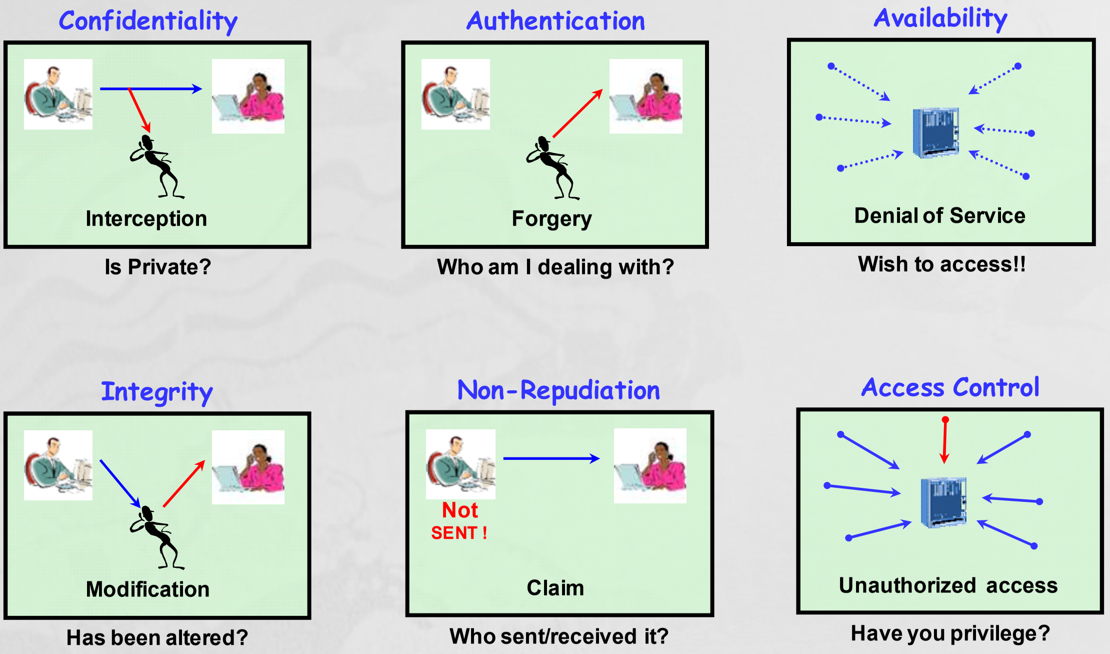
Basic Security Requirements



Basic Security Requirements

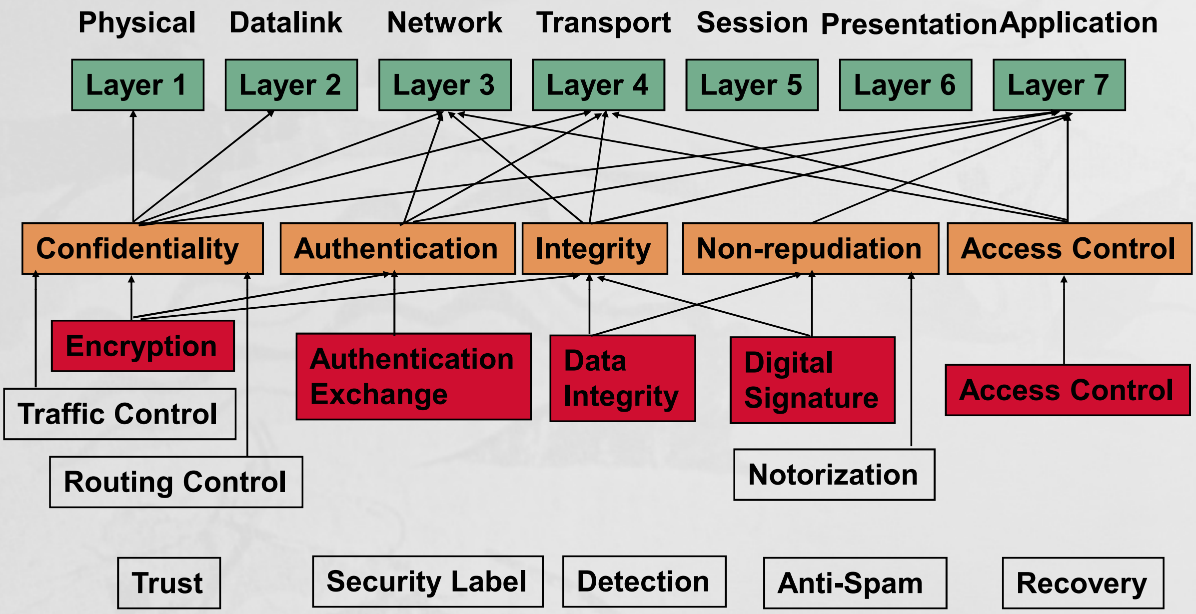
- *Confidentiality* : keeping information secret from all but those who are authorized to it.
- *Data integrity* : ensuring information has not been altered by unauthorized or unknown means
- *Authentication*
  - ✓ *Entity authentication (or identification)* : corroboration of the identity of an entity (e.g., a person, a computer terminal, etc)
  - ✓ *Message authentication: corroboration the source of information ; also known as data origin authentication*
- *Access control*: restricting access to resources to privileged entities.
- *Non-repudiation:* preventing the denial of previous commitment or actions.

