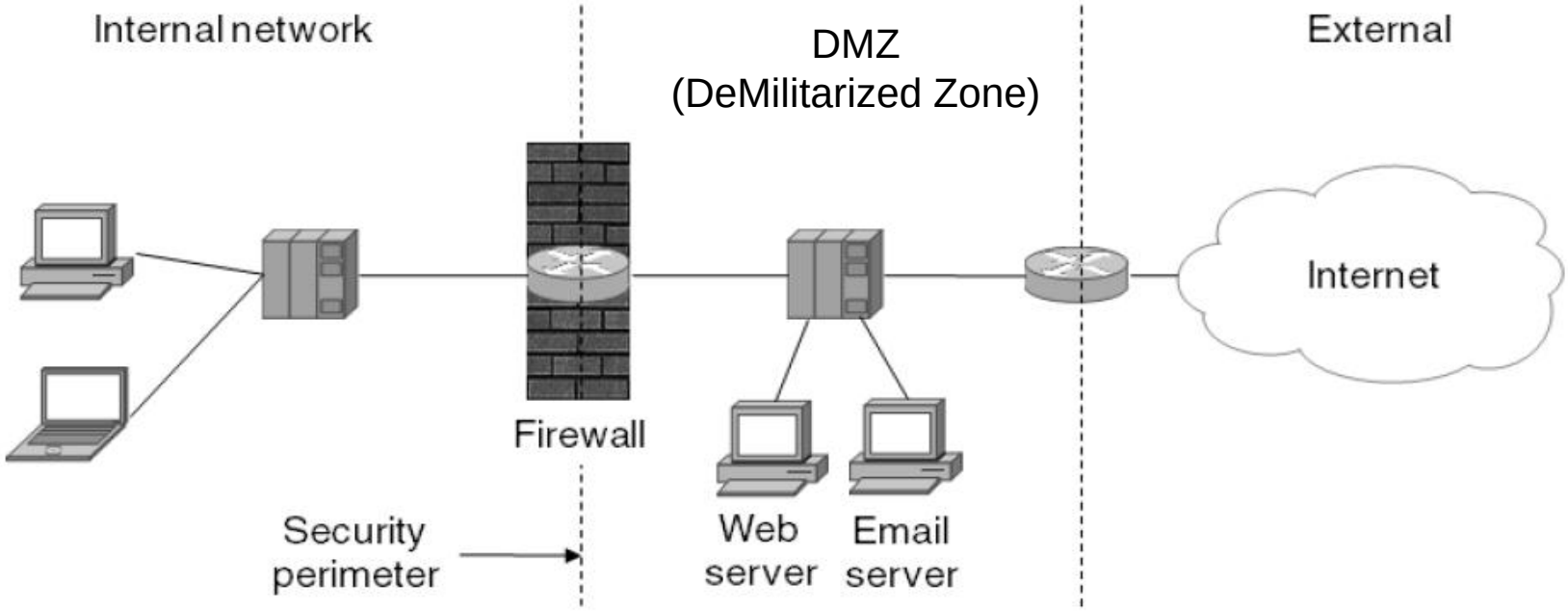
- Adds ESP header and trailer; inserted after IP header in transport or before in tunnel mode



Firewalls

A firewall protect an internal network by filtering packets

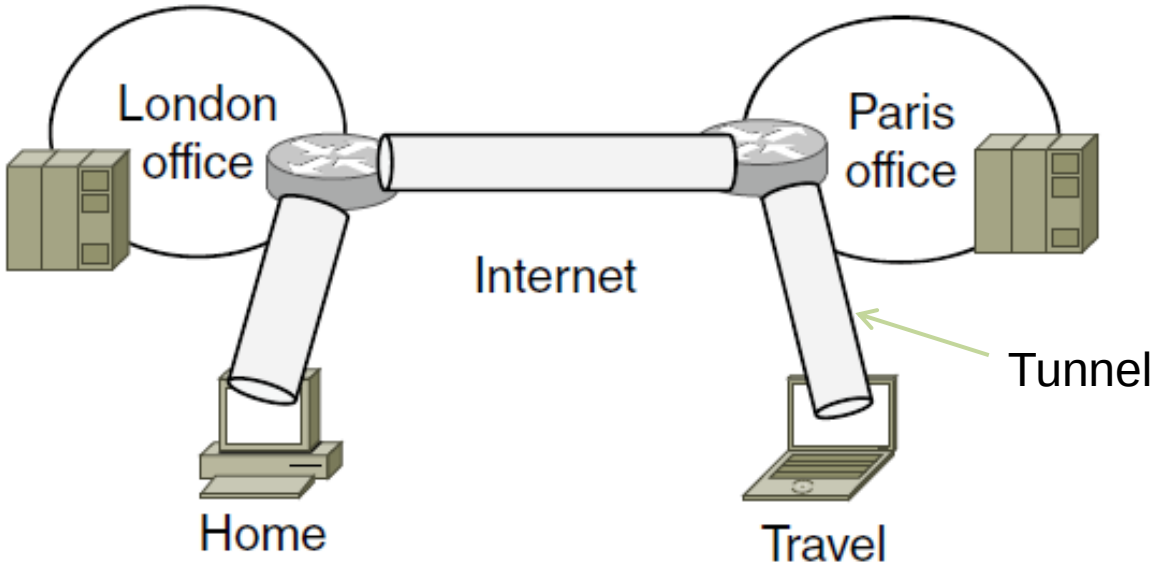
- Can have stateful rules about what packets to pass
  - E.g., no incoming packets to port 80 (Web) or 25 (SMTP)
- DMZ helps to separate internal from external traffic



Virtual Private Networks (1)

VPNs (Virtual Private Networks) join disconnected islands of a logical network into a single virtual network

- Islands are joined by tunnels over the Internet

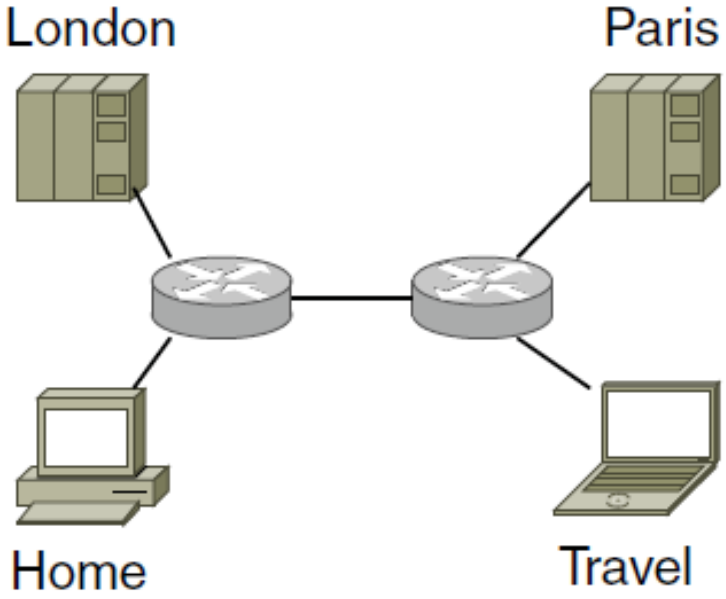


VPN joining London, Paris, Home, and Travel

Virtual Private Networks (2)

VPN traffic travels over the Internet but VPN hosts are separated from the Internet

- Need a gateway to send traffic in/out of VPN



Topology as seen from inside the VPN

Wireless Security (1)

Wireless signals are broadcast to all nearby receivers

- Important to use encryption to secure the network
- This is an issue for 802.11, Bluetooth, 3G, …

