Lecture 1: Information Security and Cryptology
정보보호와 암호

2008. 10. 17

Prof. Byoungcheon Lee
sultan (at) joongbu . ac . kr

Joongbu University

Contents

1. Information security
   - Overview
   - Computer security
   - Network Security
   - OSI security architecture
   - Security industry

2. Cryptology
   - Overview
   - Block cipher
   - Public key encryption
   - Digital signature
   - Hash and MAC

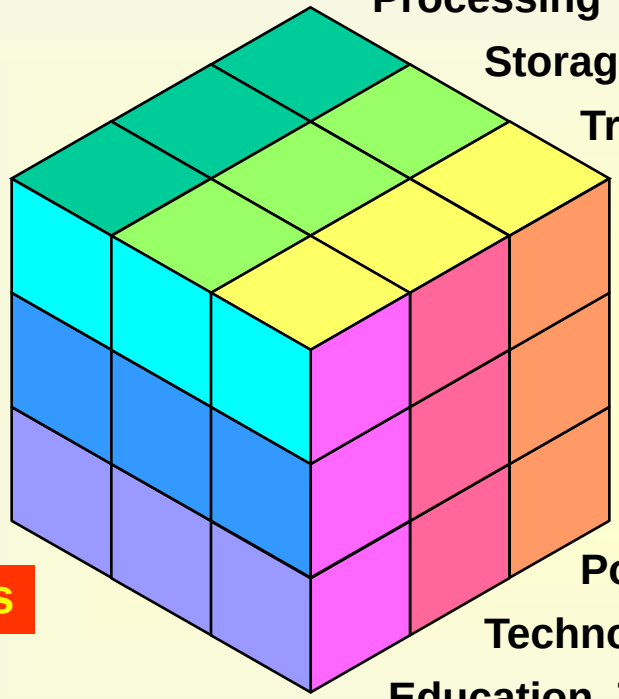
1. Information Security

What is Information Security?

- **Information Security (정보보호, 정보보안)**
  - **Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, modification, or disruption**
  - **Protecting the confidentiality, integrity and availability of information**

  - **Information security is an essential infrastructure technology to achieve successful information-based society**
  - **Highly information-based company without information security will lose competitiveness**

What is Information Security?



Processing

Storage

Transmission

Information States

Confidentiality
(기밀성)

Integrity
(무결성)

Availability
(가용성)

Security Properties

Policy & Procedures

Technology

Education, Training &
Awareness

Security Measures

NSTISSI 4011: National Training Standard for Information Systems Security Professionals, 1994

Information Security and C.I.A.

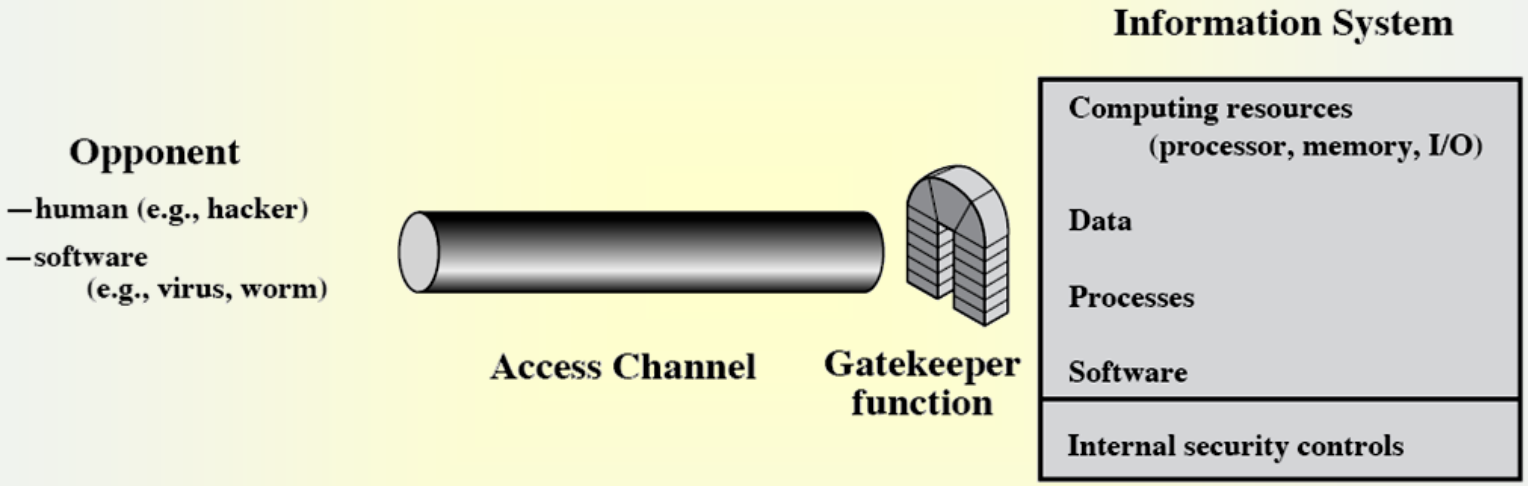
- **Information Security**
  - Discipline that protects the Confidentiality, Integrity & Availability of information, during processing, storage & transmission, through Policies, Technologies & Operations
  - Network/Communication security, Host/Computer security

