

Introduction to Information Security



Andy Ju An Wang
Department of Information Technology
School of Computing and Software Engineering

Agenda

- Why life-long learning is important?
- Why Information Security is important?
- What are the fundamental concepts in Information Security?
- Why Information Security is challenging?
- Conclusion and Discussion

Education Changes

- According to former Secretary of Education Richard Riley, the top 10 in-demand jobs in 2010 didn't exist in 2004.
- We are currently preparing students for jobs that don't yet exist . . .
- Using technologies that haven't been invented . . .
- In order to solve problems we don't even know are problems yet.

Society Changes

- 1 out of every 8 couples married in the U.S. last year met online.
- There are over 100 million registered users of MySpace. (August 2006)
- The average MySpace page is visited 30 times a day.

Pervasive Data

- We are living in *exponential* times.
- There are over 2.7 billion searches performed on Google each month.
- To whom were these questions addressed Before Google?
- The number of text messages sent and received every day exceeds the population of the planet.

Information Explosion

- There are about 540,000 words in the English language, about 5 times as many as during Shakespeare's time.
- More than 3,000 new books are published daily.
- It's estimated that a week's worth of New York Times, Contains more information than a person was likely to come across in a *lifetime* in the 18th century.

Information Explosion

- It's estimated that 40 exabytes (that's 4.0×10^{19}) of unique new information will be generated worldwide this year.
- That's estimated to be more than in the previous 5,000 years.
- The amount of new technical information is doubling every 2 years.
- It's predicted to double every 72 hours by 2010.

Technology Changes

- **Third generation fiber optics has recently been separately tested by NEC and Alcatel that pushes 10 trillion bits per second down one strand of fiber.**
- **That's 1,900 CDs or 150 million simultaneous phone calls every second.**
- **It's currently tripling about every 6 months and is expected to do so for at least the next 20 years.**

Technology Changes

- 47 million laptops were shipped worldwide last year.
- The \$100 laptop project is expecting to ship between 50 and 100 million laptops a year to children in underdeveloped countries.

Future Predictions

- By 2013 a supercomputer will be built that exceeds the computation capability of the Human Brain.
- By 2023, a \$1,000 computer will exceed the computation capability of the Human Brain.
- By 2049 a \$1,000 computer will exceed the computational capabilities of the *human race*.

What does it all mean?

- **Shift Happens.**
- **Life-long learning.**
- **Specialization / generalization.**
- **Information technology / security**

Information Security "Vision"

- CIA
- Confidentiality
- Integrity
- Availability
- CIA is the most important aspects in security.
- How do you realize this vision?
 - Set up your goals, objectives, and action plans.

Goals of Security

- Prevention
 - Prevent attackers or actions from violating the CIA of your information assets
- Detection
 - Detect any violations that compromise the CIA of your information assets
- Recovery
 - Stop attack, assess and repair damage
 - Continue to function correctly even if attack succeeds

Other goals

- **Non-repudiation**
 - Ensuring that communication parties can't later deny that the exchange took place (or when the exchange took place).
- **Legitimate use**
 - Ensuring that resources are not used by unauthorized parties or in unauthorized ways.
 - Examples:
 - Printer and disk quotas.
 - Spam-filters in E-mail servers.
- **Good Performance**

Objectives of Security

- Provide *security services* that enhance the CIA of your information assets.
- Develop *security policies* that define what is allowed and what is not for an organization.
- Implement *security functions* to support security services
- Provide *security mechanisms* to enforce security policies

