CSCI 460
Networks and Communications

Network Security

Humayun Kabir
Professor, CS, Vancouver Island University, BC, Canada

Outline

- Network Security Concepts
- Cryptography
  - Plain and Cipher Texts
  - Substitution Cipher
  - Transposition Cipher
  - Product Cipher
  - Digital Encryption Standard (DES)
- Public Key Algorithm: RSA
- Digital Signature
  - Public-Key Signatures
  - Message Digest

Network Security

Measures to prevent, detect, and correct security violations that involve the transmission of information in a network or interconnected networks

Computer Security Terminology

RFC 4949, *Internet Security Glossary*, May 2000

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

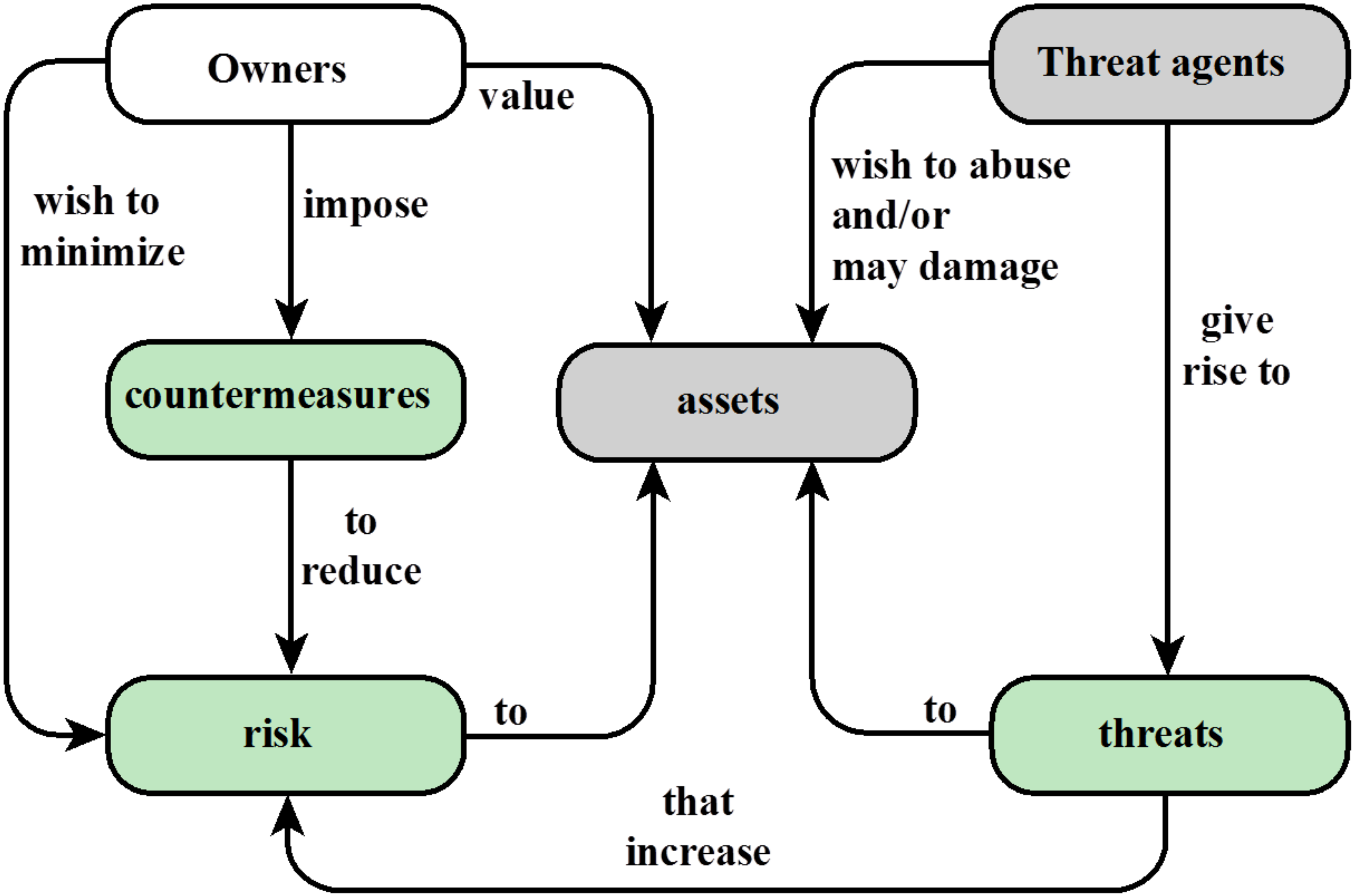
Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