- **C.I.A. of Information Security**
  - **Confidentiality**: Protecting from unauthorized disclosure
  - **Integrity**: Protecting from unauthorized modification
  - **Availability**: Making information accessible/available when needed

- **How to Achieve Information Security**
  - **Policies** : what should do, what should not do, etc., for information security
  - **Technologies**: implementing the policies
  - **Operations**: assessment & improvement on the implemented technologies

A Model for Computer Security

- Protect a system from unwanted access



Why Computer Security?

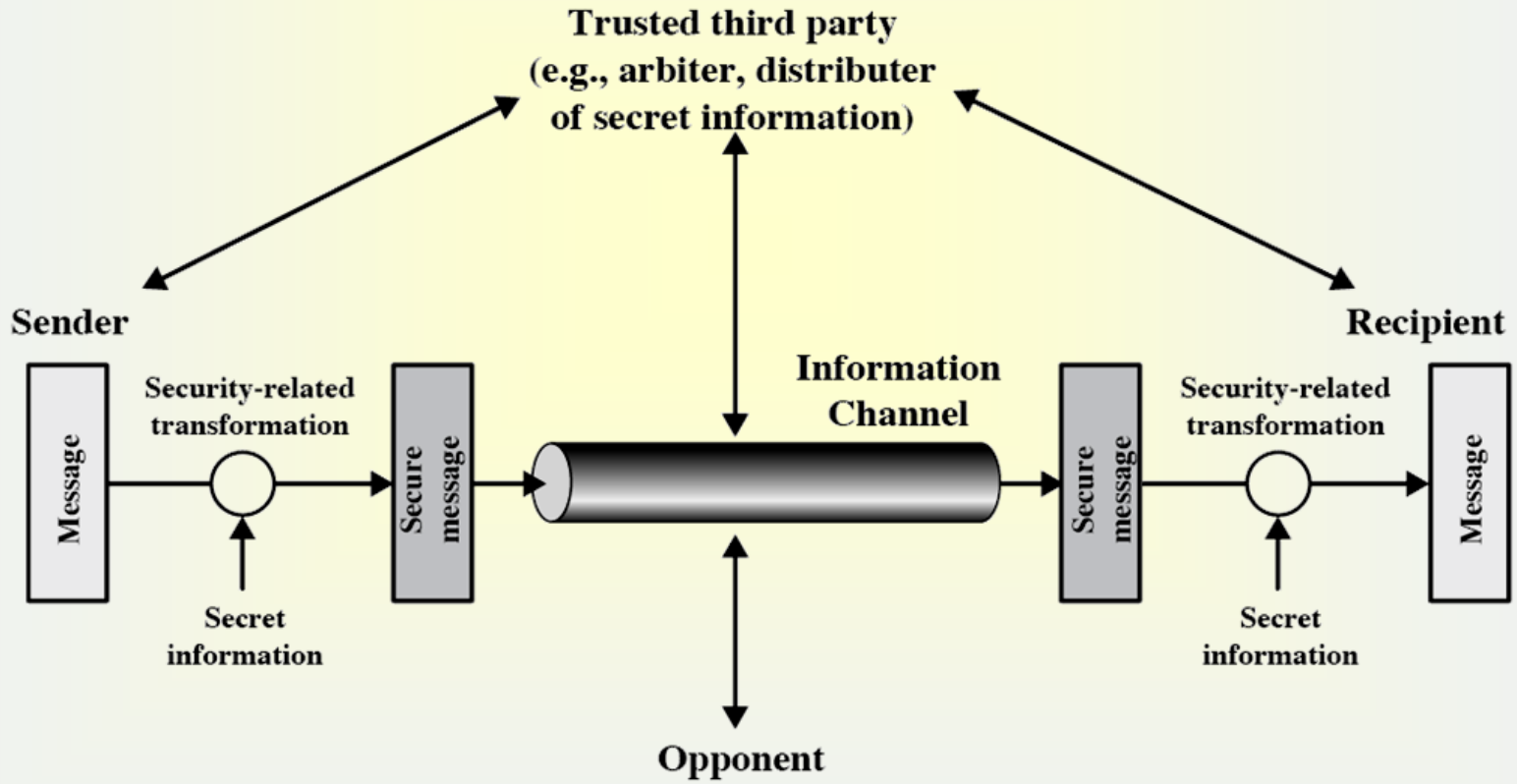
- The Internet is a dangerous place
  - We are constantly being scanned for weak or vulnerable systems
  - New unpatched systems will be exploited within minutes.
- We need to protect
  - Our data
  - Our ability to use our computers (denial of service attacks)
  - Our reputation
- Major sources of danger
  - Running malicious code on your machine due to system or application vulnerabilities or improper user actions