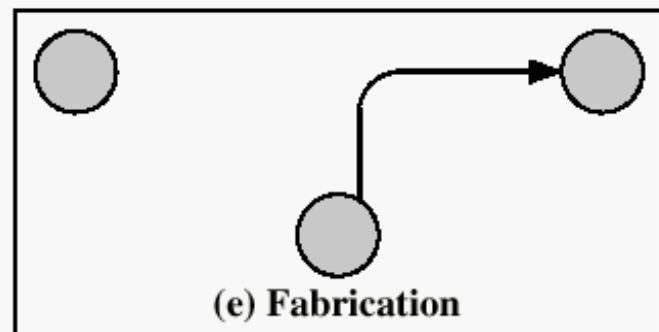
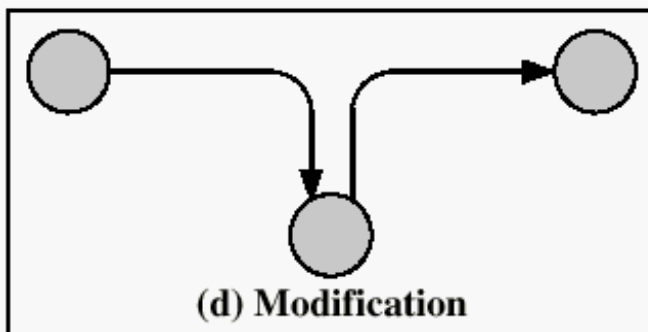
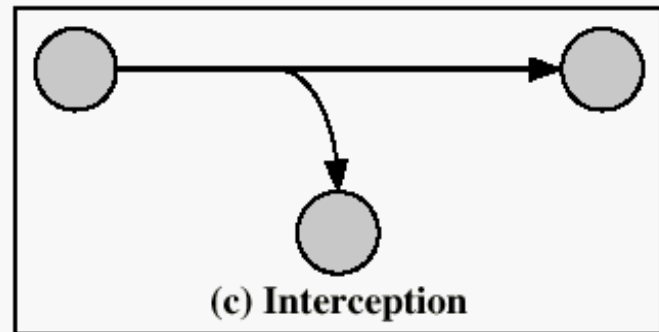
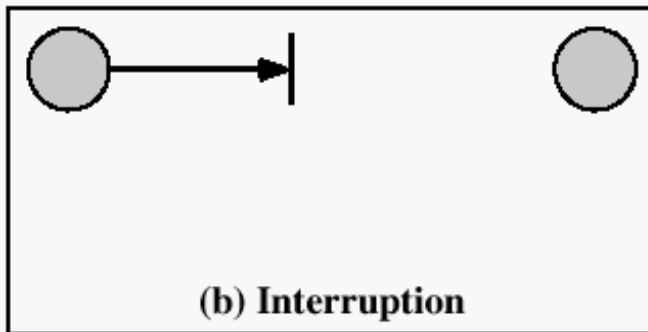
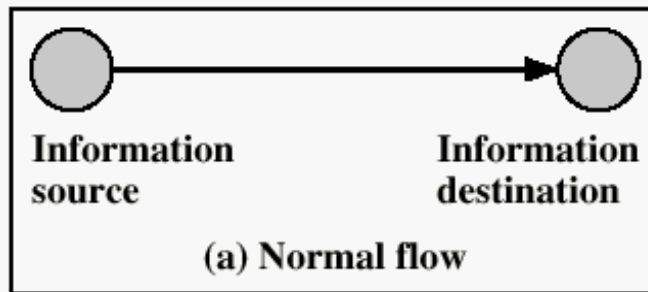


Figure 1.1 Security Threats

Common Controls

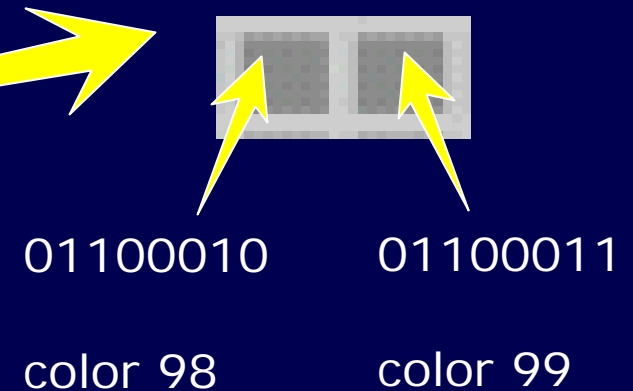
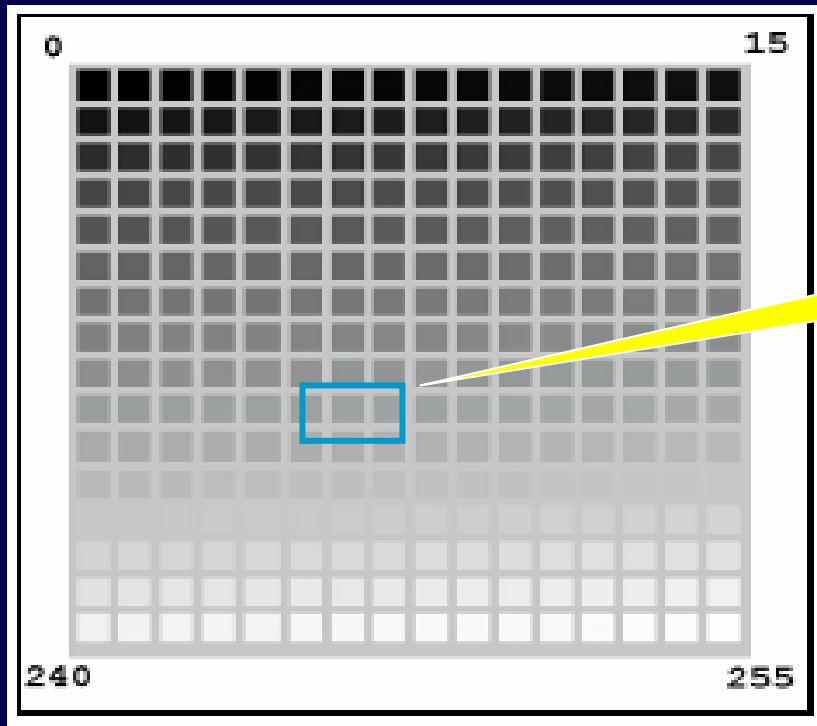
- Encryption
- Software controls
- Hardware controls
- Policies and procedures
- Physical controls

What is cryptology?