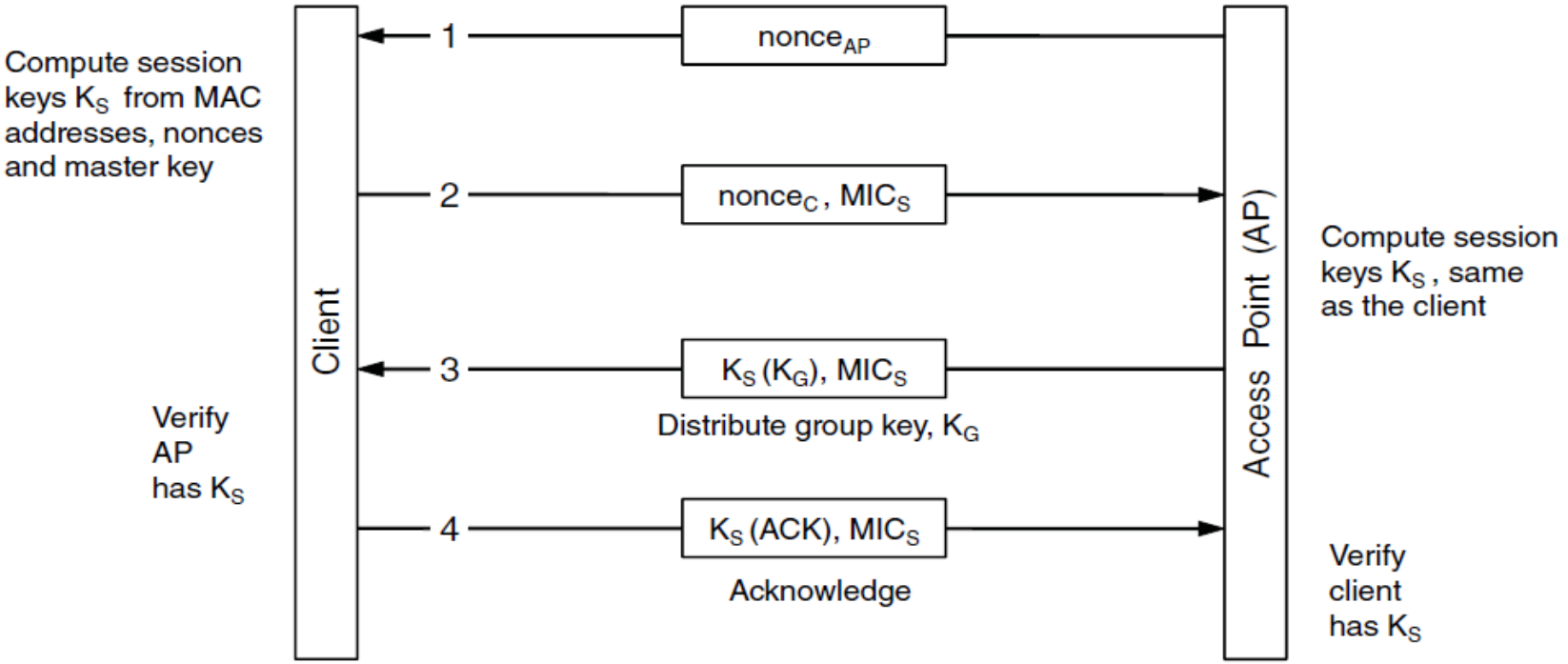
Common design:

1. Clients have a password set up for access
2. Clients authenticate to infrastructure and set up a session key
3. Session key is then used to encrypt packets

Wireless Security (2)

802.11i session key setup handshake (step 2)

- Client and AP share a master key (password)
- MIC (Message Integrity Check) is like a signature
- $K_X(M)$ means a message M encrypted with key K_X



Authentication Protocols

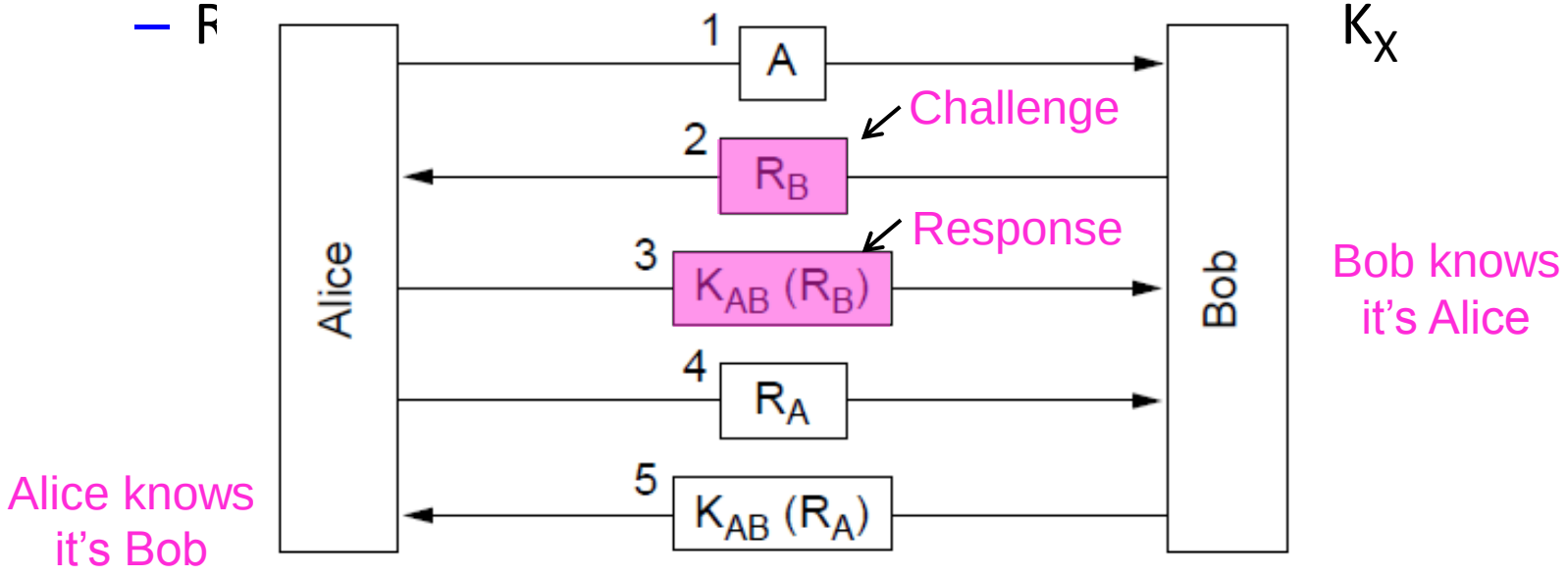
Authentication verifies the identity of a remote party

- Shared Secret Key »
- Diffie-Hellman Key Exchange »
- Key Distribution Center »
- Kerberos »
- Public-Key Cryptography »

Shared Secret Key (1)

Authenticating with a challenge-response (first attempt)

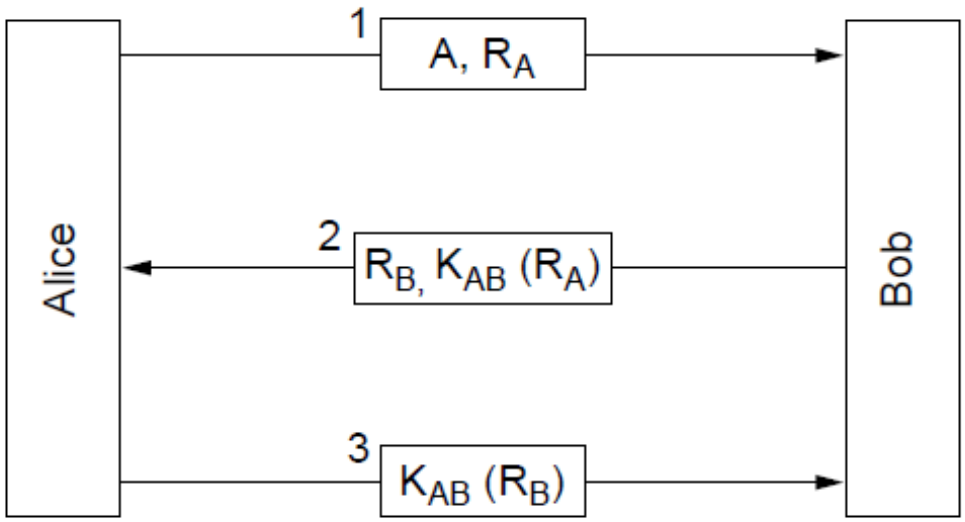
- Alice (A) and Bob (B) share a key K_{AB}
- R



Shared Secret Key (2)

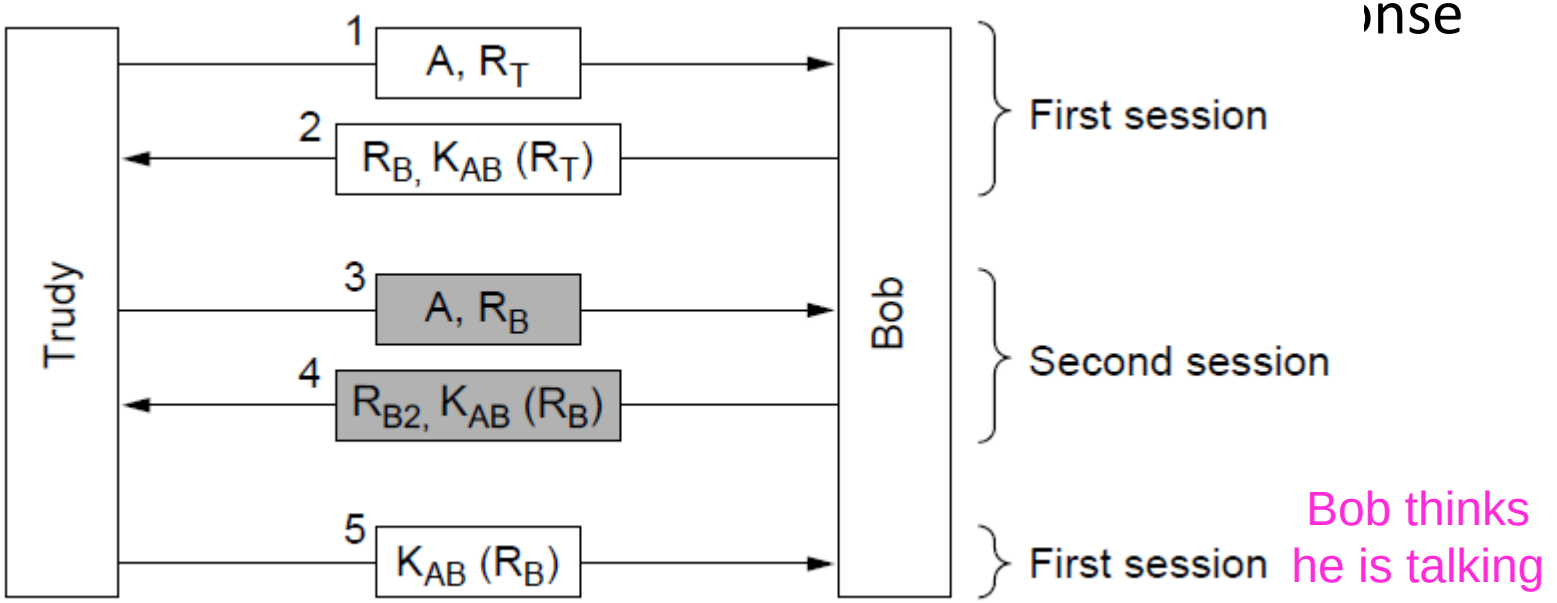
A shortened two-way authentication (second attempt)