Good Computer Security Practices

1. Don’t keep restricted data on portable devices.
2. Back-up your data.
3. Use cryptic passwords that can’t be easily guessed and protect your passwords - don’t write them down and don’t share them!
4. Make sure your computer has anti-virus, anti-spyware and firewall protection as well as all necessary security patches.
5. Don’t install unknown or unsolicited programs on your computer.
6. Don't open unknown, unscanned or unexpected email attachments.
7. Don't share access to your computers with strangers. Learn about file sharing risks.
8. Disconnect from the Internet when not in use.
9. Physically secure your area and data when unattended
10. Lock your screen
11. Check your security on a regular basis. Understand the risks and use measures to minimize your exposure.
12. Share security tips with family members, co-workers and friends.

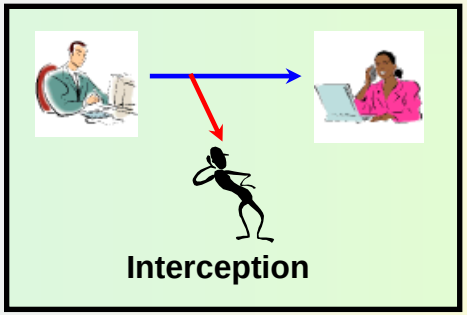
A Model for Network Security

- Protect the communication from opponents.



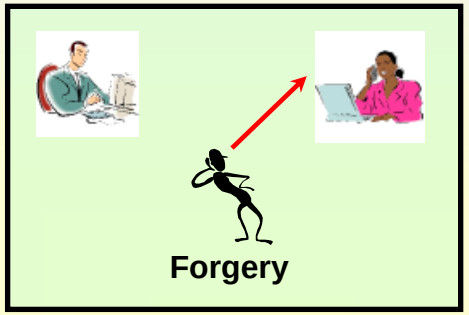
Security Needs for Network Communications

Confidentiality



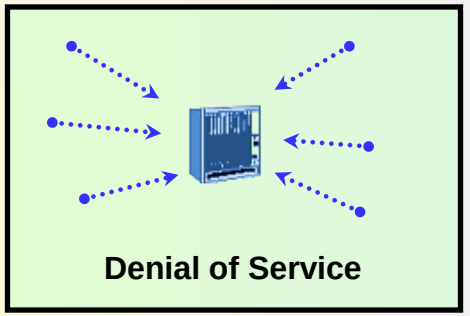
Is Private?

Authentication



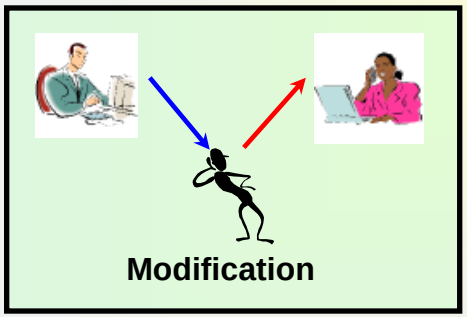
Who am I dealing with?

Availability



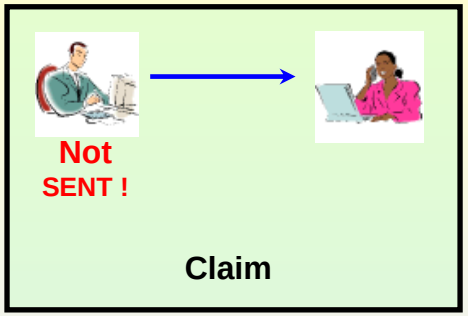
Wish to access!!

Integrity



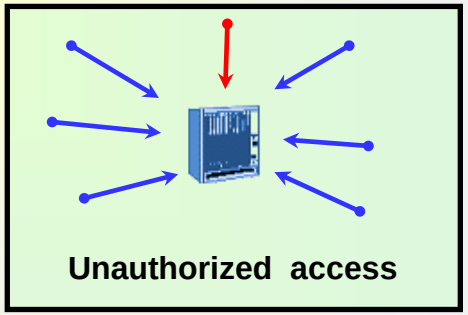
Has been altered?

Non-Repudiation



Who sent/received it?