- Greek: “krypto” = hide
- Cryptology – science of hiding
 - = cryptography + cryptanalysis + steganography
- Cryptography – secret writing
- Cryptanalysis – analyzing (breaking) secrets
 - *Cryptanalysis* is what attacker does
 - *Decipher* or *Decryption* is what legitimate receiver does

Embedding data

Image: 256 Gray Scale Pallet. Audio, Video, etc.



Why cryptography?

- Network information needs to be communicated through insecure channel.
- Stored information may be accessed without proper authorization.
- Cryptography is a *systematic* way to make that harder.

Conventional encryption principles

- An encryption scheme has five ingredients:
 - Plaintext
 - Encryption algorithm
 - Secret Key
 - Ciphertext
 - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm
- Three kinds of cryptography: 0 key, 1 key, 2 keys

0 key: Hash Functions

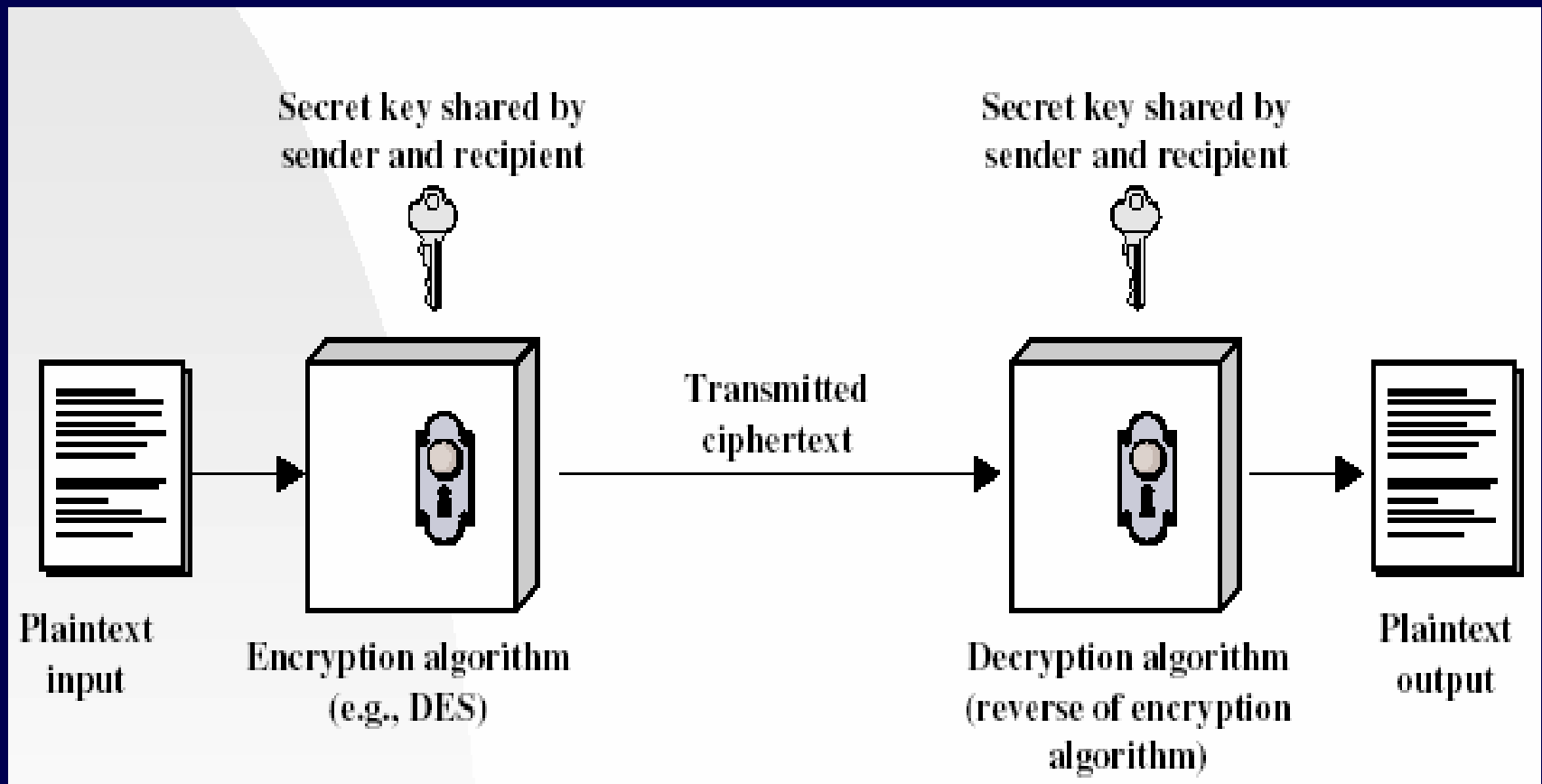


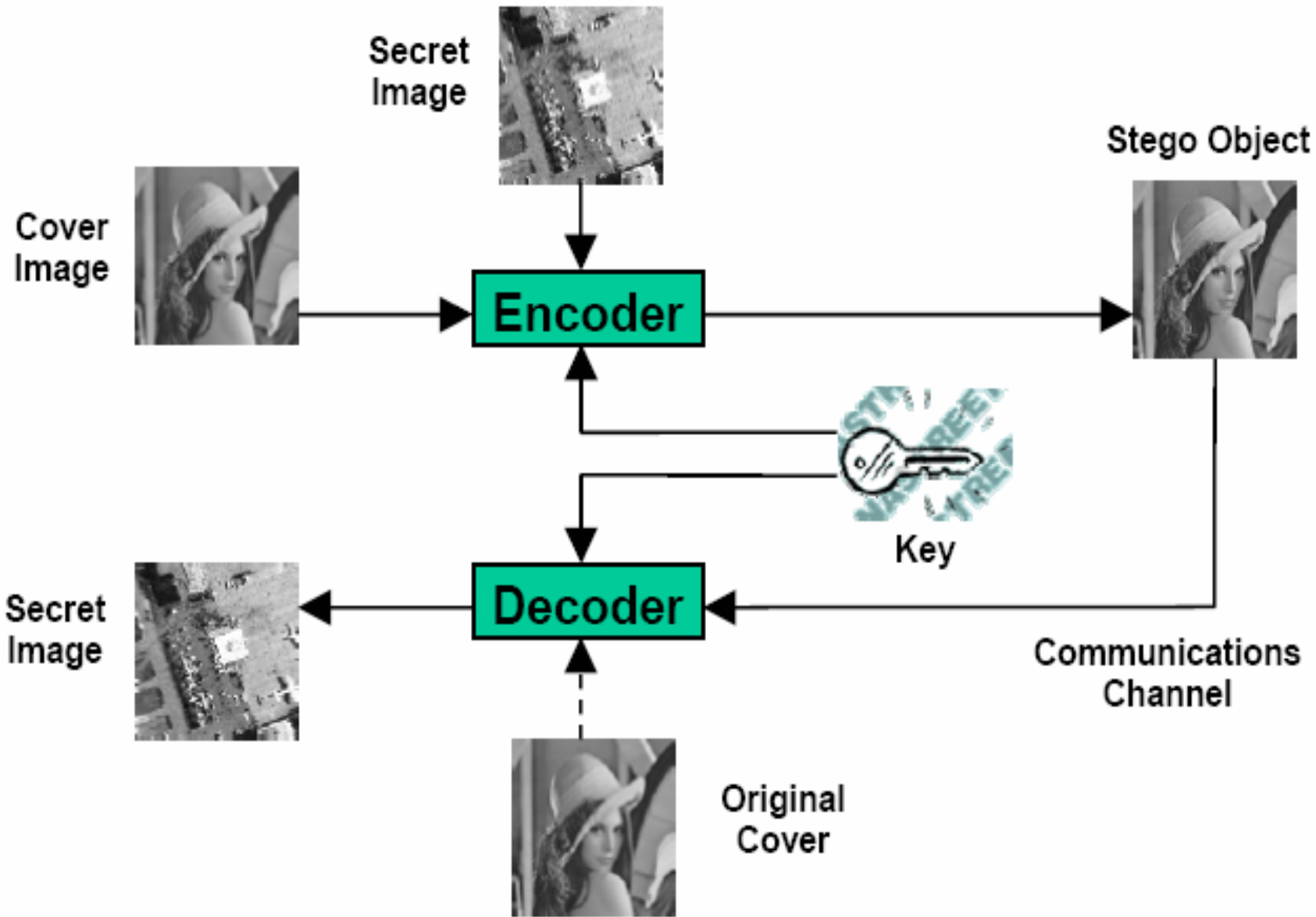
- Plaintext (and length of plaintext) is not recoverable from the ciphertext.
- Examples: HMAC, MD2, MD4, MD5, RIPEMD-160, SHA
- Also called message digests or one-way encryption
- Primary use: Message integrity