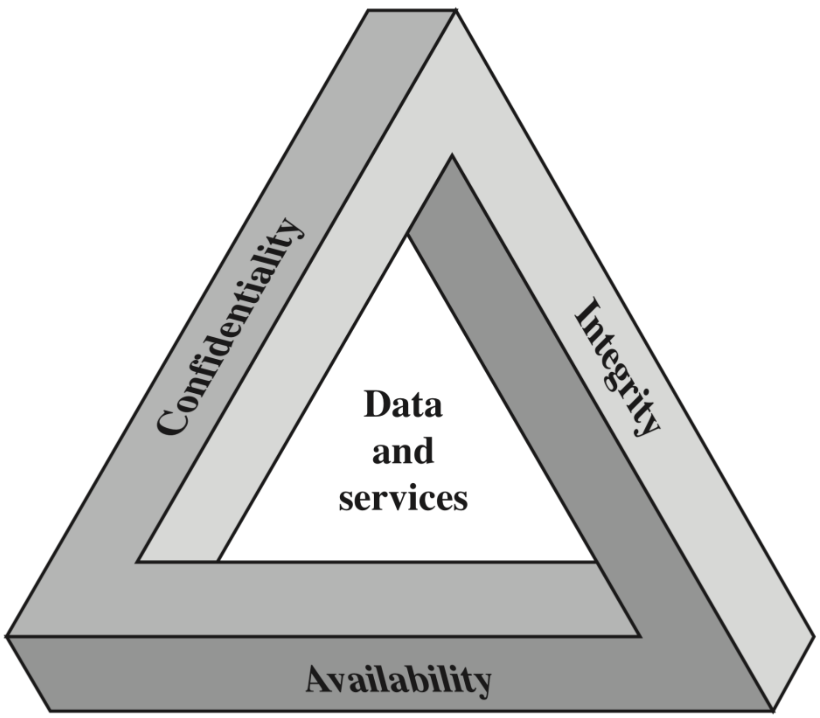
Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

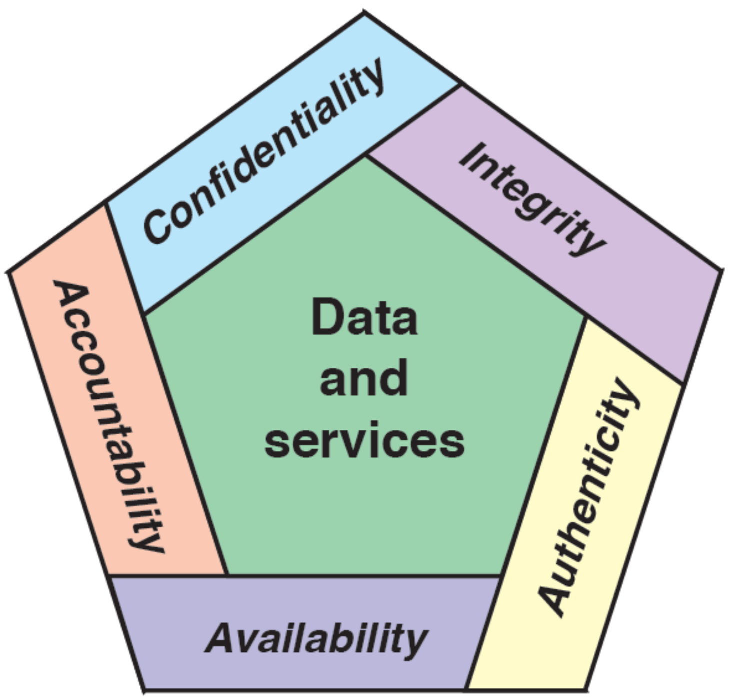
Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Relationships among the security Concepts



Security Objectives: CIA Triad and Beyond





Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Additional concepts:

Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- Being able to trace the responsible party/process/entity in case of a security incident or action.

Services, Mechanisms, Attacks

- 3 aspects of information security:
  - security attacks (and threats)
    - actions that (may) compromise security
  - security services
    - services counter to attacks
  - security mechanisms
    - used by services
    - e.g. secrecy is a service, encryption (a.k.a. encipherment) is a mechanism

Attacks

- Network Security
  - Active attacks
  - Passive attacks
- Passive attacks
  - interception of the messages
  - What can the attacker do?
    - use information internally
      - hard to understand
    - release the content
      - can be understood
    - traffic analysis
      - hard to avoid
  - Hard to detect, try to prevent