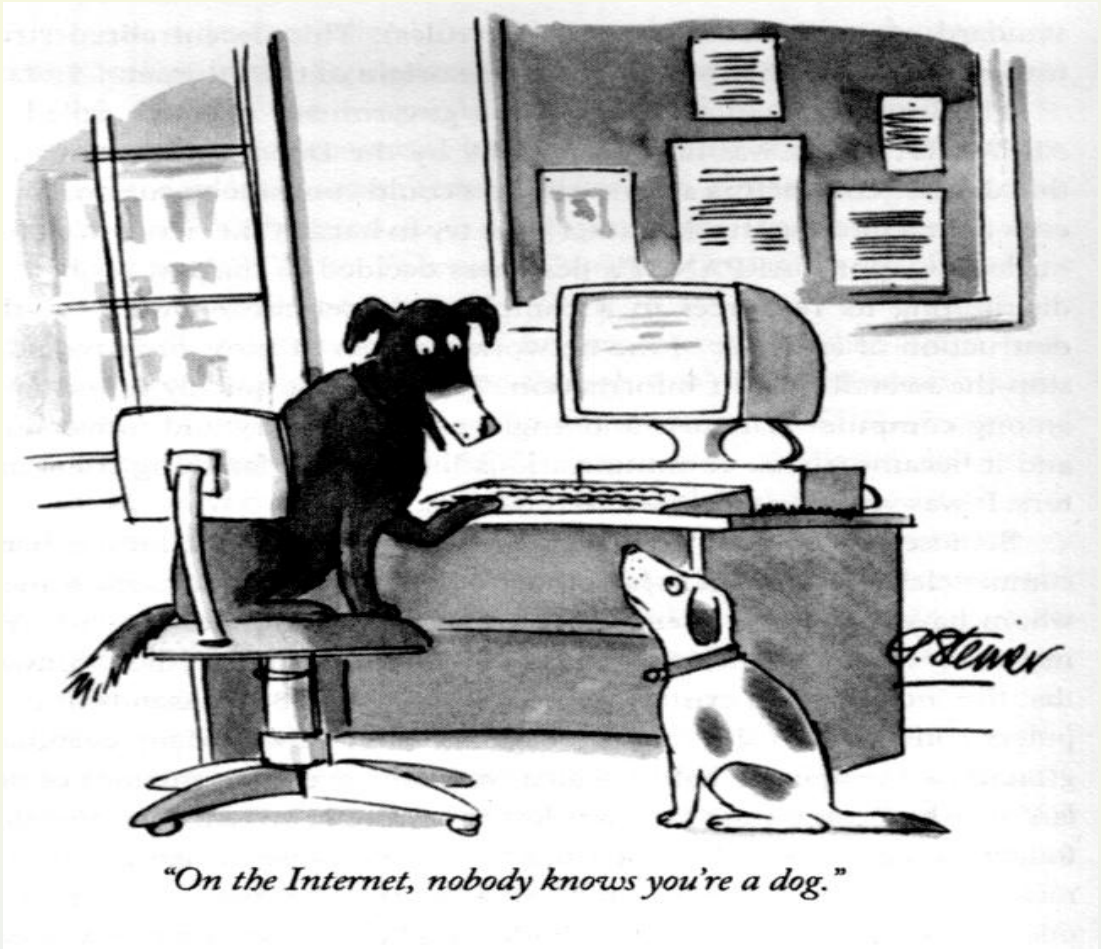
Access Control



Have you privilege?

Authenticity

On the Internet, nobody knows you're a dog



"On the Internet, nobody knows you're a dog."

What is the Internet?

- Collection of networks that communicate
  - with a common set of standard protocols (TCP/IP)
  - by multilateral agreement
- Collection of networks with
  - no central control
  - no central authority
  - no common legal oversight or regulations
  - no standard acceptable use policy
- Physical network connections not important
  - leased lines, dial-up, wireless
- Logical connectivity
  - everything is connected to everything else