- But it is vulnerable to reflection attack



Shared Secret Key (3)

Trudy impersonates Alice to Bob with reflection attack



Bob thinks he is talking to Alice now

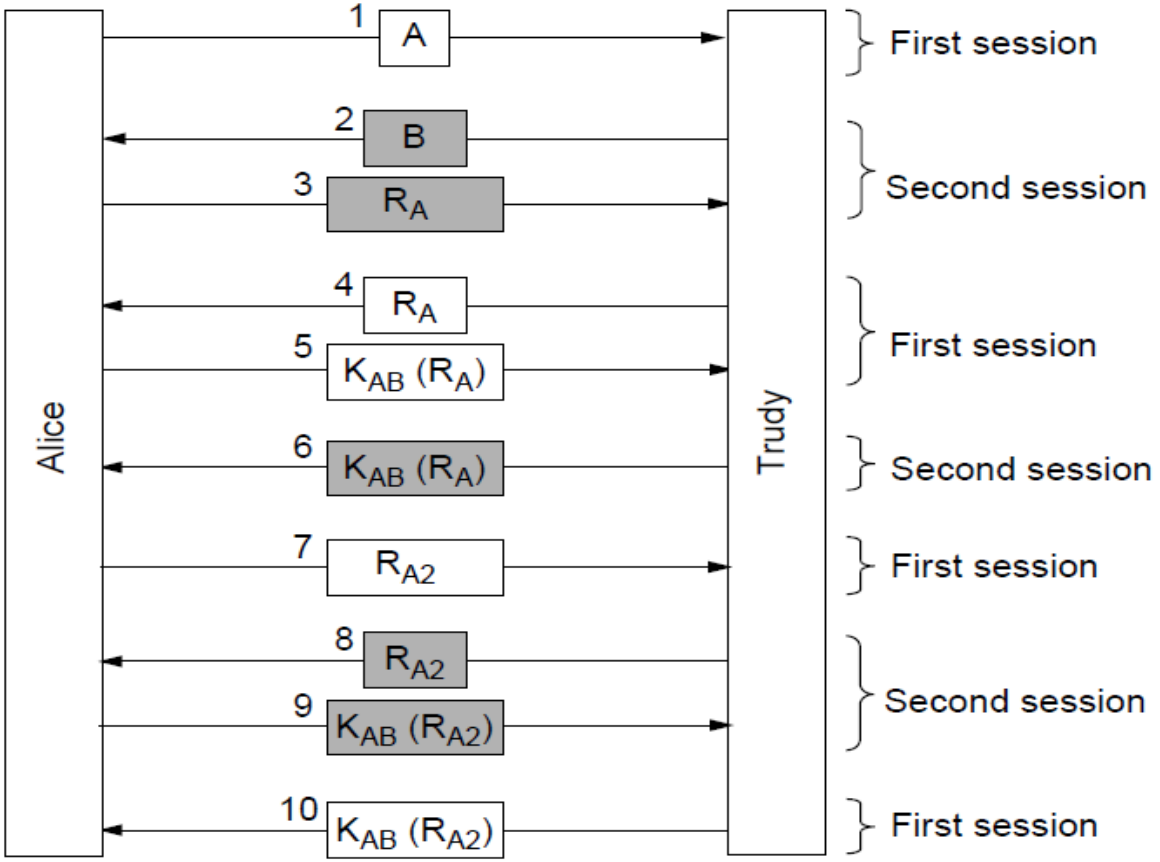
Shared Secret Key (4)

First attempt is also vulnerable to reflection attack!

- Trudy impersonates Bob to Alice after Alice initiates

Alice thinks she is talking to Bob

Alice thinks she is talking to Bob again



Shared Secret Key (5)

Moral: *Designing a correct authentication protocol is harder than it looks; errors are often subtle.*

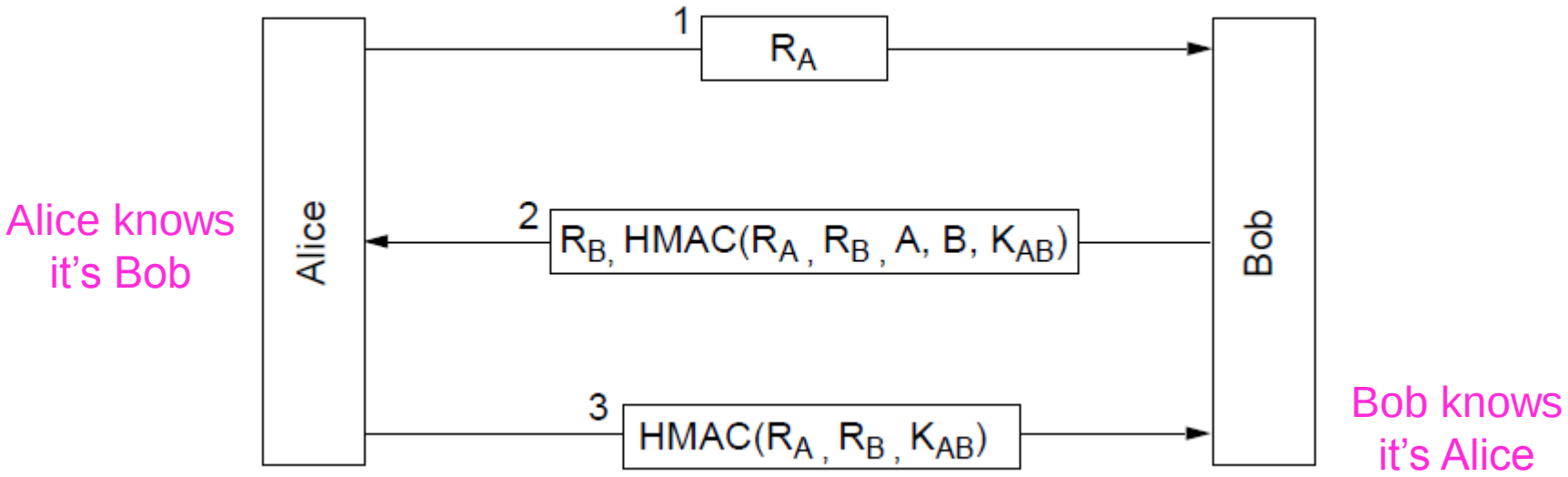
General design rules for authentication:

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

Shared Secret Key (6)

An authentication protocol that is not vulnerable

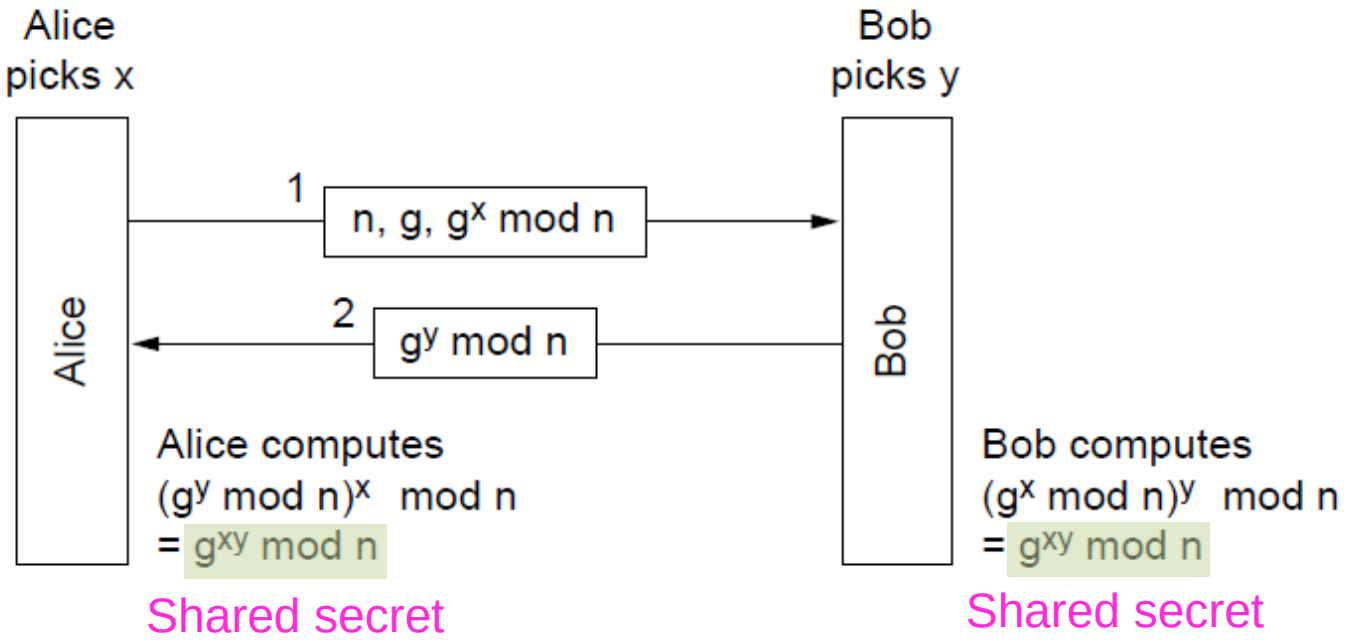
- HMAC (Hashed Message Authentication Code) is an authenticator, like a signature