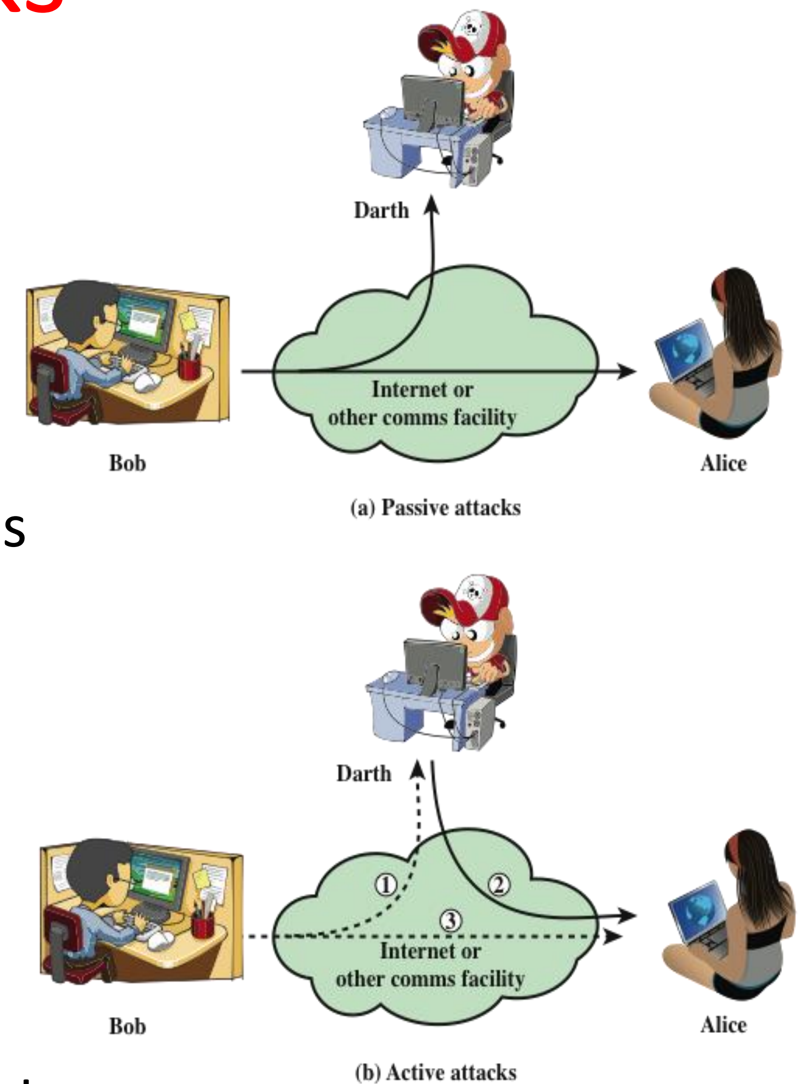
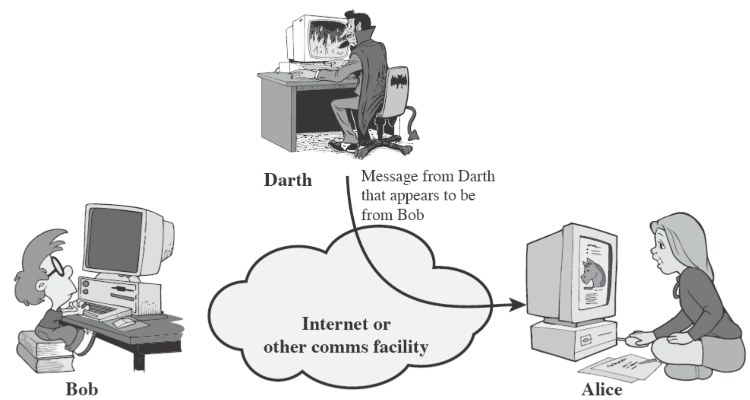
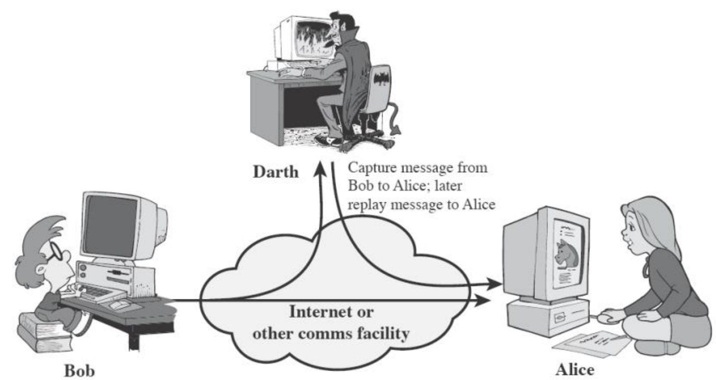