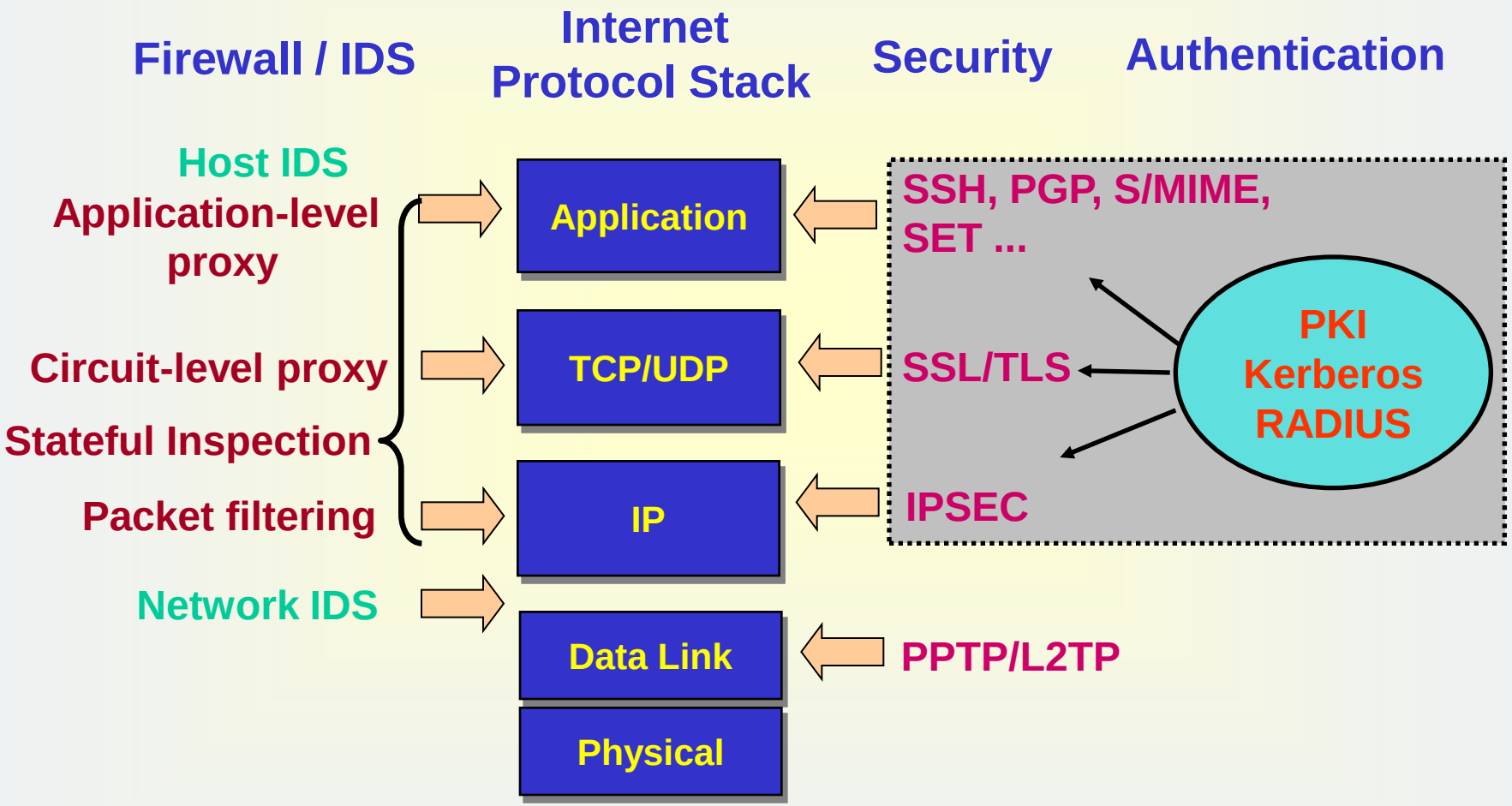
Internet Security Issues

- **Internet Infrastructure is Inherently Insecure**
  - Security was not a design consideration of Internet protocols
  - Unauthenticated routing protocols control Internet reachability
  - Add-on security is hard on users and hard to integrate into applications
- **Increasing Complexity of Network & Applications**
  - Increasing complexity of network connectivity
    - Varying collection of ISPs, Wireless WAN/LAN, Home networking …
    - Dial-up, DSL, Cable modem, Wireless, Satellite, Power line …
  - Increasing complexity of network protocols & applications
    - Peer-to-peer networking protocols, multimedia over IP
  - Internet everywhere: More complexity of management
    - Mobile phones, home appliances ...
  - Complexity is the Worst Enemy of Security & Management

Internet Security Issues

- **More Distributed Networking / Applications Emerging**
  - Distributed file sharing/computing
  - Peer-to-peer networking, Home networking
  - Ubiquitous computing
- **Vulnerable Software Everywhere**
  - Vulnerability in software is inevitable and continues to appear
  - Vulnerable security products deployed
- **Sophistication & Automation of Attack Tools**
  - Attack tools / toolkits are becoming more sophisticated, automated, easy to use & hard to trace back
  - No specific knowledge required to mount attacks
  - Global collaboration is essential

Major Internet Security Technologies



The OSI Security Architecture

- ITU-T Recommendation X.800, *Security Architecture for OSI* defines
  - **Security attack**
    - Any action that compromises the security of information
  - **Security mechanism**
    - A process designed to detect, prevent, or recover from a security attack
  - **Security service**
    - A service making use of security mechanisms to counter security attacks.