Diffie-Hellman Key Exchange (1)

Lets two parties establish a shared secret

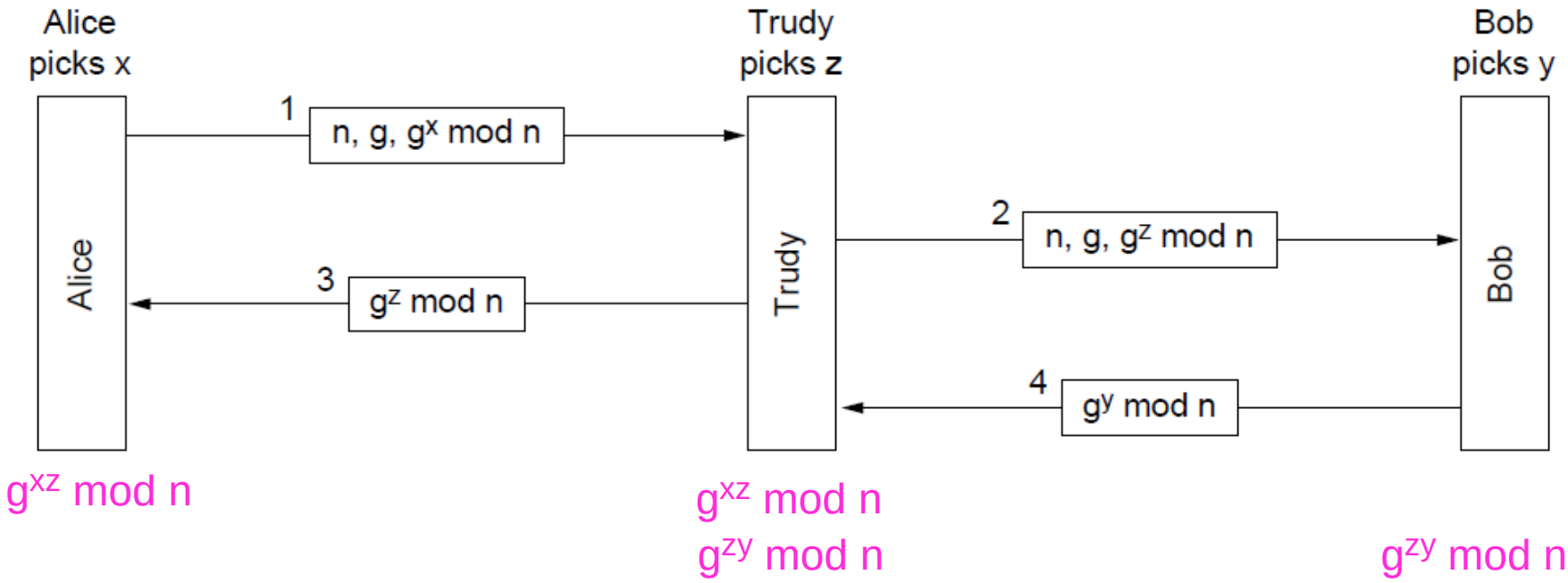
- Eavesdropper can't compute secret g^{xy} mod n without knowing x or y



Diffie-Hellman Key Exchange (2)

But it is vulnerable to a man-in-the-middle attack

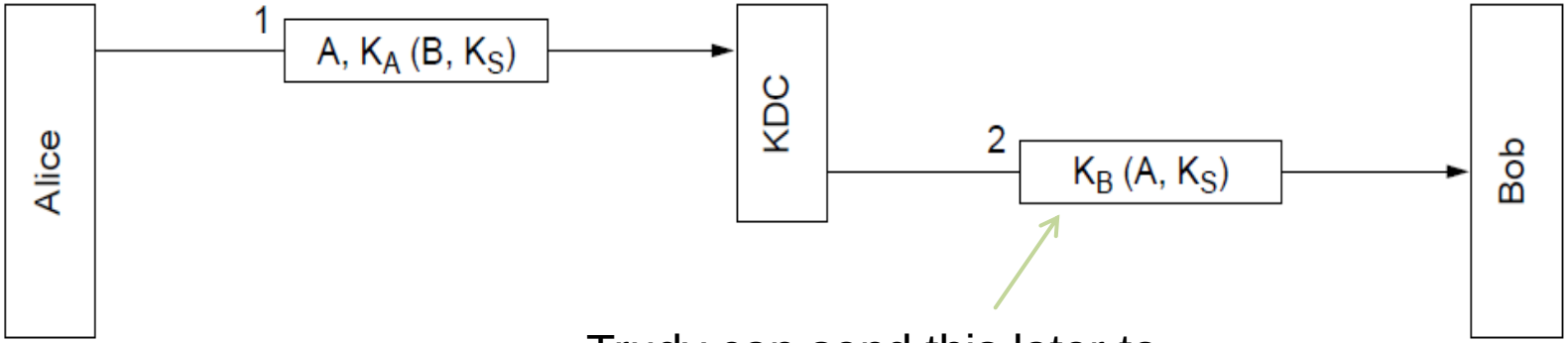
- Need to confirm identities, not just share a secret



KDC – Key Distribution Center (1)

Trusted KDC removes need for many shared secrets

- Alice and Bob share a secret only with KDC (K_A, K_B)
- End up with K_S, a shared secret session key
- First attempt below is vulnerable to replay attack in which Trudy captures and later replays messages



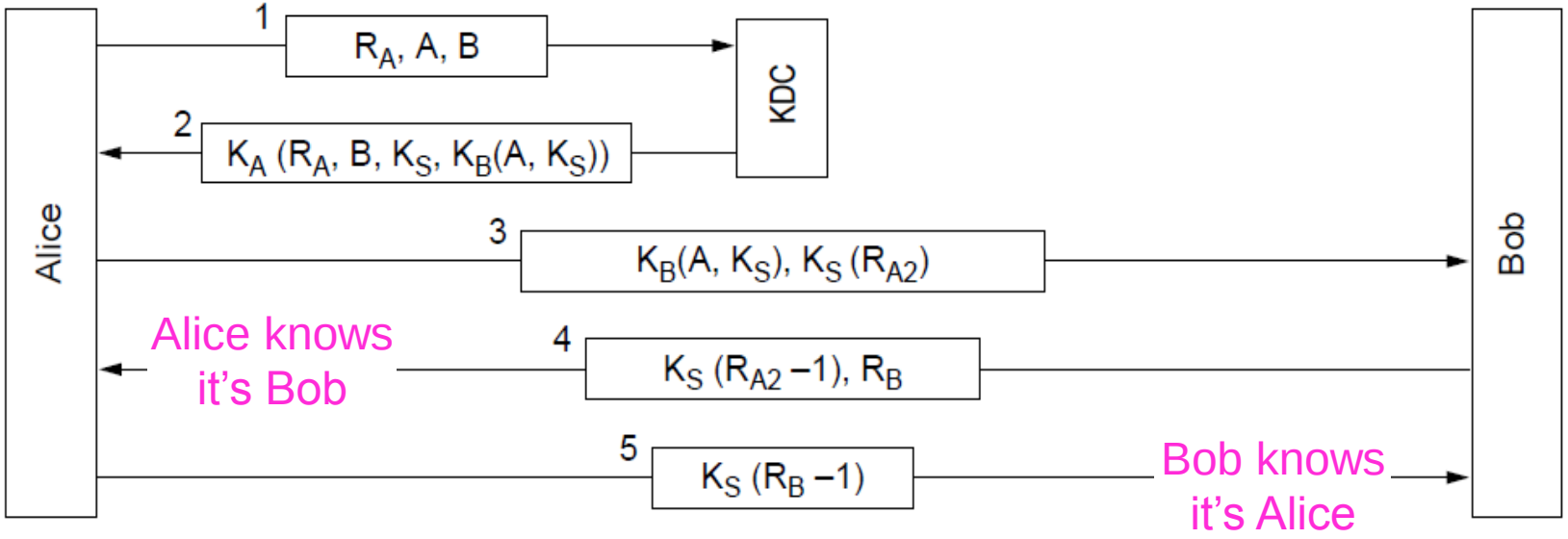
Alice has session key K_S

Bob has session key K_S

Key Distribution Center (2)