Advanced Security Requirements

- Authorization: conveyance, to another entity, of official sanction to do or be something.
- Validation: a means to provide timeliness of authorization to use or manipulate information or services
- Certification: endorsement of information by a trusted entity
- Revocation: retraction of certification or authorization
- Time stamping: recording the time of creation or existence of information
- Witnessing : verifying the creation or existence of information by an entity other than the creator
- Receipt: acknowledgement that information has been received
- Ownership: a means to provide an entity with the legal right to use or transfer a resource to others
- Anonymity: concealing the identity of an entity involved in some process

---

What is Network Security ?



Physical Datalink Network Transport Session Presentation Application

Layer 1 Layer 2 Layer 3 Layer 4 Layer 5 Layer 6 Layer 7

Confidentiality Authentication Integrity Non-repudiation Access Control

Encryption

Traffic Control

Routing Control

Authentication Exchange

Data Integrity

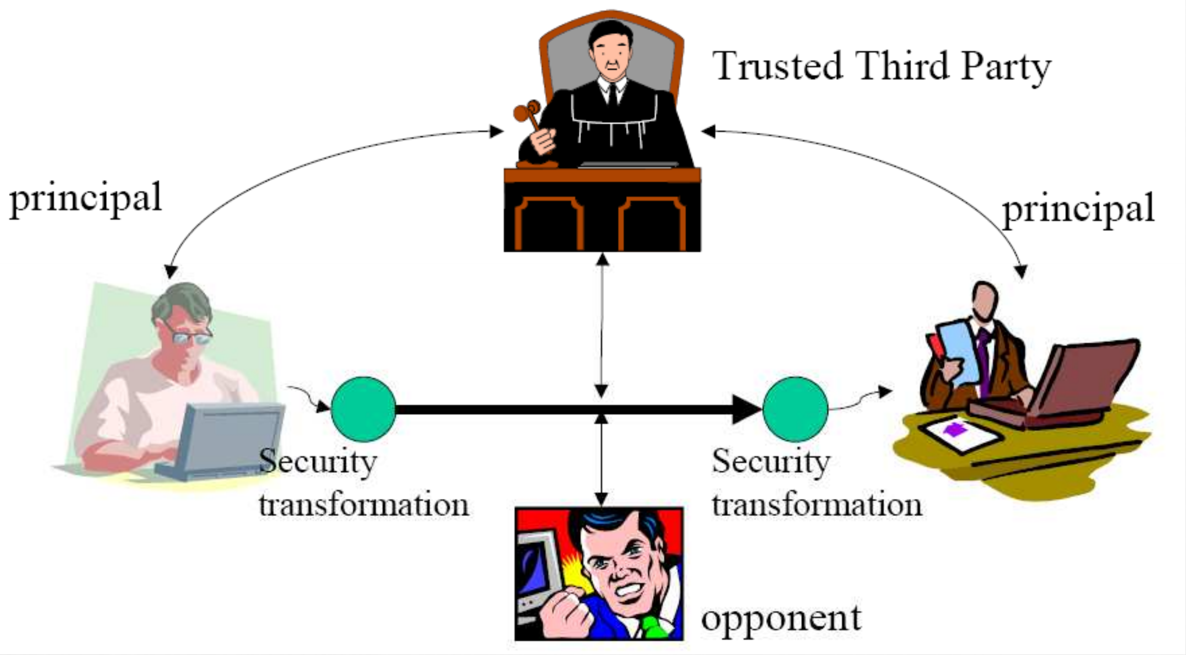
Digital Signature

Notorization

Access Control

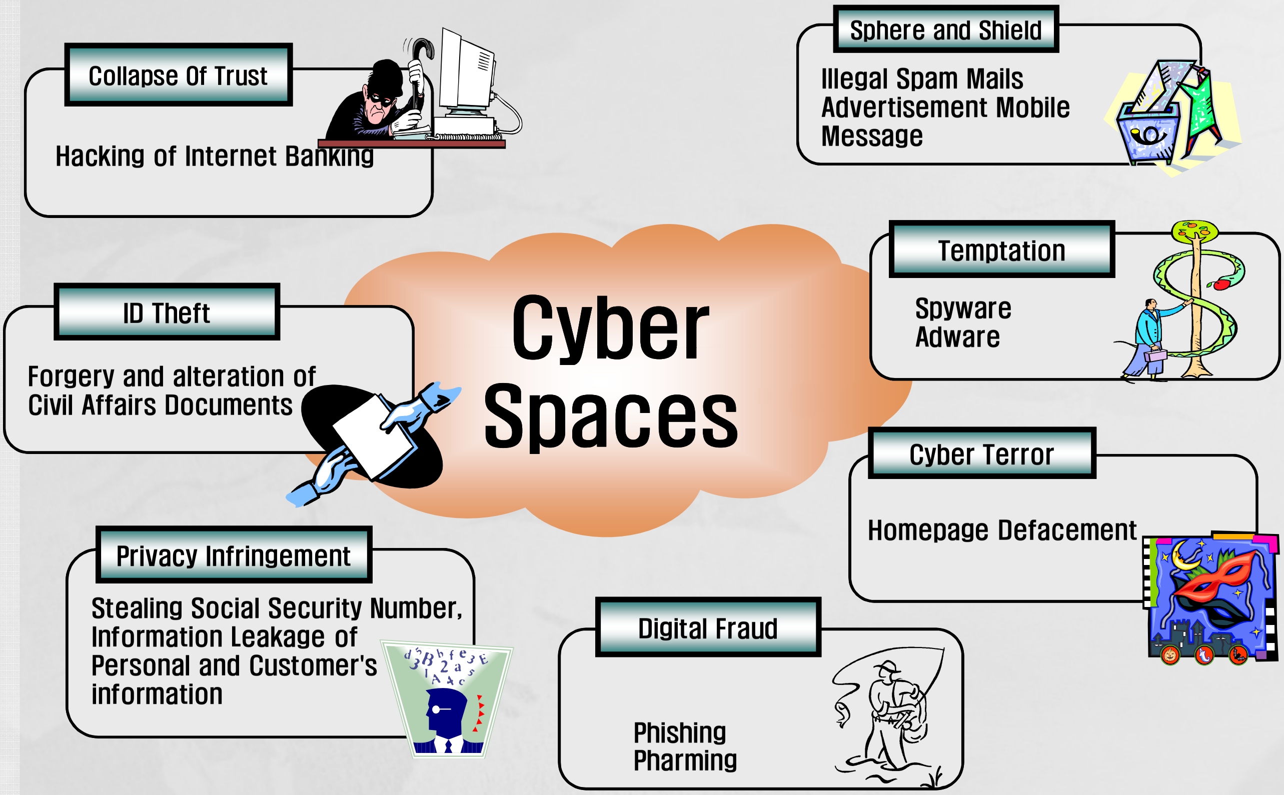
Trust Security Label Detection Anti-Spam Recovery

Network Security Model



---

7 Sins in CyberSpace