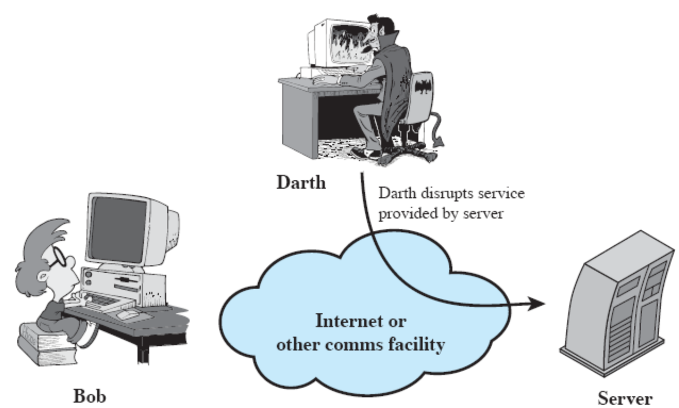
Figure 1.2 Security Attacks

Attacks

- Active attacks
  - Attacker actively manipulates the communication
  - Masquerade
    - pretend as someone else
    - possibly to get more privileges
  - Replay
    - passively capture data and send later
  - Denial-of-service
    - prevention the normal use of servers, end users, or network itself

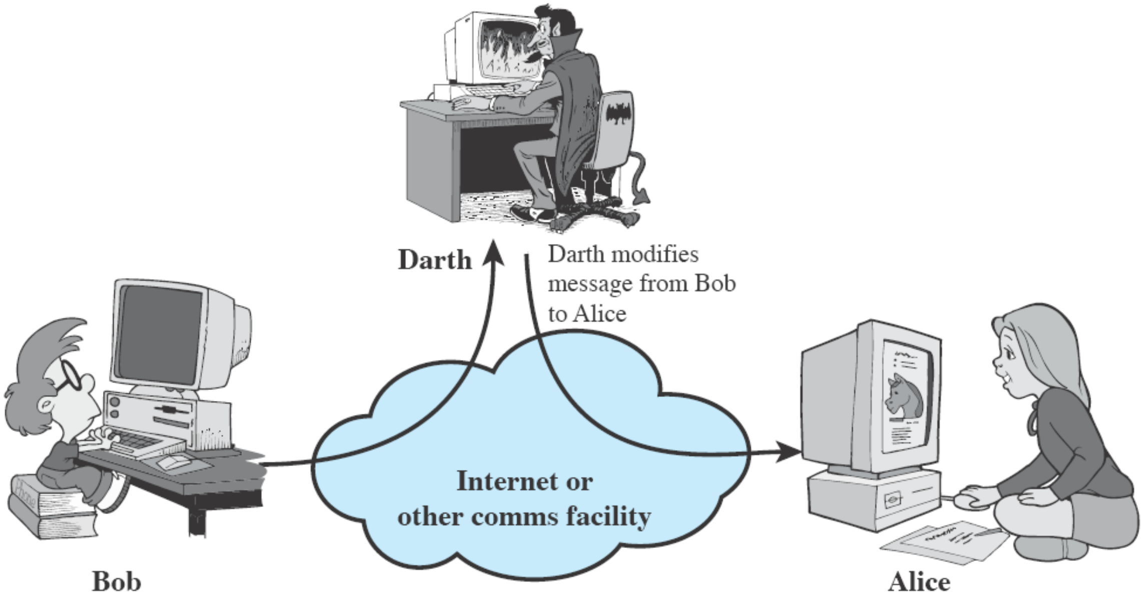






Attacks

- Active attacks (cont'd)
  - deny
    - repudiate sending/receiving a message later
  - modification
    - change the content of a message



Security Services

- to prevent or detect attacks
- to enhance the security
- replicate functions of physical documents
  - e.g.
    - have signatures, dates
    - need protection from disclosure, tampering, or destruction
    - notarize
    - record

Basic Security Services

- Authentication
  - assurance that the communicating entity is the one it claims to be
  - peer entity authentication
    - mutual confidence in the identities of the parties involved in a connection
  - Data-origin authentication
    - assurance about the source of the received data
- Access Control
  - prevention of the unauthorized use of a resource
  - to achieve this, each entity trying to gain access must first be identified and authenticated, so that access rights can be tailored to the individual