The Needham-Schroeder authentication protocol

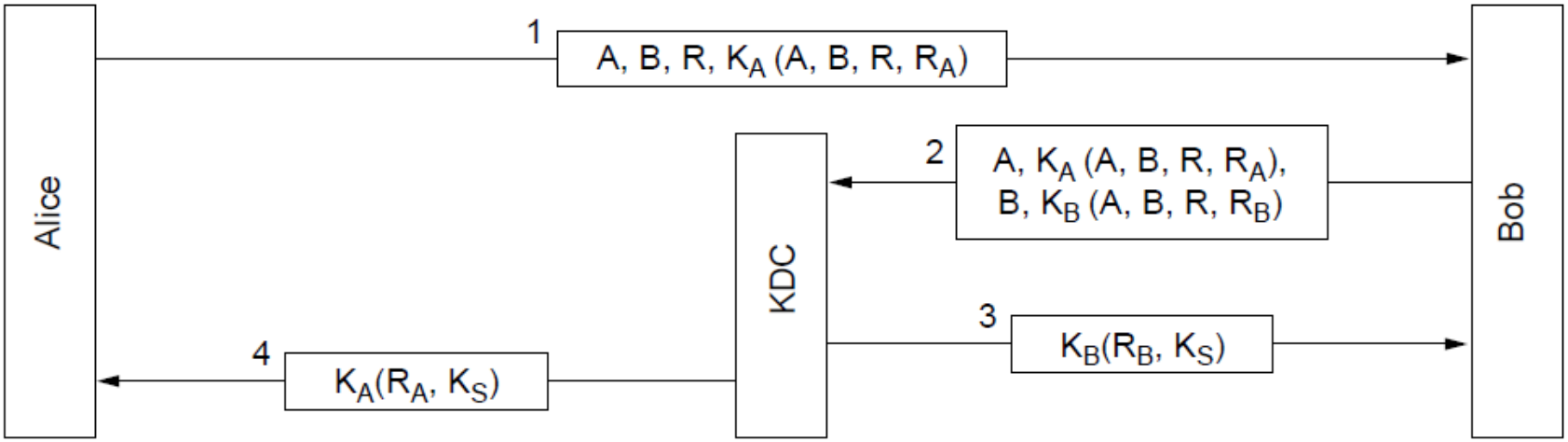
- Not vulnerable to replays; doesn't use timestamps



Key Distribution Center (3)

The Otway-Rees authentication protocol (simplified)

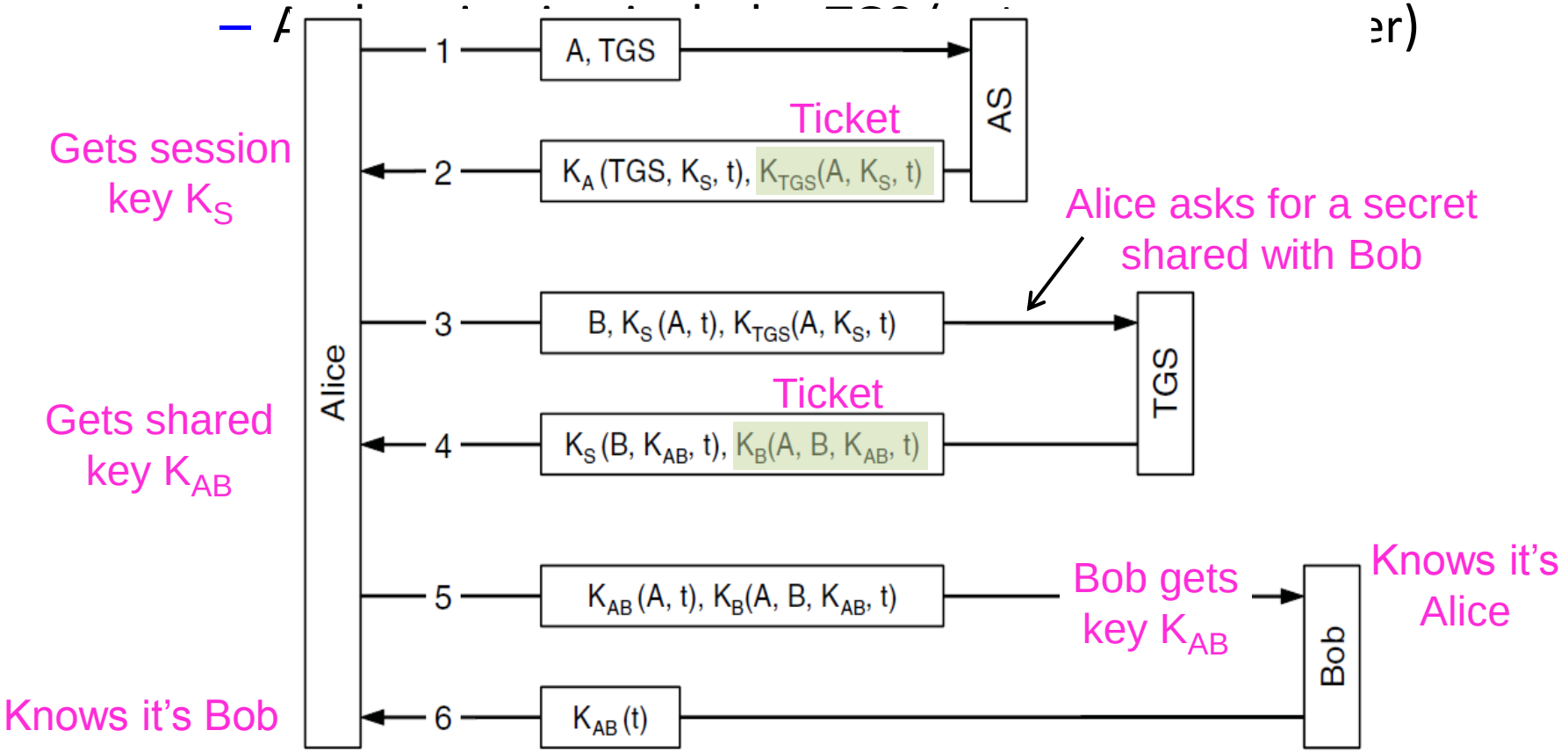
- Slightly stronger than previous; Trudy can't replay even if she obtains previous secret K_S



Kerberos

Kerberos V5 is a widely used protocol (e.g., Windows)

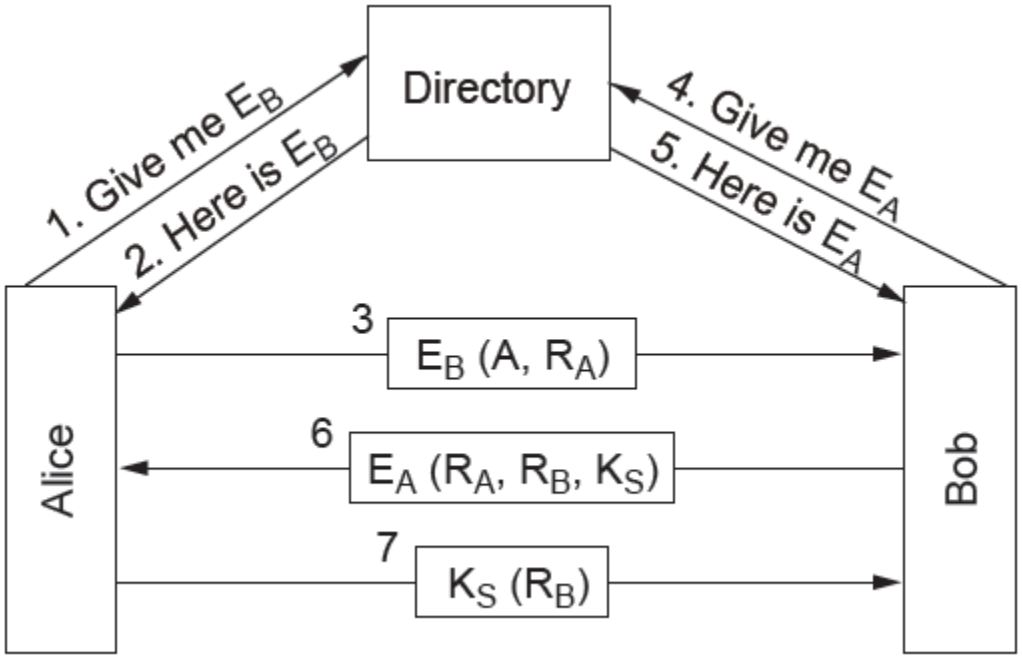
– A[illegible]er)



Public-Key Cryptography

Mutual authentication using public-key cryptography

- Alice and Bob get each other's public keys (E_A, E_B) from a



Email Security

Use of security for authenticated, confidential email

- PGP—Pretty Good Privacy »

PGP—Pretty Good Privacy (1)

PGP uses public- and symmetric-key cryptography for email secrecy and signatures; it also manages keys