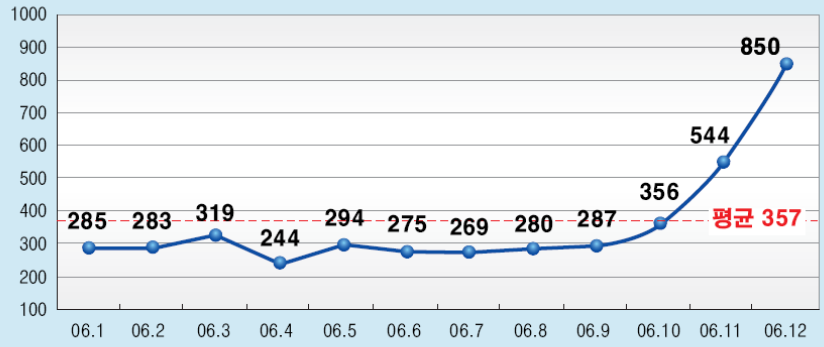
The OSI Security Architecture

Security Attacks	Security Mechanisms	Security Services
Interception Forgery Modification Denial of facts Unauthorized access Interruption	Encryption Authentication Digital signature Key exchange Access control Monitoring & Responding	Confidentiality Authentication Integrity Non-repudiation Access control Availability

Security Violations

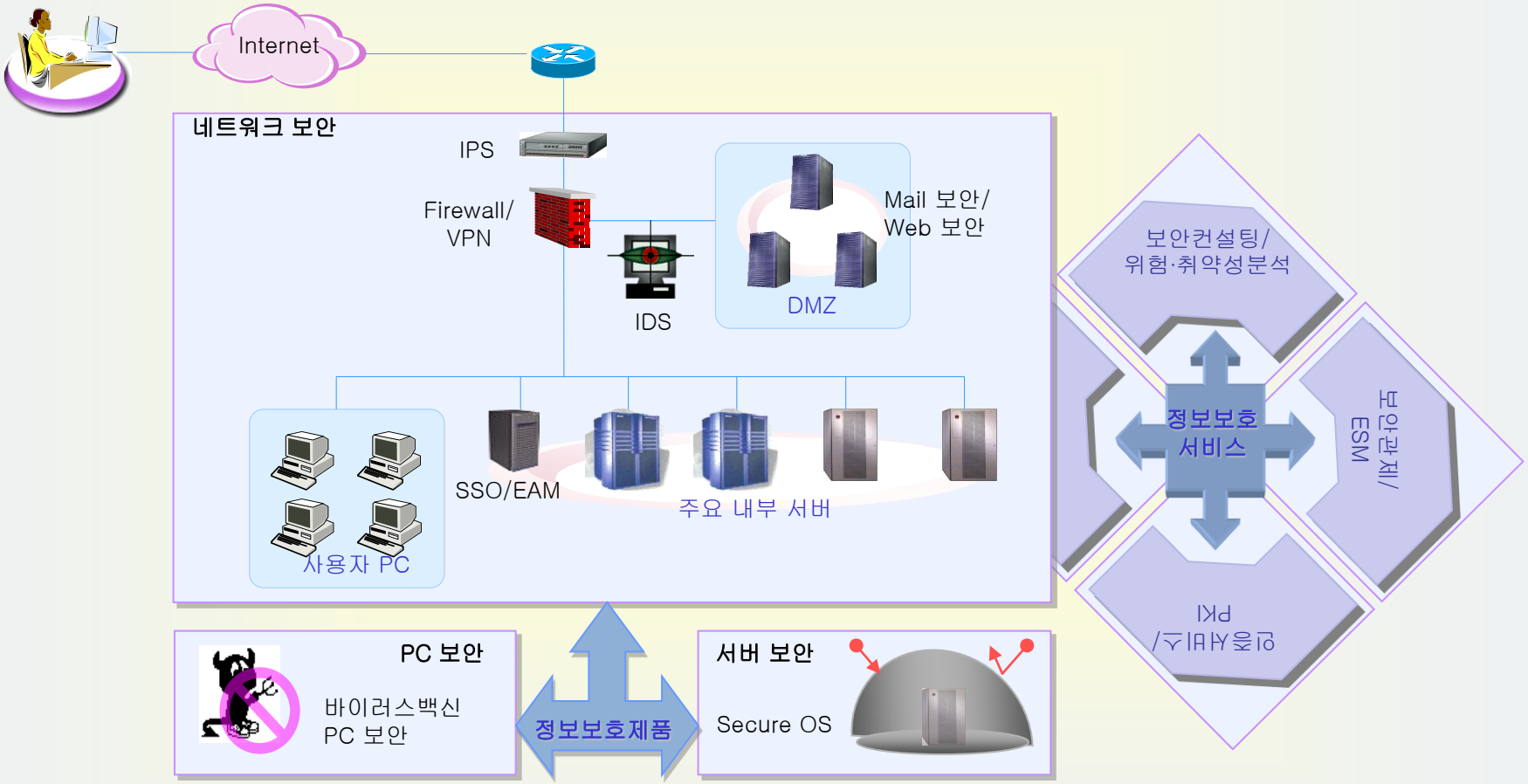
구분	2005년 총계	2006년												2006년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
웜·바이러스	16,093	606	859	556	395	427	745	396	683	865	892	773	592	7,789
해킹신고처리	33,633	2,225	1,968	2,032	1,799	2,175	2,433	2,284	2,787	2,263	2,503	2,409	1,930	26,808
- 스팸릴레이	6,334	782	682	957	788	1,162	1,418	1,314	1,685	1,318	1,336	1,407	1,206	14,055
- 피싱경유지	1,087	78	118	125	120	130	114	85	119	97	97	83	100	1,266
- 단순침입시도	-	161	218	225	365	285	227	327	353	444	561	350	195	3,711
- 기타해킹	9,520	330	358	248	325	444	556	406	530	355	380	325	313	4,570
- 홈페이지변조	16,692	874	592	477	201	154	118	152	100	49	129	244	116	3,206
봇(Bot)	18.8%	10.0%	11.8%	14.6%	10.1%	9.1%	11.4%	14.1%	13.1%	13.1%	16.9%	12.6%	13.2%	12.5%