Hash Collisions

- There are only 2^K possible hash values (where K = hash length) while there are an infinite number of files
 - Since $\infty \gg 2^K$, there will be duplicate hashes
- The problem: Can hash collisions be forced?
If so, what is the impact on computer forensics
- Solutions to collisions:
 - Use longer hashes (i.e., larger K)
 - Use multiple hashes (e.g., MD5 and SHA-1)

1 key: Secret Key Cryptography





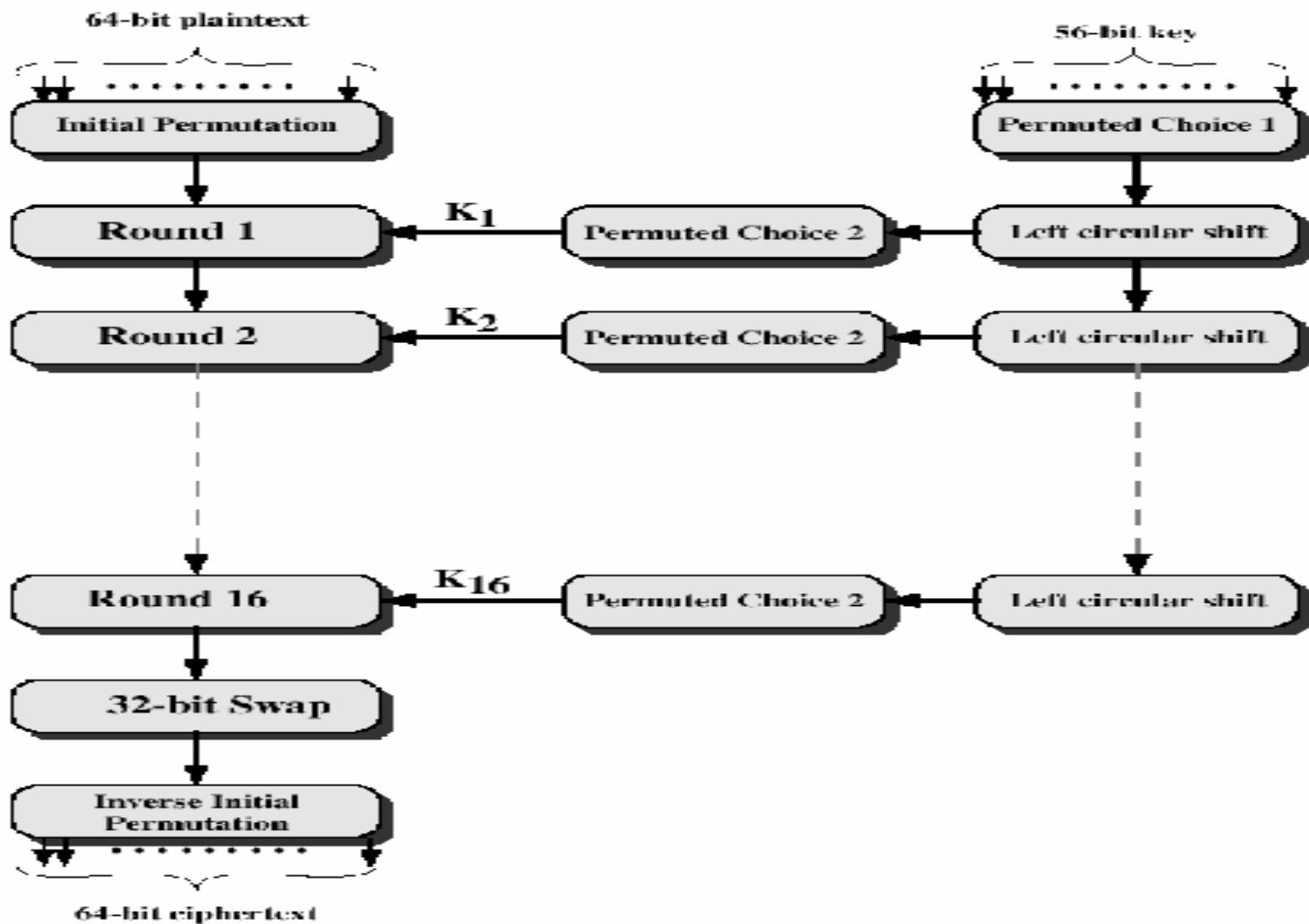
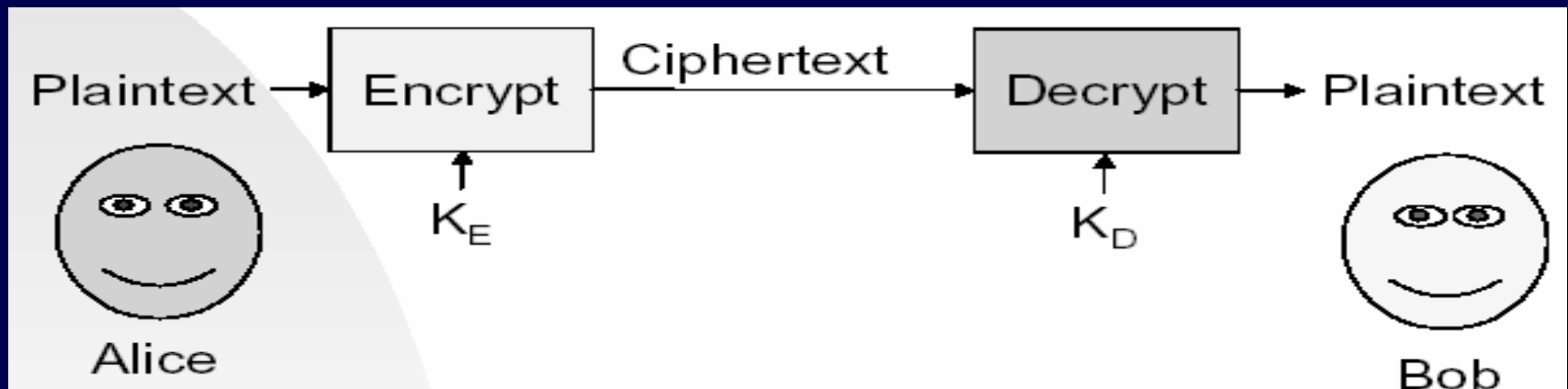