Collapse Of Trust

Hacking of Internet Banking

Sphere and Shield

Illegal Spam Mails Advertisement Mobile Message

Cyber Spaces

ID Theft

Forgery and alteration of Civil Affairs Documents

Temptation

Spyware
Adware

Cyber Terror

Homepage Defacement

Privacy Infringement

Stealing Social Security Number, Information Leakage of Personal and Customer's information

Digital Fraud

Phishing
Pharming

Risk analysis in Cyberspace

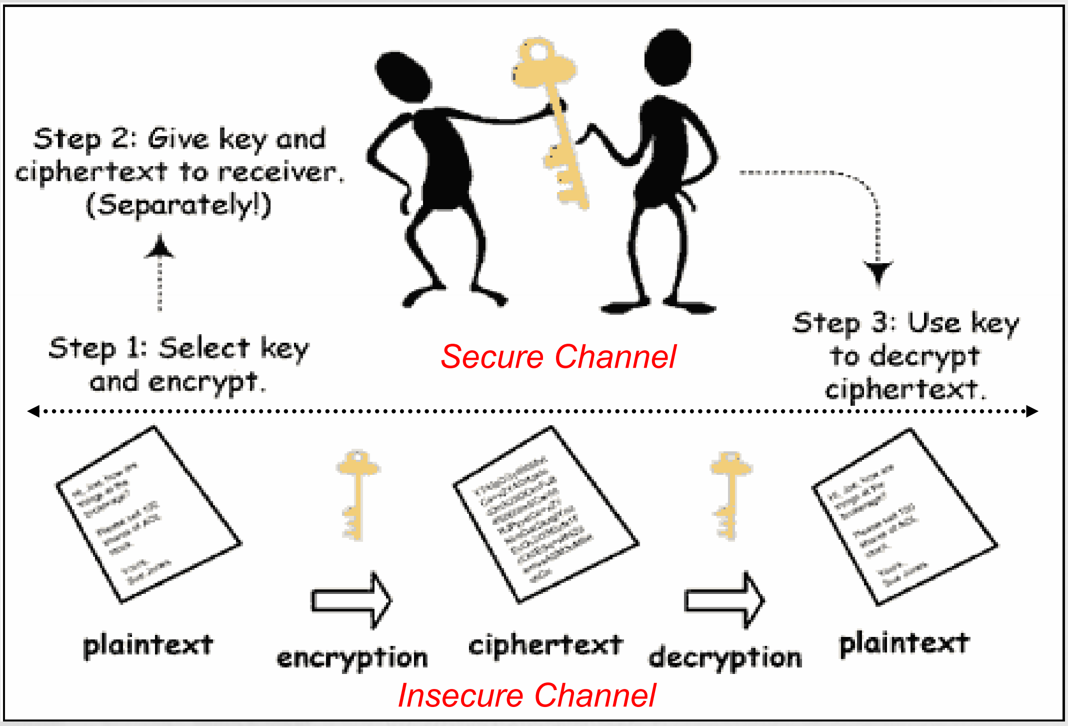
Risks	Type of Intrusion	Problem	Countermeasures
Theft or Stolen	**Confidentiality** **Authentication**	**Device holders have authentication information**	**Entity (or device) authentication/Cryptography**
Illegal Access Point	**Authentication**	**1-way authentication**	**Mutual authentication**
IP Spoofing	**Confidentiality**	**Radiation of RF signal to unwanted user**	**Cryptography**
(D)DoS	**Availability**	**Degraded availability**	**Availability**
Trojan Horse, Worm, Virus	**Availability, Confidentiality, Integrity**	**Degraded availability & integrity**	**Anti-Virus program**
Attack by harmful signal	**Availability**	**Interfered communication channel**	**Spread Spectrum-Frequency Hopping**
Resource consumption attack	**Availability**	**Out of battery power**	**Availability**
Revealing Location or ID- information	**Confidentiality**	**Privacy**	**Anonymity**