Basic Security Services

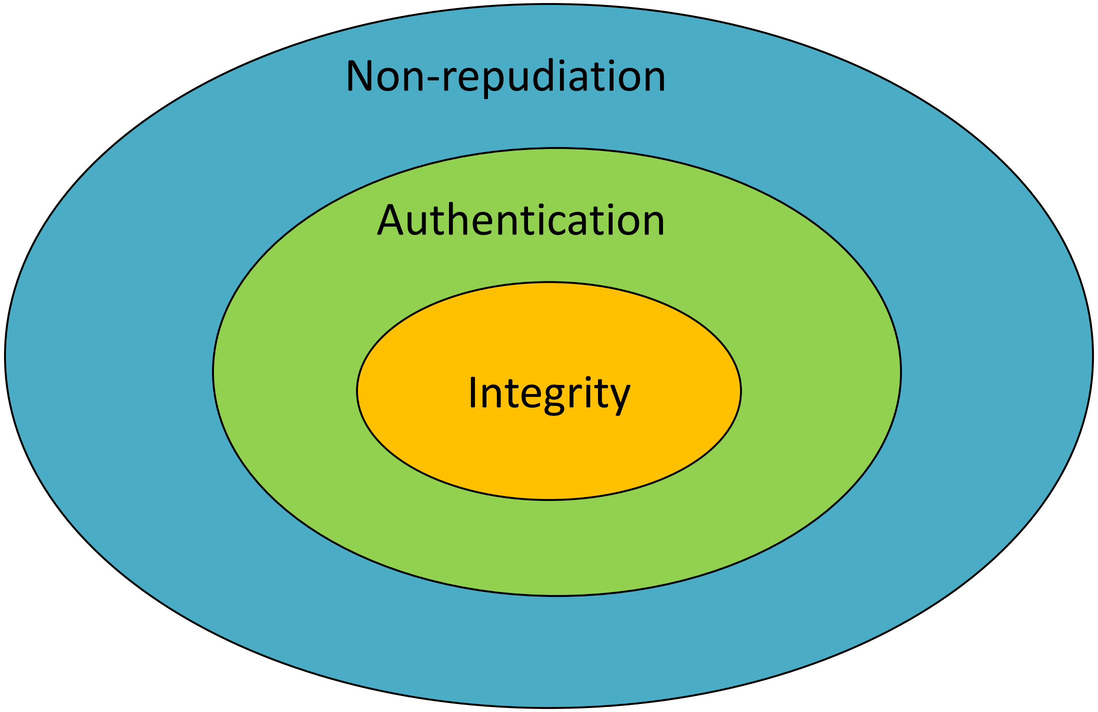
- Data Confidentiality
  - protection of data from unauthorized disclosure (against eavesdropping)
  - traffic flow confidentiality is one step ahead
    - this requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility
- Data Integrity
  - assurance that data received are exactly as sent by an authorized sender
  - i.e. no modification, insertion, deletion, or replay

Basic Security Services

- Non-Repudiation
  - protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

Relationships

- among integrity, data-origin authentication and non-repudiation



Security Mechanisms

- Cryptographic Techniques
  - Product Cipher, Public Key Algorithm
- Software and hardware for access limitations
  - Firewalls
- Intrusion Detection and Prevention Systems
- Traffic Padding
  - against traffic analysis
- Hardware for authentication
  - Smartcards, security tokens
- Security Policies / Access Control
  - define who has access to which resources.
- Physical security
  - Keep it in a safe place with limited and authorized physical access

Cryptographic Security Mechanisms

- Encryption (a.k.a. Encipherment)
  - use of mathematical algorithms to transform data into a form that is not readily intelligible
    - keys are involved

Cryptography: 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

Cryptography: Transposition Ciphers

Transposition ciphers reorder letters to

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

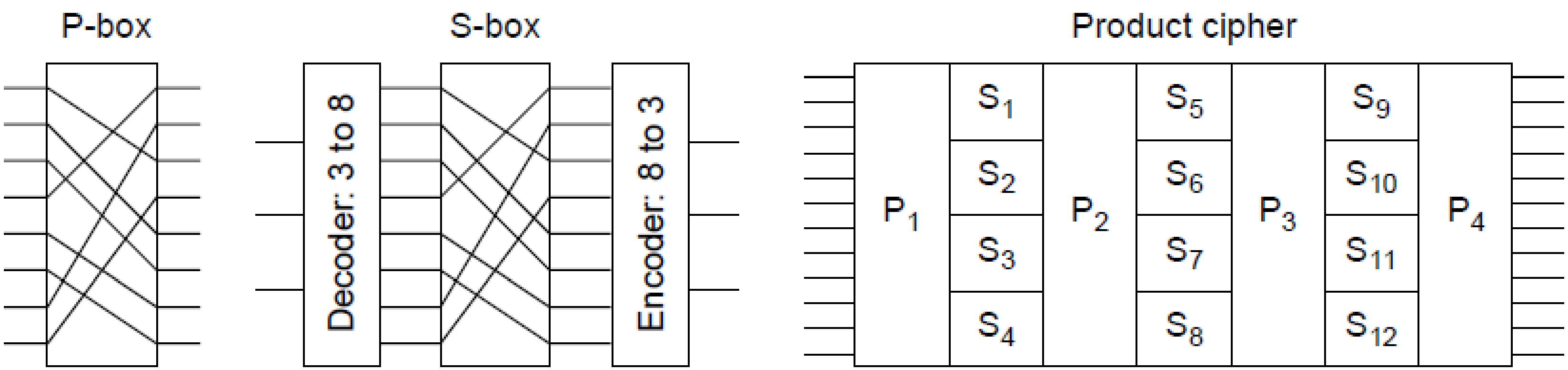
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Column 5 ESILYNTW, 6 RNNTSOWD, 7 PAEDOBUO, 8 ERIRICXB