Figure 2.3 General Depiction of DES Encryption Algorithm

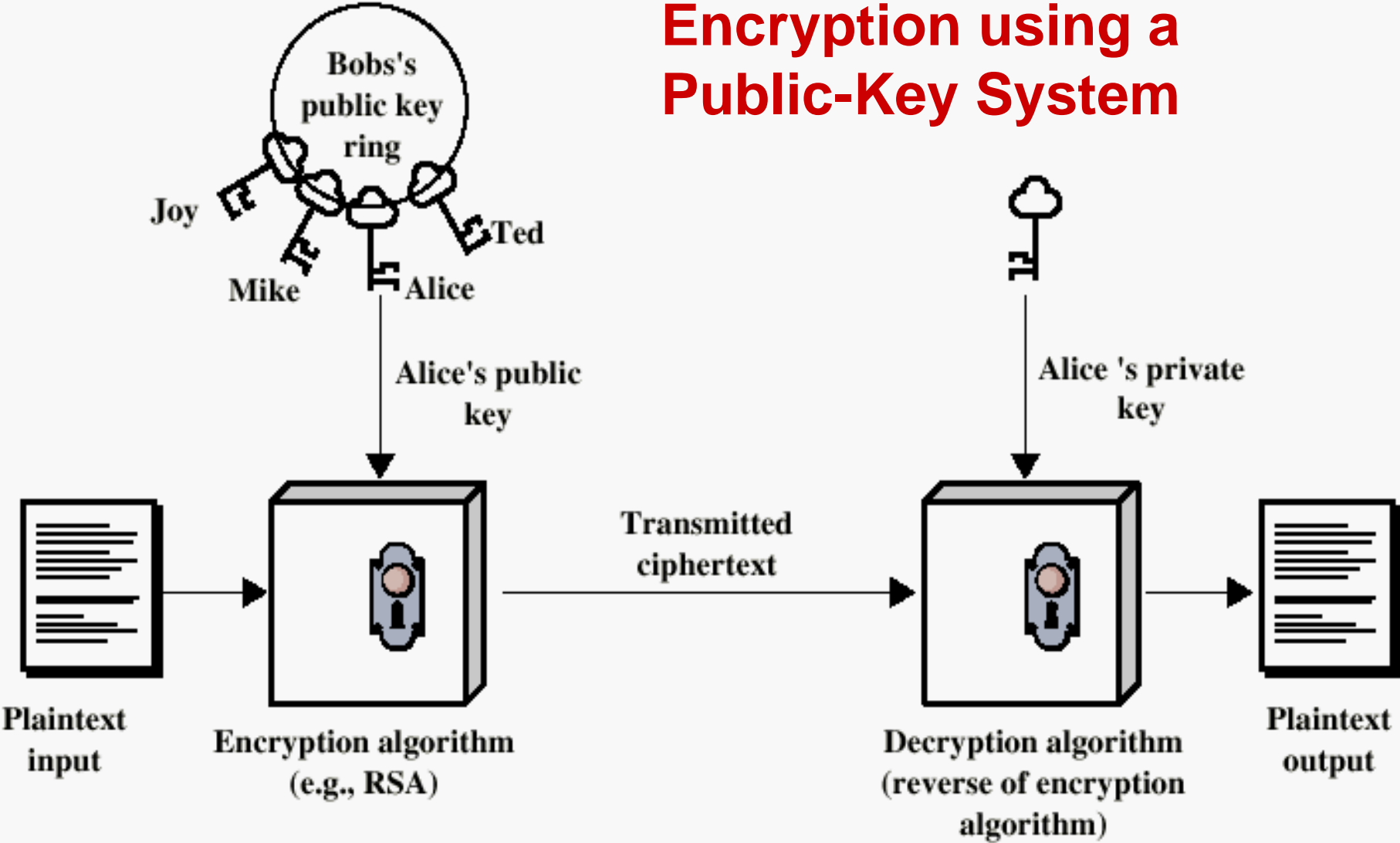
Attacker	Budget	Tool	Time for 40-bit key	Time for a 56-bit key	Key length for protection
Individual hacker	Tiny \$400	PC	1 week	Never	45
		FPGA	5 hours	38 years	50
Small Business	\$10K	FPGA	12 min.	18 mon.	55
Corporate dept.	\$300K	FPGA	24 sec.	19 days	60
		ASIC	0.18 sec.	3 hours	
Big Comp	\$10M	FPGA	7 sec	13 hours	70
		ASIC	5 ms	6 min.	
Government	\$300M	ASIC	0.2 ms	12 sec	75