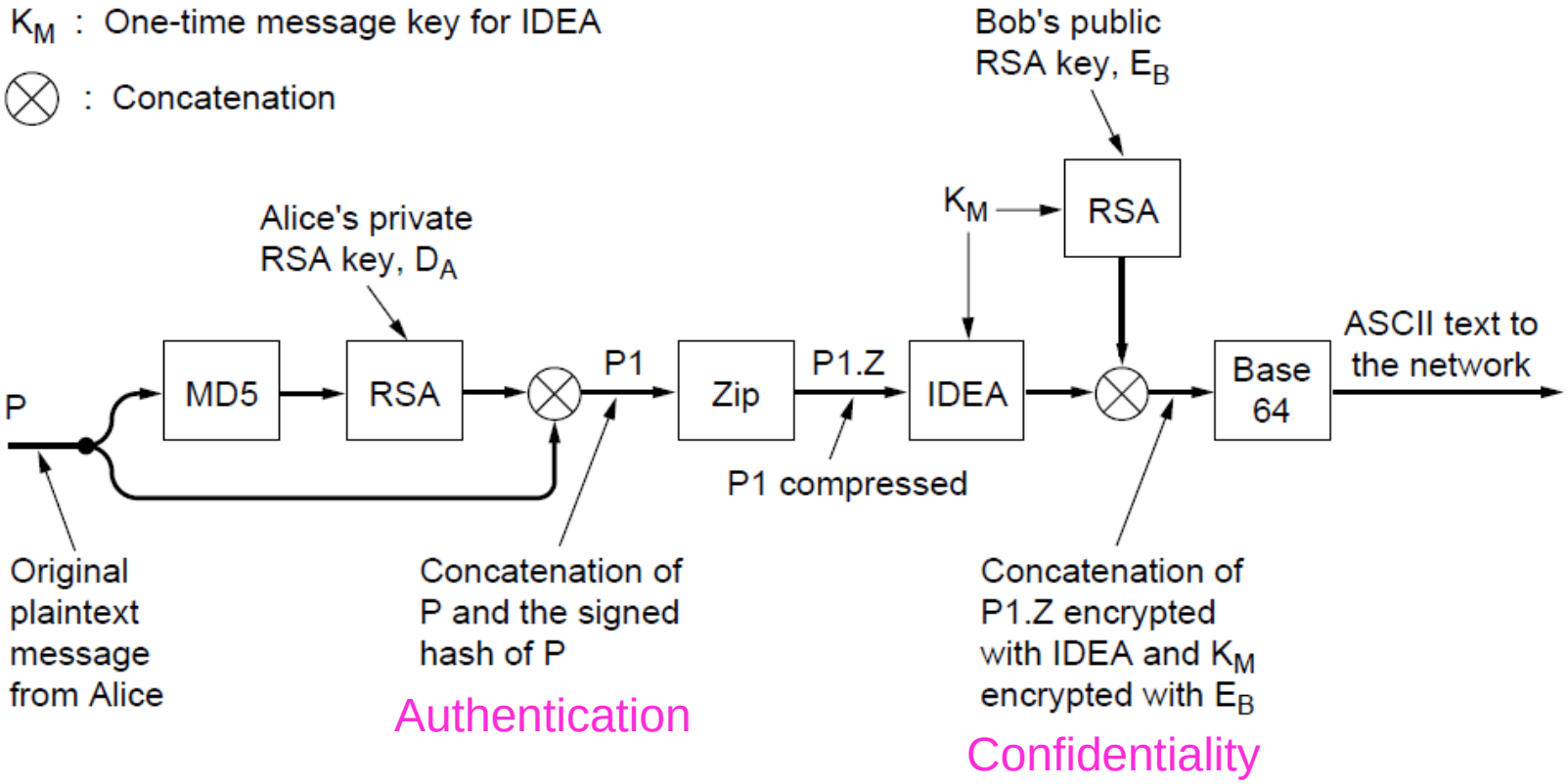
Levels of public-key strengths:

- 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 (2)

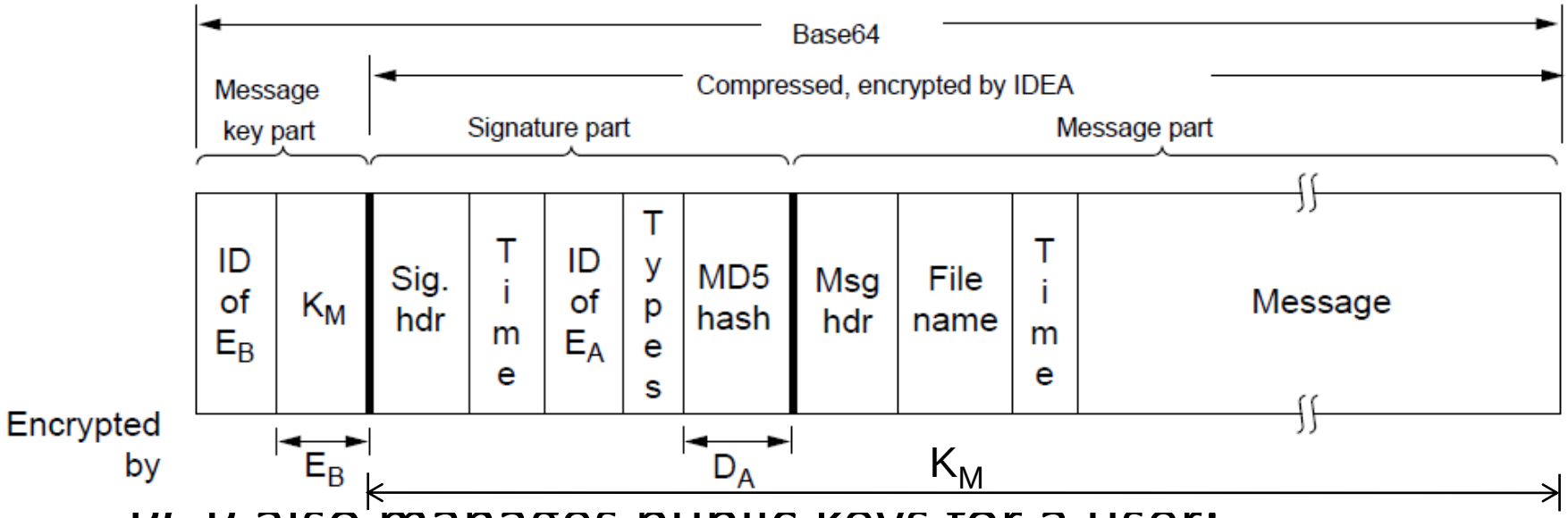
Signing and encrypting a message from Alice to Bob

- For speed, message symmetric-key IDEA encrypted with K_M; K_M is RSA public-key encrypted with K_B



PGP—Pretty Good Privacy (3)

Three parts of a PGP message and their encryption:



PGP also manages public keys for a user:

- Private key ring has user's public/private keys
- Public key ring has correspondent's public keys

Web Security

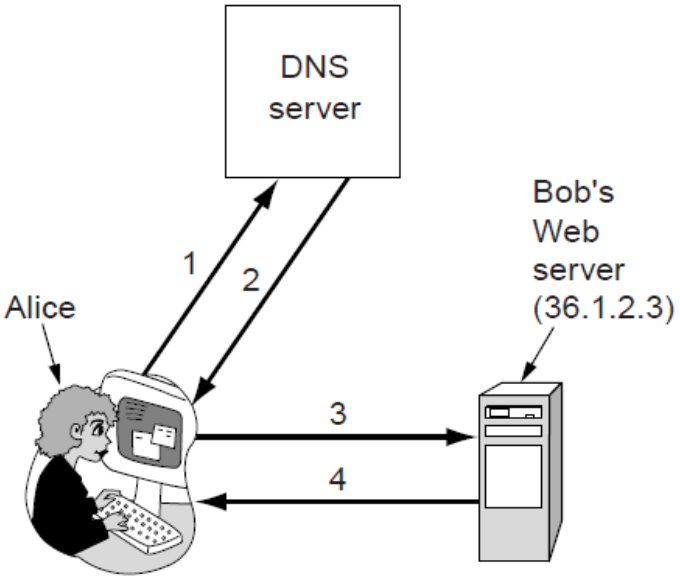
Applications of security to the Web

- Secure naming »
- SSL—Secure Sockets Layer »