Example of Security Engineering in a Network

Security requirement		Special Requirement in U-network
Basic	Authentication	Mutual authentication, use of dynamic key, Wireless PKI, device authentication, Central authentication, QoS
	Confidentiality	Key management, light weight cryptography, secure DB, mobile cryptography
	Integrity	Integrity mechanism for U-network
Additional	Availability	DoS attack, Priority management in access control, Differentiated service
	Control of delegate	Entity authentication and authorization Access control
	Anonymity	Transfer of real ID information
	Safe roaming	Global roaming, DRM, Seamless secure roaming

Introduction to Cryptography

Model of Symmetric Cryptosystem



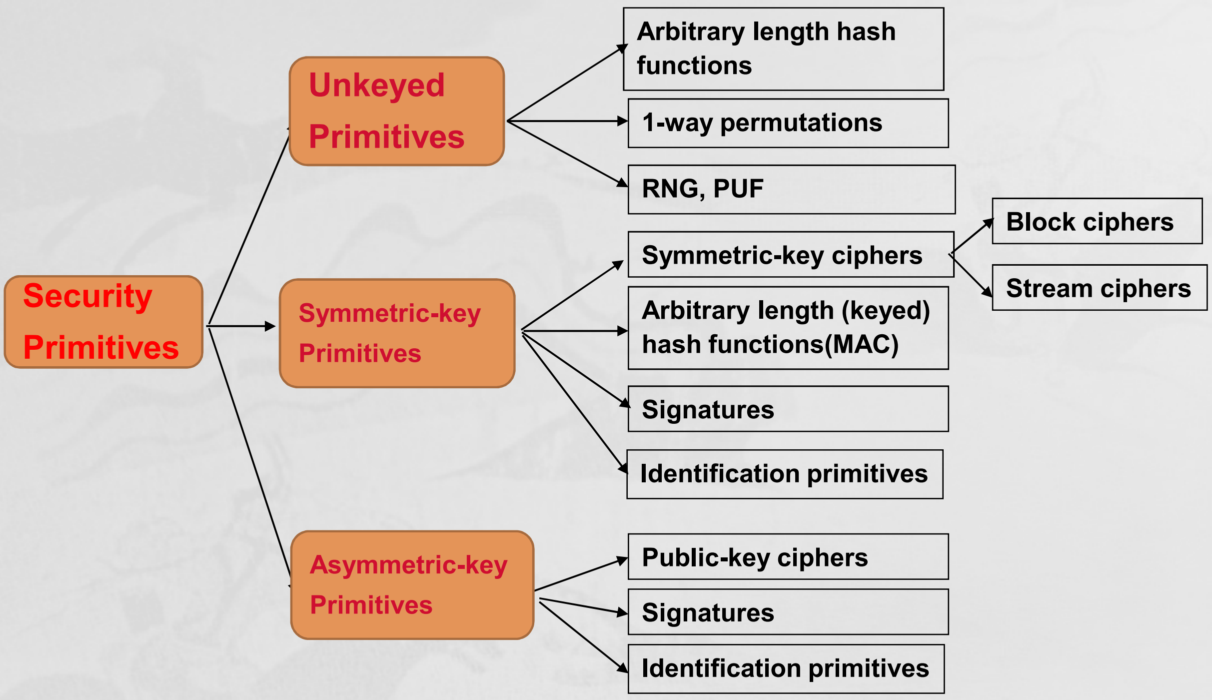
Terminology (I)

- Channel
  - Secure : trust, registered mail, tamper-proof device
  - Insecure : open, public channel
- Entity
  - Sender (Alice)
  - Receiver (Bob)
  - Adversary (Charlie)
    - ✓Passive attack : wiretapping ->Privacy
    - ✓Active attack : modification,impersonation
      -> Authentication

Terminology (II)

- Classification of crypto algorithms
  - by date
    - ✓Traditional(~19C): Caesar
    - ✓Mechanical(WW I, II): Rotor Machine, Purple
    - ✓Modern(‘50~): DES, IDEA, AES and RSA, ECC
  - by number of keys
    - ✓Conventional: {1,single,common} key, symmetric
    - ✓Public key cryptosystem: {2,dual} keys, asymmetric
  - by size of plaintext
    - ✓Block Cipher
    - ✓Stream Cipher