Symmetric vs asymmetric encryption

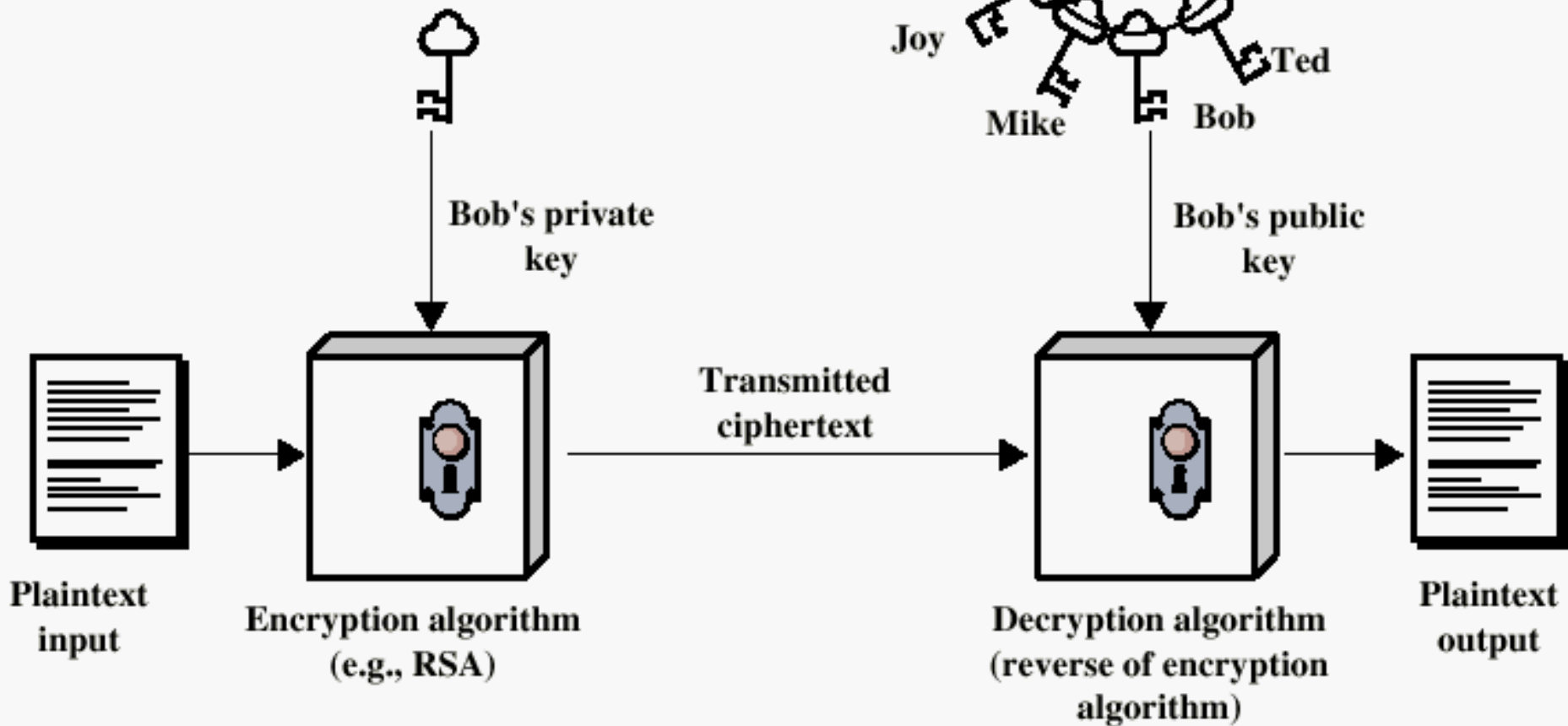


- $C = E(K_E, P) = E_{K_E} (P)$
- $P = D(K_D, C) = D_{K_D} (C)$
- If $K_E \neq K_D$ it is *asymmetric* encryption
- If $K_E = K_D$ it is *symmetric* encryption

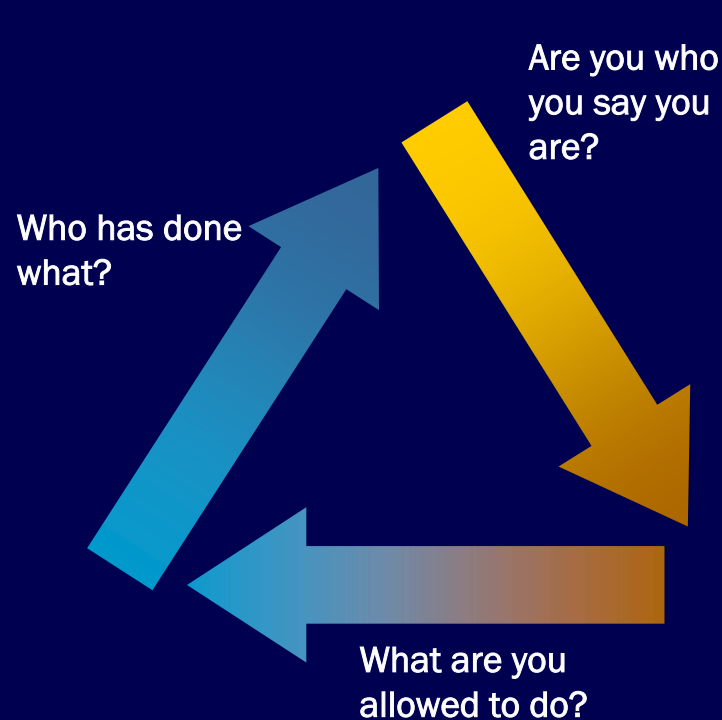
Encryption using a Public-Key System



Authentication using a Public-Key System



Gold Standard



1. **Authentication** – *The process of identifying an individual, usually based on the combination of a username and some kind of credential.*
2. **Authorization** – *The process of granting or denying access to a resource.*
3. **Auditing** – **A record showing who has accessed a network and what operations were performed.**

Establishing Identity

- One or more of the following
 - What entity knows (*eg.* password)
 - What entity has (*eg.* badge, smart card)
 - What entity is (*eg.* fingerprints, retinal characteristics)
 - Where entity is (*eg.* In front of a particular terminal)

Why Info Sec is Difficult?

1. The defender must defend all points; the attacker can choose the weakest point.
2. The defender can defend only against known attacks; the attacker can probe for unknown vulnerabilities.
3. The defender must be constantly vigilant; the attacker can strike at will.
4. The defender must play by the rule; the attacker can play dirty.

– Michael Howard & David LeBlanc, "Writing Secure Code",
MSPress, 2003

12 Security certifications

- Certified Information Systems Security Professional (CISSP)[™]
- Certified Information Systems Auditor (CISA)[™]
- Certified Protection Professional (CPP)
- Computing Technology Industry Association (CompTIA)
- DoD CIO Certificate Program (with Security and Assurance Competencies)
- Global Information Assurance Certification (GIAC) Information Security KickStart
- Global Information Assurance Certification (GIAC) LevelOne Security Essentials
- Global Information Assurance Certification (GIAC) LevelTwo subject area modules
- Global Information Assurance Certification (GIAC) Security Engineer
- System Security Certified Practitioner (SSCP)[™]
- Security Certified Network Professional (SCNP)
- Security+, CompTIA (Computing Technology Industry Association)

CISSP

- CISSP -- Certified Information Systems Security Professional
- Register for the exam at www.isc2.org.
- At least 3 years of experience in information security
- Exam fee: \$450
- Experience counted:
 - Security investigator, security practitioner, information security related work, security auditor, security consultant, security vendor, security instructor
- Recertification every 3 years

Q & A

Thank You !