* From KrCERT/CC



2006년 월별 사이버 침해사고 발생 추이

Information Security Industry

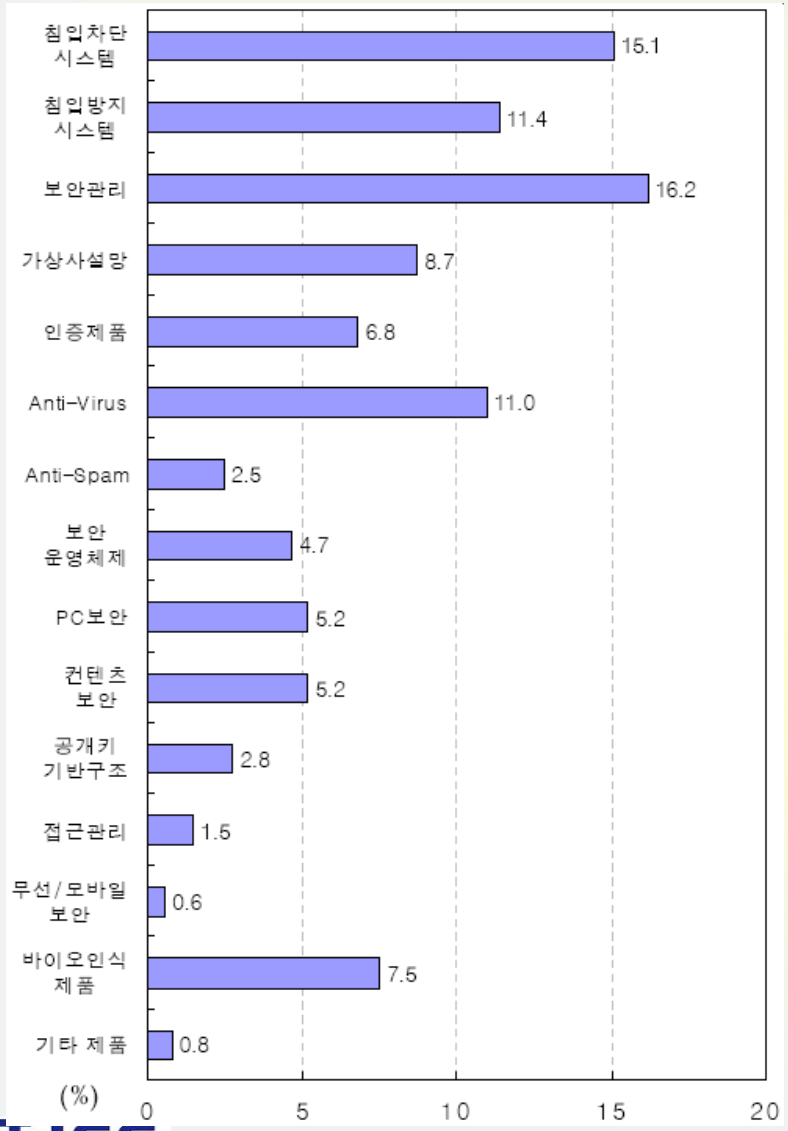


Information Security Industry

Current view

대분류	소분류	기호	세부 항목 예시
정보보호 H/W	침입차단	A	1. 침입차단시스템 2. 웹방화벽 3. 통합보안제품**
	침입방지	B	1. 방화벽 기반 2. 침입탐지시스템 기반 3. 네트워크장비 기반 4. 통합보안 제품**
	가상사설망	C	1. VPN 단일제품 2. 통합보안제품**
	망 전환 장치	D	1. 망 전환 장치
	H/W 인증	E	1. 보안 스마트카드 2. H/W 토큰
	생체인식	F	1. PC/네트워크보안 2. 출입통제/근태관리 3. 법 집행용 4. 금융/결재 시스템 5. 신원인증 6. 기타
정보보호 S/W	보안 관리 S/W	G	1. 통합보안관리 툴 2. 로그 관리/분석 툴 3. 취약점 분석 툴
	침입탐지 S/W	H	1. HIDS 2. HIPS 3. NIDS
	방화벽 S/W	I	1. 개인용 2. 기업용
	Anti Virus	J	1. Virus 백신 2. Anti 스파이웨어
	Anti Spam	K	1. 스팸차단 S/W
	시스템 보안	L	1. Secure OS 2. 서버 보안
	PC 보안	M	1. PC 보안
	어플리케이션 보안	N	1. 내부정보유출방지 2. DB보안 3. DRM(문서/이메일)
	3A	O	1. PKI 2. EAM 3. SSO 4. IM/IAM
	무선/모바일 보안	P	1. WPKI 2. WLAN 보안 3. 모바일 백신
정보보호 서비스	인증 서비스	Q	1. 공인/사설 인증 서비스
	보안 관제	R	1. 보안관제 서비스
	보안 컨설팅	S	1. 안전진단 2. 인증 3. 기반보호
	유지 보수	T	1. 판매 후 유료서비스
	기술 공급	U	1. 기술/ DB 제공
	기타서비스	V	1. 교육 훈련 서비스 2. 보안 제품 렌탈/임대

Information Security Industry



[단위 : 백만원]

대분류	소분류	2005년	2006년	증감율(%)
시스템 및 네트워크 정보보호 제품	침입차단(방화벽)시스템	89,108	94,554	6.1
	침입방지시스템(IPS)	62,406	71,469	14.5
	보안관리	87,957	101,038	14.9
	가상사설망(VPN)	53,776	54,558	1.5
	인증제품	56,736	42,691	-24.8
	Anti-Virus	57,935	68,671	18.5
	Anti-Spam	10,756	15,438	43.5
	보안운영체제(Secure OS)	28,652	29,144	1.7
	PC 보안	29,500	32,662	10.7
	컨텐츠 보안	27,329	32,554	19.1
	공개키기반구조(PKI)	16,085	17,735	10.3
	접근관리	11,221	9,087	-19.0
	무선/모바일 보안	2,516	3,646	44.9
	바이오인식 제품	43,195	46,725	8.2
	기타 제품	6,251	5,210	-16.7
	소 계	583,423	625,182	7.2
정보보호 서비스	인증서비스	6,549	7,465	14.0
	보안관제	22,241	26,602	19.6
	보안컨설팅	26,331	31,093	18.1
	유지보수	40,051	43,186	7.8
	기타서비스	2,110	1,264	-40.1
	소 계	97,282	109,610	12.7
합 계		680,705	734,792	7.9

2. Cryptology