Simple column transposition cipher

Cryptography: Product Cipher

Product cipher combines transpositions/substitutions



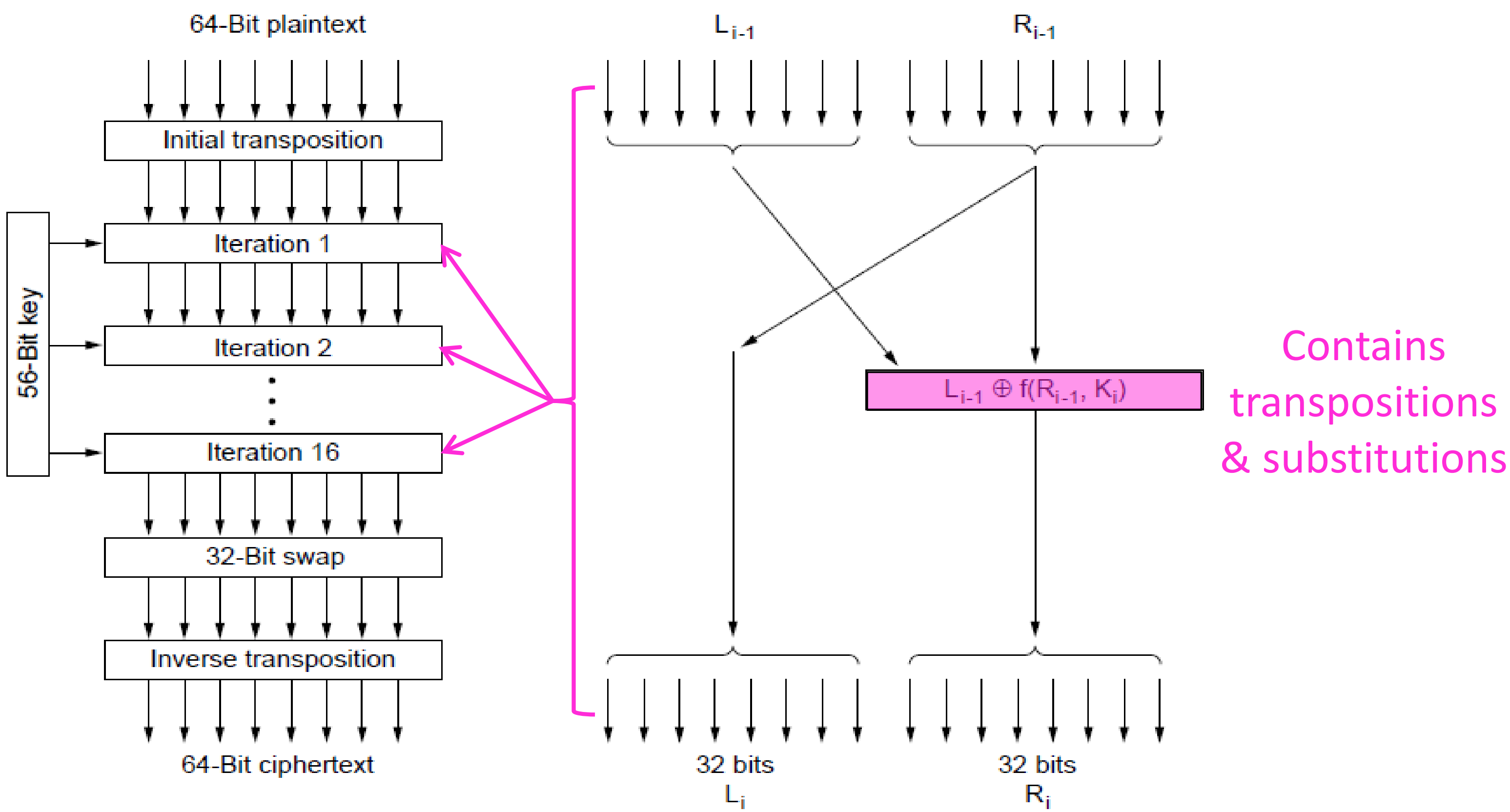
Permutation (transposition) box

Substitution box

Product with multiple P- and S-boxes

Data Encryption Standard (DES)

- A symmetric cipher, uses the same secret key to encrypt and decrypt
- Operates on a block at a time



DES steps

A single iteration

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

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

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

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 (Symbolic through P^3 (mod 33))

Receiver's computation (P^3 (mod 33) through Symbolic)