A Taxonomy of Cryptographic Primitives



Security Primitives

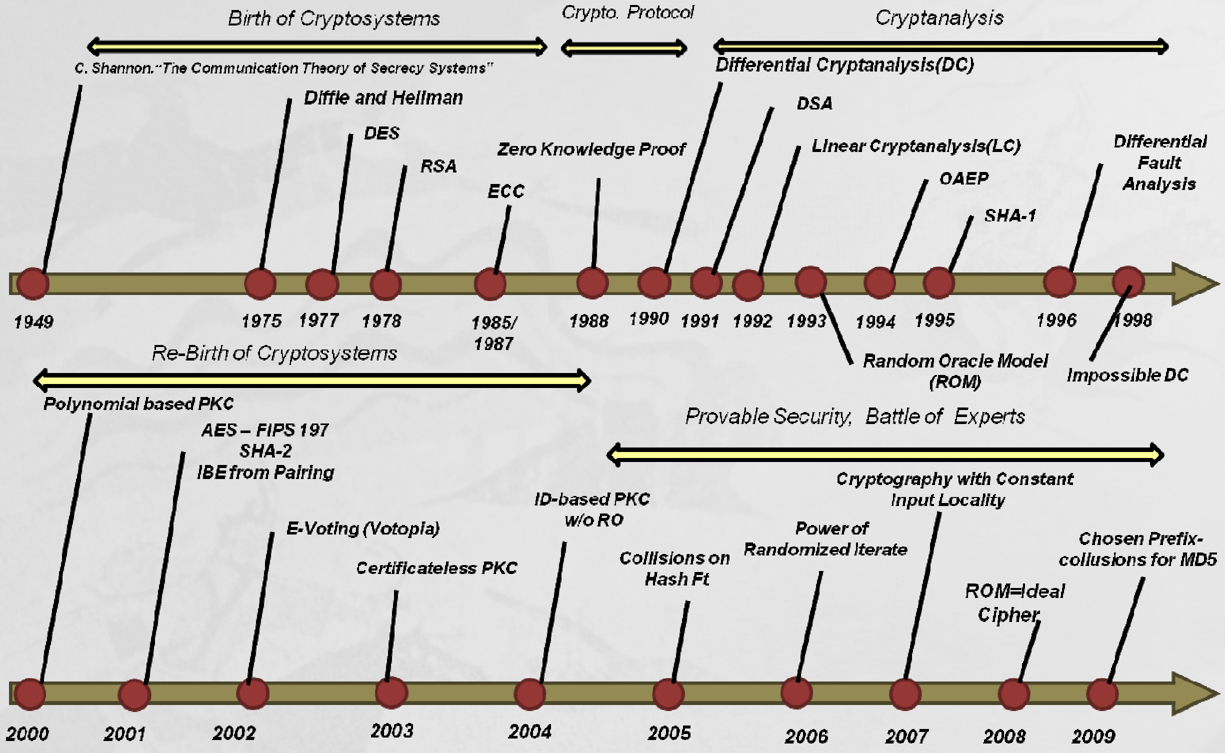
- **Unkeyed Primitives**
  - **Arbitrary length hash functions**
  - **1-way permutations**
  - **RNG, PUF**
- **Symmetric-key Primitives**
  - **Symmetric-key ciphers**
    - **Block ciphers**
    - **Stream ciphers**
  - **Arbitrary length (keyed) hash functions(MAC)**
  - **Signatures**
  - **Identification primitives**
- **Asymmetric-key Primitives**
  - **Public-key ciphers**
  - **Signatures**
  - **Identification primitives**

RNG(Random Number Generator), PUF(Physically Unclonable Function)

Classification of Security

- Unconditionally secure : unlimited power of adversary, perfect (*ex.* : one-time pad)
- Provably secure : under the assumption of well-known hard mathematical problem
- Computationally secure : amount of computational effort by the best known methods (*Practical Secure*)

History of Modern Cryptography



Birth of Cryptosystems

Crypto. Protocol

Cryptanalysis

C. Shannon."The Communication Theory of Secrecy Systems"

Diffie and Hellman

DES

RSA

ECC

Zero Knowledge Proof

Differential Cryptanalysis(DC)

DSA

Linear Cryptanalysis(LC)

OAEP

SHA-1

Differential Fault Analysis

1949 1975 1977 1978 1985/1987 1988 1990 1991 1992 1993 1994 1995 1996 1998

Random Oracle Model (ROM)

Impossible DC

Re-Birth of Cryptosystems

Polynomial based PKC

AES – FIPS 197
SHA-2
IBE from Pairing

E-Voting (Votopia)

Certificateless PKC

ID-based PKC w/o RO

Provable Security, Battle of Experts

Collisions on Hash Ft

Power of Randomized Iterate

Cryptography with Constant Input Locality

ROM=Ideal Cipher

Chosen Prefix-collusions for MD5

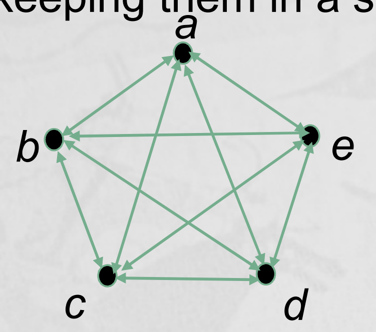
2000 2001 2002 2003 2004 2005 2006 2007 2008 2009

"Toward basing fully homomorphic encryption on worst-case hardness", Crypto2010 Best paper

---

Key Distribution Problem

- In symmetric key cryptosystems
  - Over complete graph with *n* nodes, $_{n}C_{2} = n(n-1)/2$ pairs secret keys are required.
  - (Example) n=100, 99 x 50 = 4,950 keys are required
  - Problem: Managing large number of keys and keeping them in a secure manner is difficult

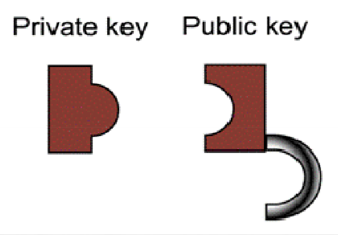


Secret keys are required between

(a,b), (a,c), (a,d), (a,e), (b,c), (b,d), (b,e), (c,d), (c,e), (d,e)

PKC – concept (1/3)

Using a pair of keys which have special mathematical relation.
Each user needs to keep securely only his private key.
All public keys of users are published.