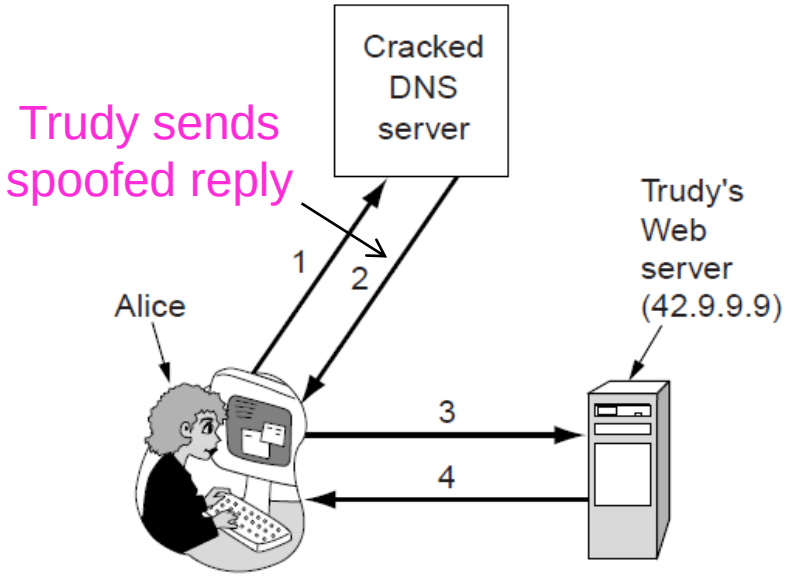
Many other issues with downloaded code

Secure Naming (1)

DNS names are included as part of URLs – so spoofing DNS resolution causes Alice contact



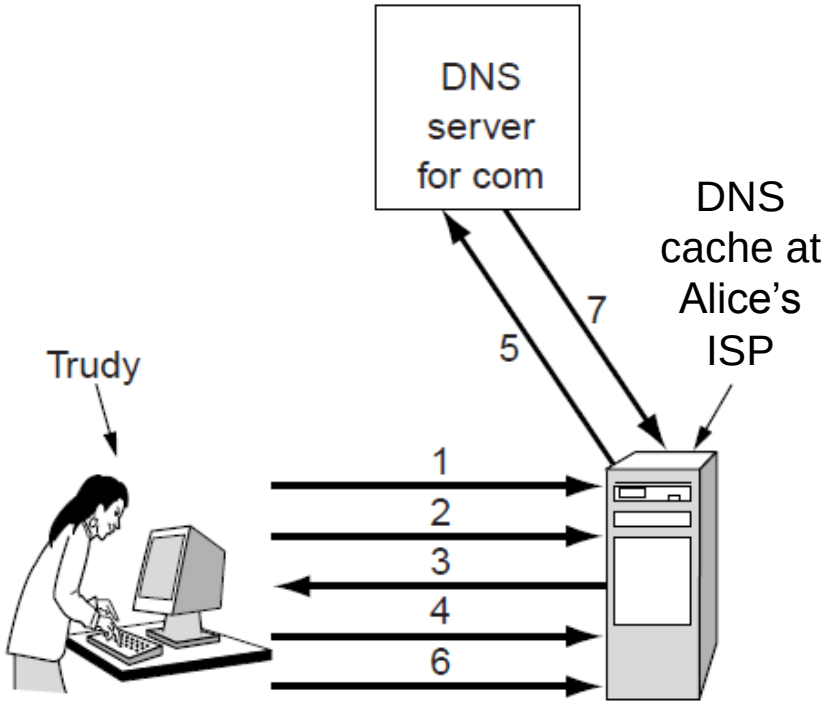
1. Give me Bob's IP address
2. 36.1.2.3 (Bob's IP address)
3. GET index.html
4. Bob's home page



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

Secure Naming (2)

How Trudy spoofs the DNS for *bob.com* in more detail



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)

Secure Naming (3)

DNSsec (DNS security) adds strong authenticity to DNS

- Responses are signed with public keys
- Public keys are included; client starts with top-level
- Also optional anti-spoofing to tie request/response

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...

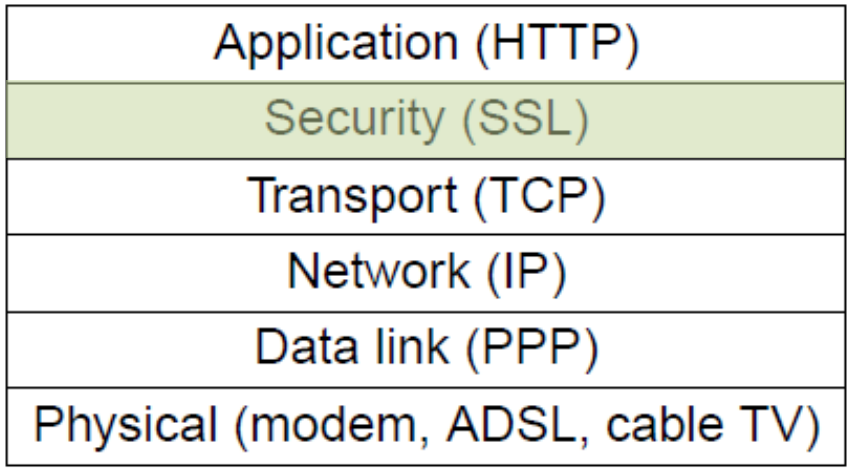
Resource Record set for *bob.com*.
Has Bob's public key (KEY), and is signed by .com server (SIG)

SSL—Secure Sockets Layer (1)

SSL provides an authenticated, secret connection between two sockets; uses public keys with X.509

- TLS (Transport Layer Security) is the IETF version

SSL runs on top of TCP and below the application →



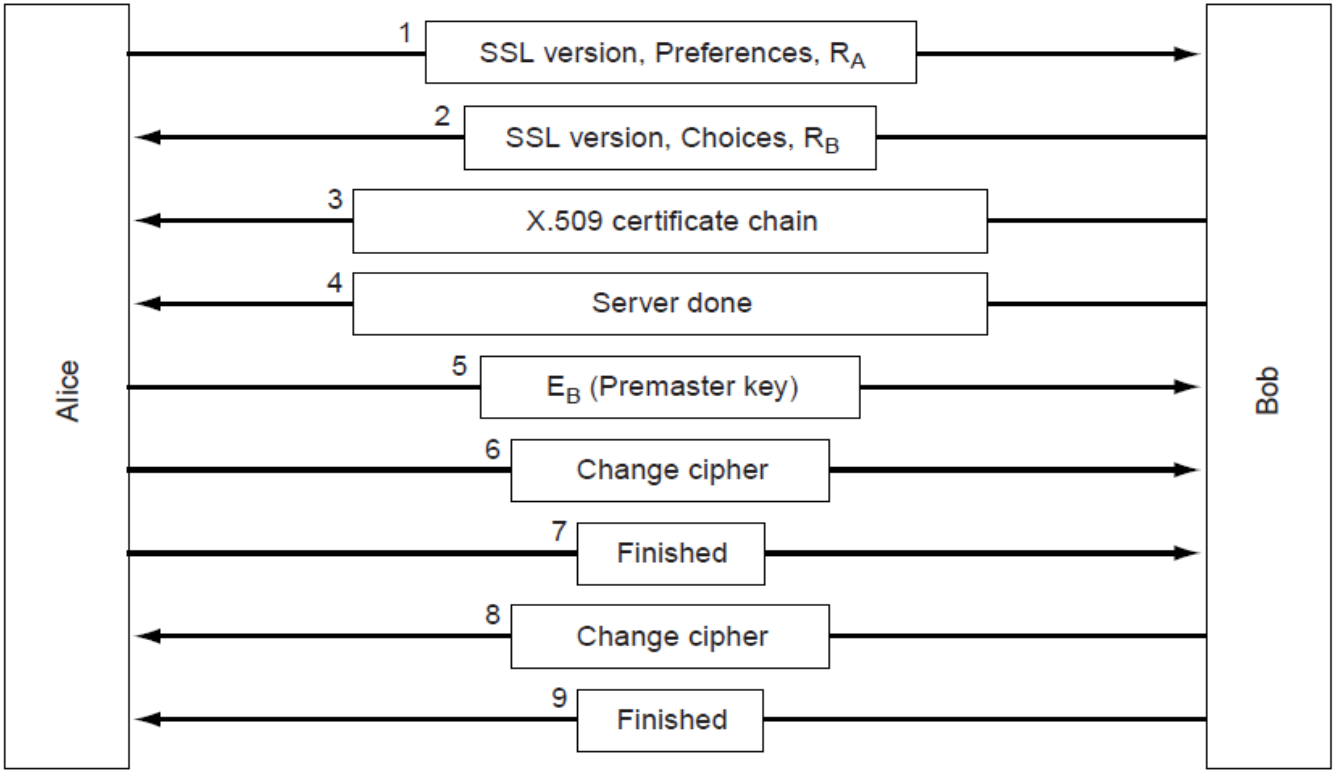
HTTPS means HTTP over SSL

SSL in the protocol stack

SSL—Secure Sockets Layer (2)