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

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

Digital Signatures

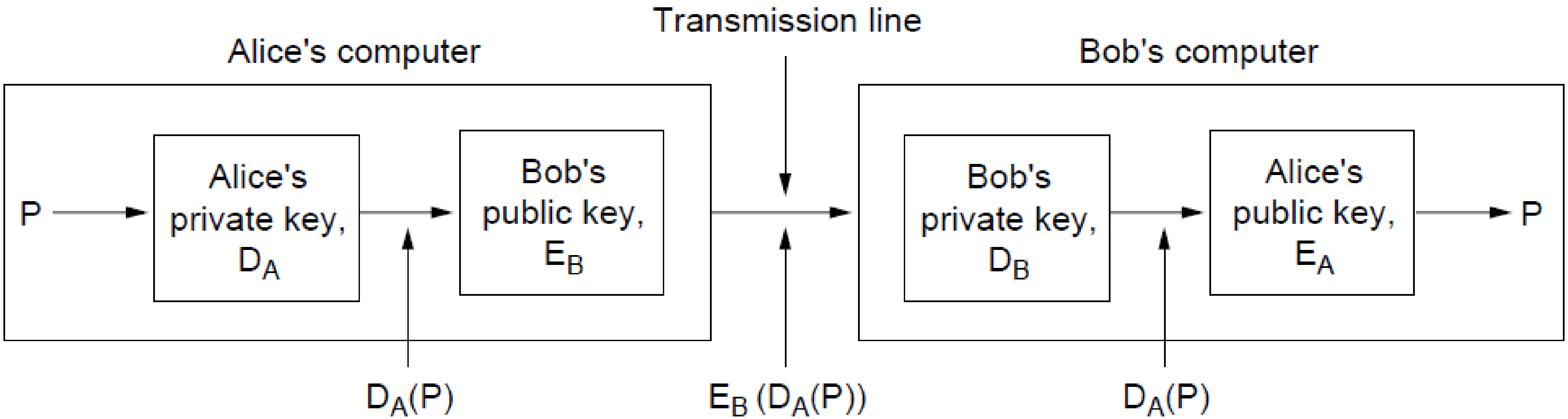
Requirements for a signature:

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

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
- RSA & DSS (Digital Signature Standard) widely used



Message Digests

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

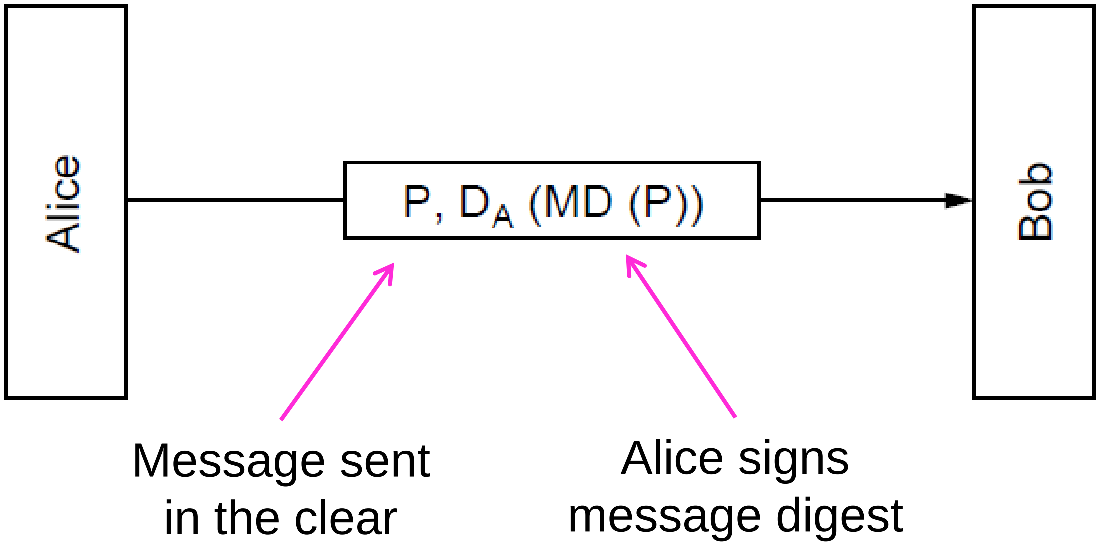
- Given P, easy to compute MD(P).
- Given MD(P), effectively impossible to find P.
- Given P no one can find P′ so that MD(P′) = MD(P).
- Changing 1 bit of P produces very different MD.