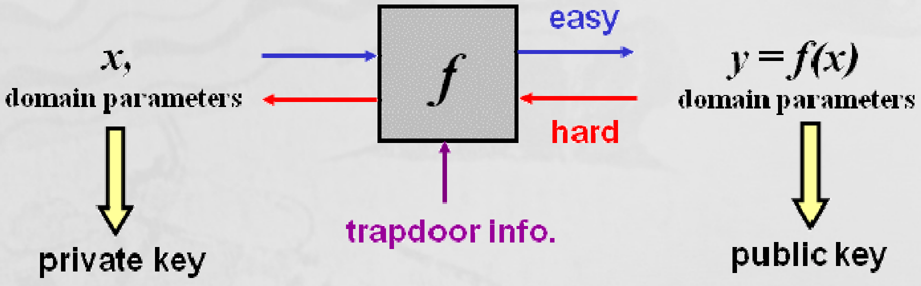


In Encryption
- Anyone can lock (using the public key)
- Only the receiver can unlock (using the private key)

In Digital Signature
- Only the signer can sign (using the private key)
- Anyone can verify (using the public key)

PKC – concept (2/3)

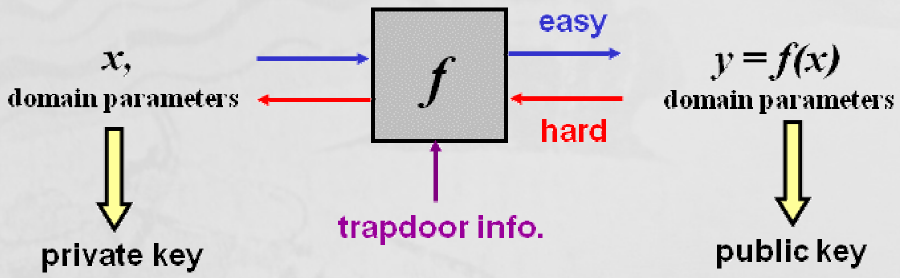
- ❖ Trapdoor one-way functions
  - ❖ Given *x*, easy to compute *f(x)*
  - ❖ Given *y*, difficult to compute $f^{-1}(y)$ in general
  - ❖ Easy to compute $f^{-1}(y)$ for given *y* to only who knows certain information (which we call trapdoor information)



But, easy if trapdoor info. is given.

PKC – concept (3/3)

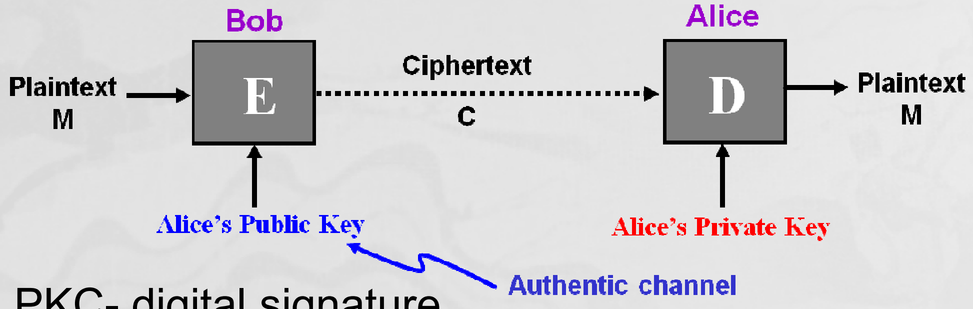
- Concept
  - invented by Diffie and Hellman in 1976, “*New directions in Cryptography*”, IEEE Tr. on IT. ,Vol. 22, pp. 644-654, Nov., 1976.
  - Overcome the problem of secret key sharing in symmetric cryptosystems
  - Two keys used: public key & private key
  - Also known as two-key or asymmetric cryptography
  - Based on (trapdoor) one-way function



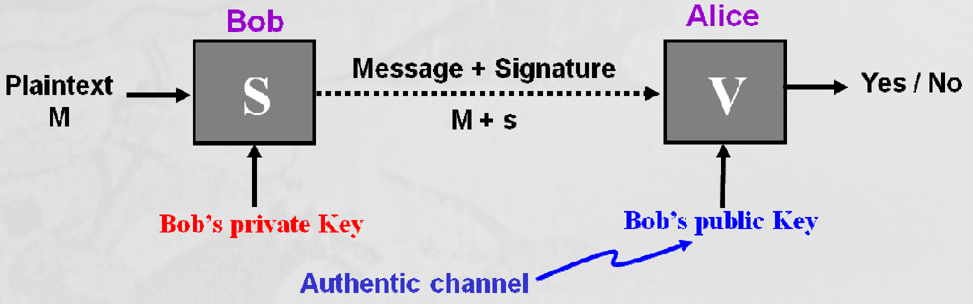
But, easy if trapdoor info. is given.