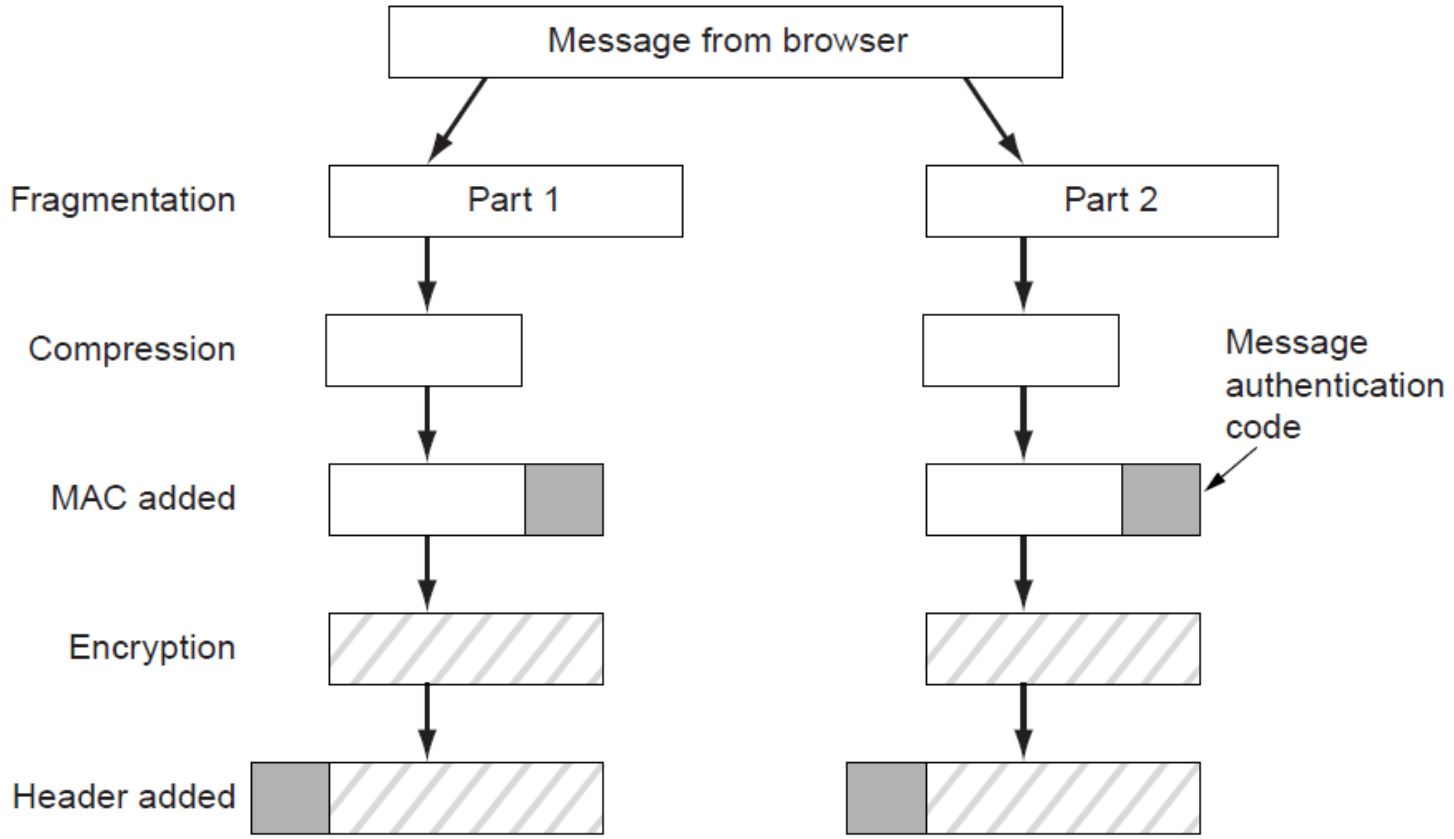
Phases in SSL V3 connection establishment (simplified)

- Only the client (Alice) authenticates the server (Bob)



SSL—Secure Sockets Layer (3)

Data transmission using SSL. Authentication and encryption for a connection use the session key.



Social Issues

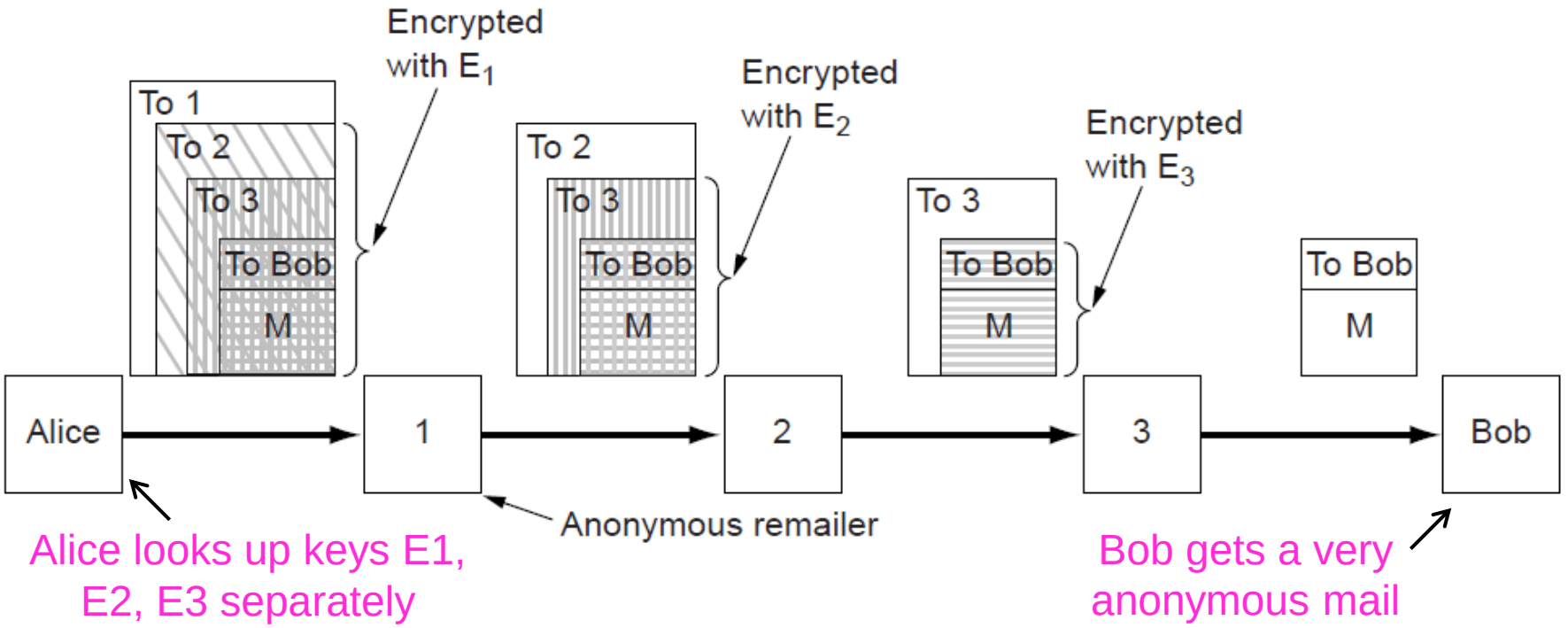
Networks give rise to many social issues

- Privacy »
- Freedom of speech »

Privacy

Anonymous remailers hide the identity of the sender

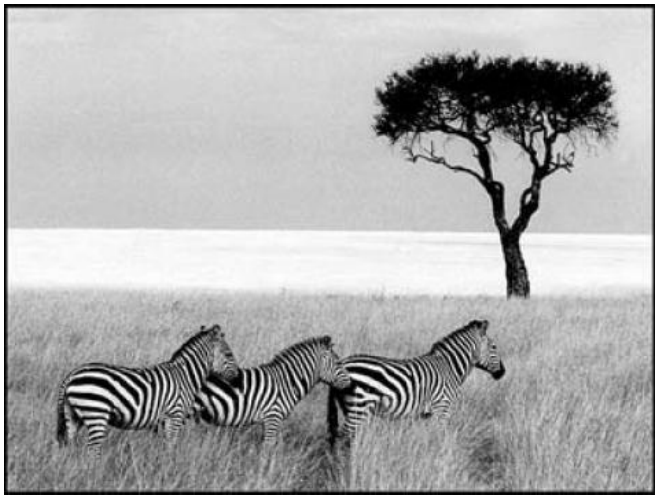
- Unlike PGP, which only hides message contents



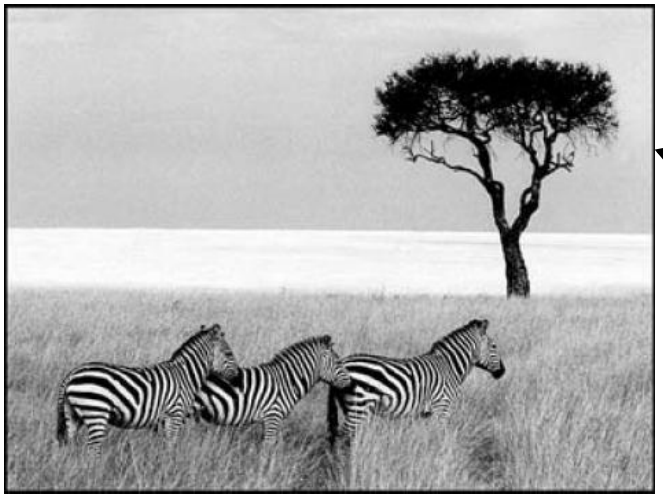
Freedom of Speech

Steganography hides messages on unrelated content

- Can help avoid censorship or protect ownership



"Three zebras and a tree"



Text hidden in low-order bits

"Three zebras and a tree," with five plays by Shakespeare"

End

Chapter 8