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

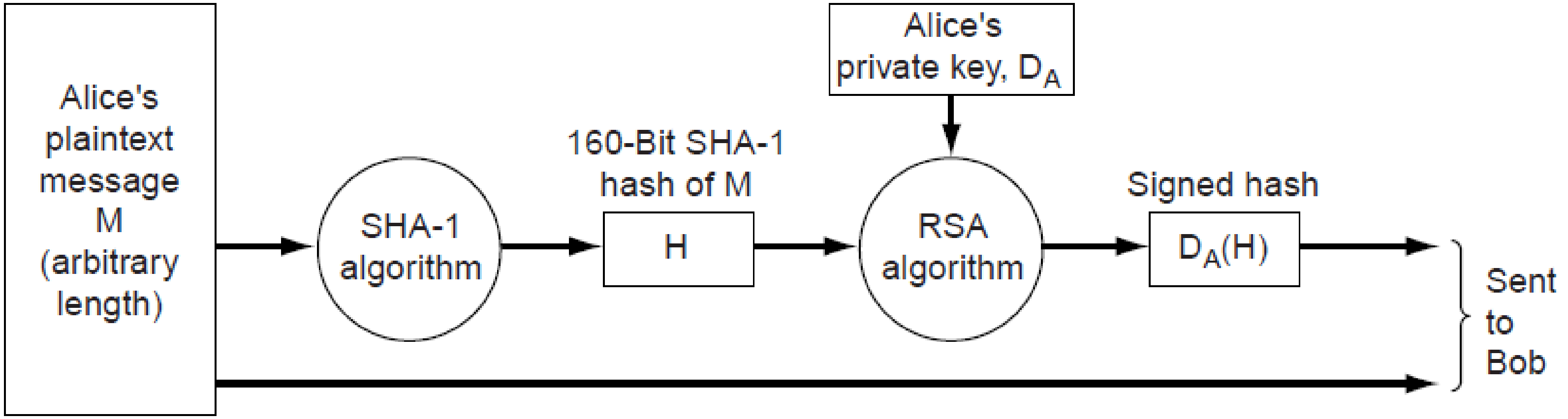
Message Digests

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



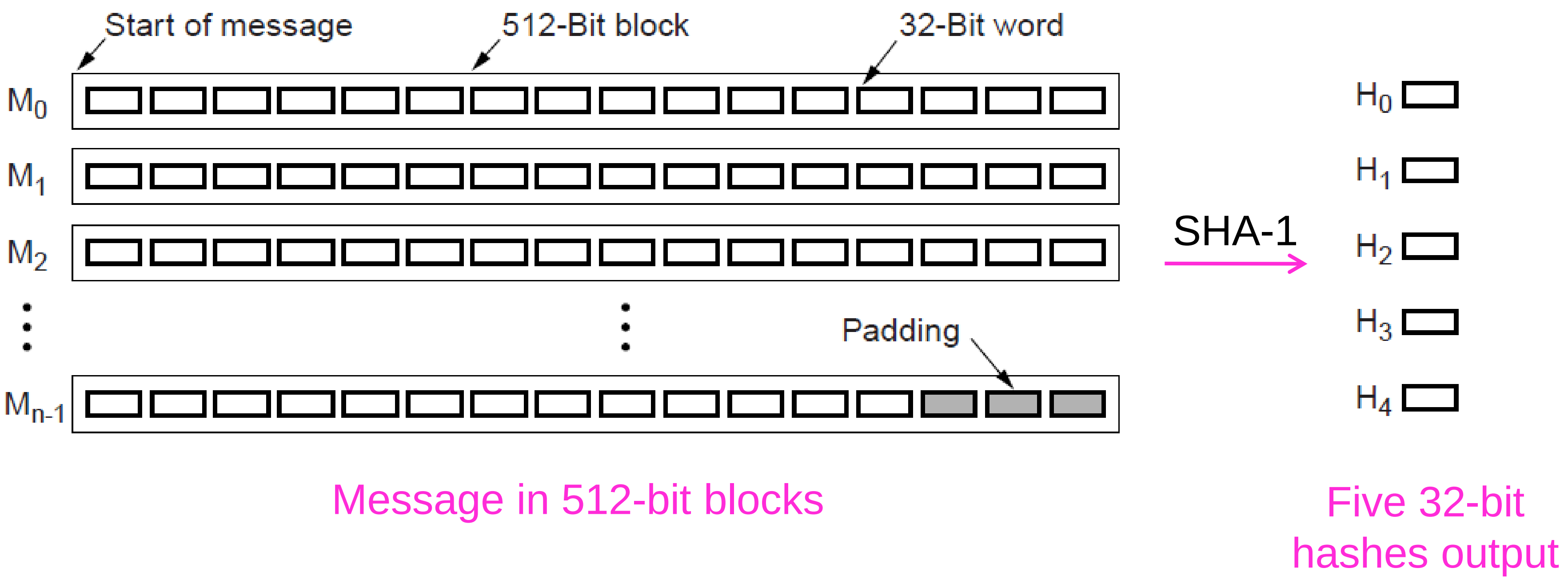
Message Digests

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



Message Digests

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



Summary

- Network Security Concepts
- Cryptography
  - Plain and Cipher Texts
  - Substitution Cipher
  - Transposition Cipher
  - Product Cipher
  - Digital Encryption Standard (DES)
- Public-Key Algorithm: RSA
- Digital Signature
  - Public-Key Signatures
  - Message Digest

End of CSCI 460

Thank You