PKC- operations

- ❑ PKC-encryption/decryption



- ❑ PKC- digital signature



Examples of PKC

- RSA scheme (1978)
  - *R.L.Rivest, A.Shamir, L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems",CACM, Vol.21, No.2, pp.120-126,Feb,1978*
- McEliece scheme (1978)
- Rabin scheme (1979)
- Knapsack scheme (1979-): Merkle-Hellman, Chor-Rivest, *etc.*
- ElGamal scheme (1985)
- Elliptic Curve Cryptosystem (1985): Koblitz, Miller
- Non-Abelian group Cryptography (2000): Braid group

Pros and Cons

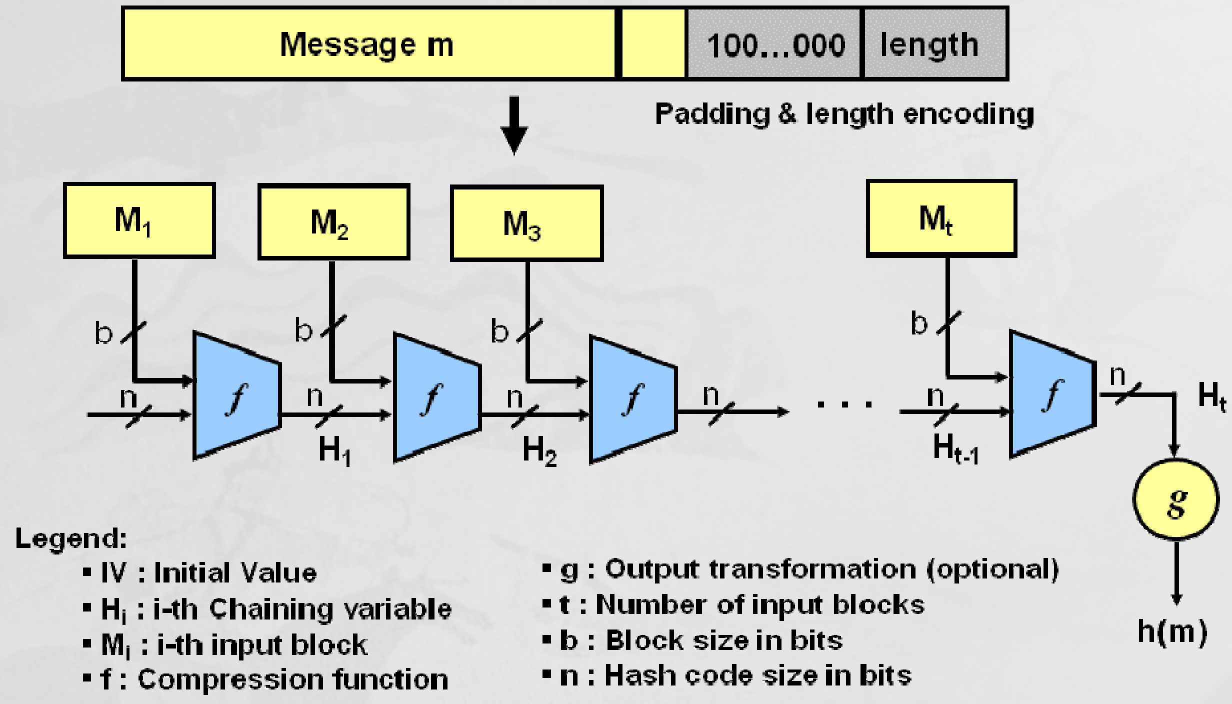
	Symmetric	Asymmetric
Key relation	Enc. key = Dec. key	Enc. Key ≠ Dec. key
Enc. Key	Secret	Public, {Private}
Dec. key	Secret	Private, {Public}
Algorithm	Classified Open	Open
Example	SKIPJACK AES	RSA
Key Distribution	Required (X)	Not required (○)
Number of key	Many (X)	Small (○)
Performance	Fast(○)	Slow(X)

Hash Function

- Definition
  - Compression: arbitrary length input to fixed length output
  - Ease of computation

- Security Properties
  - Preimage resistance (One-wayness) :
    - Given y, it is computationally infeasible to find any input x such that $y = h(x)$
  - 2nd preimage resistance (Weak collision resistance) :
    - Given x, it is computationally infeasible to find another input $x' \neq x$ such that $h(x) = h(x')$
  - Collision resistance (Strong collision resistance) :
    - It is computationally infeasible to find any two distinct inputs x and x' such that $h(x) = h(x')$

Construction of Secure Hash Function



Legend:
- IV : Initial Value
- H_i : i-th Chaining variable
- M_i : i-th input block
- f : Compression function
- g : Output transformation (optional)
- t : Number of input blocks
- b : Block size in bits
- n : Hash code size in bits

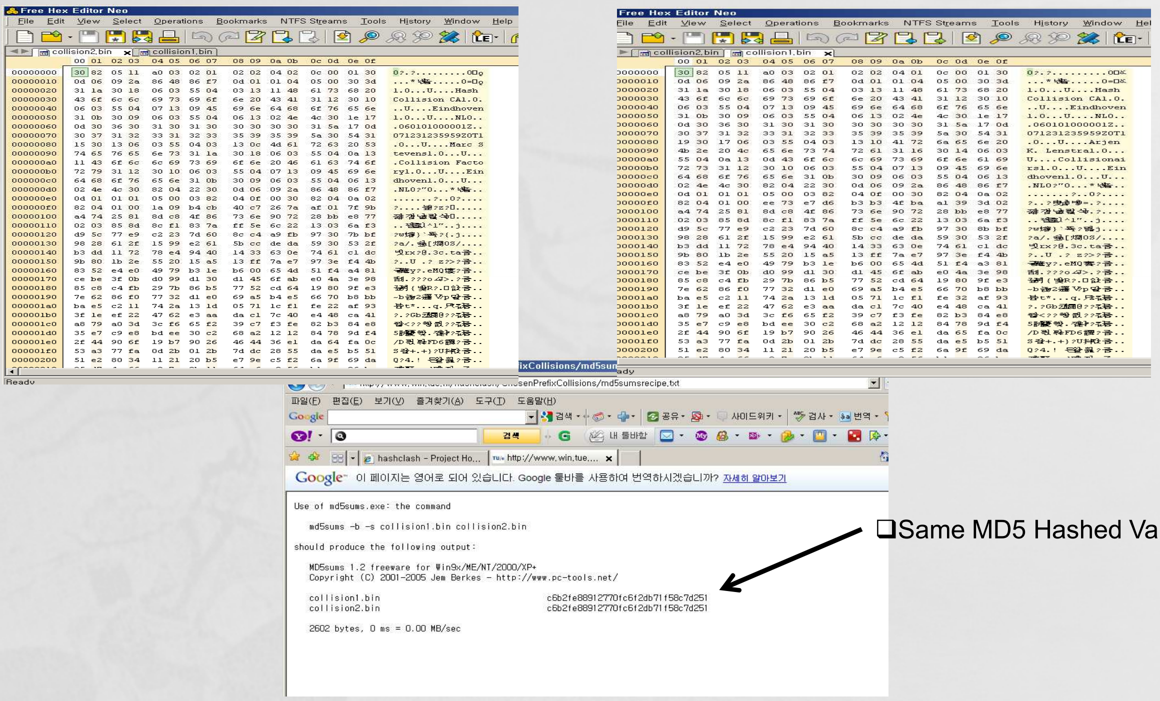
Secure Hash Algorithm

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Operation	Collisions found
SHA-0		160	160	512	$2^{64}-1$	32	80	+,and,or, xor,rot	Yes
SHA-1		160	160	512	$2^{64}-1$	32	80	+,and,or, xor,rot	Yes (2^{52} attack (*))
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64}-1$	32	64	+,and,or, xor,shr,rot	None
	SHA-512/384	512/384	512	1024	$2^{128}-1$	64	80	+,and,or, xor,shr,rot	None

* Cameron McDonald, Philip Hawkes and Josef Pieprzyk, SHA-1 collisions now 2^52, Eurocrypt 2009 Rump session, http://eurocrypt2009rump.cr.yp.to/ 837a0a8086fa6ca714249409ddfae43d.pdf.

Collision in MD5

- Collision1.bin
- Collision2.bin



```
Use of md5sums.exe: the command

   md5sums -b -s collision1.bin collision2.bin

should produce the following output:

   MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
   Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/

   collision1.bin                         c6b2fe88912770fc6f2db71f58c7d251
   collision2.bin                         c6b2fe88912770fc6f2db71f58c7d251

   2602 bytes, 0 ms = 0.00 MB/sec
```

- Same MD5 Hashed Value !!

SHA-3 Project

CRYPTOGRAPHIC HASH PROJECT

Background Information

A hash function takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash function is a hash function that is designed to achieve certain security properties. The Federal Information Processing Standard 180-2, Secure Hash Standard, specifies algorithms for computing five cryptographic hash functions — SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. FIPS 180-2 was issued in August, 2002, superseding FIPS 180-1.

In recent years, several of the non-NIST approved cryptographic hash functions have been successfully attacked, and serious attacks have been published against SHA-1. In response, NIST held two public workshops (see menu at left) to assess the status of its approved hash functions and to solicit public input on its cryptographic hash function policy and standard. As a result of these workshops, NIST has decided to develop one or more additional hash functions through a public competition, similar to the development process of the Advanced Encryption Standard (AES). NIST has proposed a tentative timeline for the competition, and also published a policy on the use of the current hash functions.

NIST issued draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash algorithms in January, 2007 [Federal Register Notice (January 23, 2007)] for public comments; the comment period ended on April 27, 2007. Based on the public feedback, NIST has revised the requirements and evaluation criteria and issued a Call for a New Cryptographic Hash Algorithm (SHA-3) Family on November 2, 2007 [Federal Register Notice (November 2, 2007)] to launch the hash algorithm competition. Details of the competition are available at www.nist.gov/hash-competition .

Key Length by NIST

Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptique Curve	Hash (A)	Hash (B)
2007 - 2010	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

Recommendation for Key Management, Special Publication 800-57 Part 1, NIST, 03/2007.

http://www.keylength.com