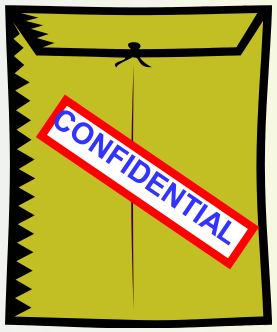
Cryptography

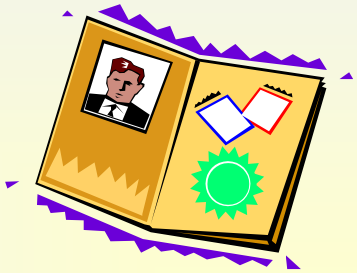
- Cryptography is a basic tool to implement information security

- Security goals
  - Secrecy (confidentiality)
  - Authentication
  - Integrity
  - Non-repudiation
  - Verifiability
  - More application-specific security goals

- Achieve these security goals using cryptography
  - Without cryptography …. ???

Physical vs. Cryptographic Solutions





Physical Solutions

- Temper-evident sealed envelope
- ID-card, Passport, Drivers license
- Signature

Cryptographic Solutions (for communications over open network)

- Encryption with MAC : Confidentiality, Authentication, Integrity Protection
- Digital Certificate : Identification
- Digital Signature : Authentication, Integrity Protection, Non-Repudiation
- Security mechanisms are combined to provide a security service
  - ✓ VPN, Firewall, IDS, etc.

Cryptology = Cryptography + Cryptanalysis

- **Cryptography(암호설계) : designing secure cryptosystems**
  - **Cryptography (from the Greek kryptós and gráphein, “to write”) was originally the study of the principles and techniques by which information could be concealed in ciphers and later revealed by legitimate users employing the secret key.**
- **Cryptanalysis(암호해독) : analyzing the security of cryptosystems**
  - **Cryptanalysis (from the Greek kryptós and analýein, “to loosen” or “to untie”) is the science (and art) of recovering or forging cryptographically secured information without knowledge of the key.**
- **Cryptology(암호학) : science dealing with information security**
  - **Science concerned with data communication and storage in secure and usually secret form. It encompasses both cryptography and cryptanalysis.**

Common Terms

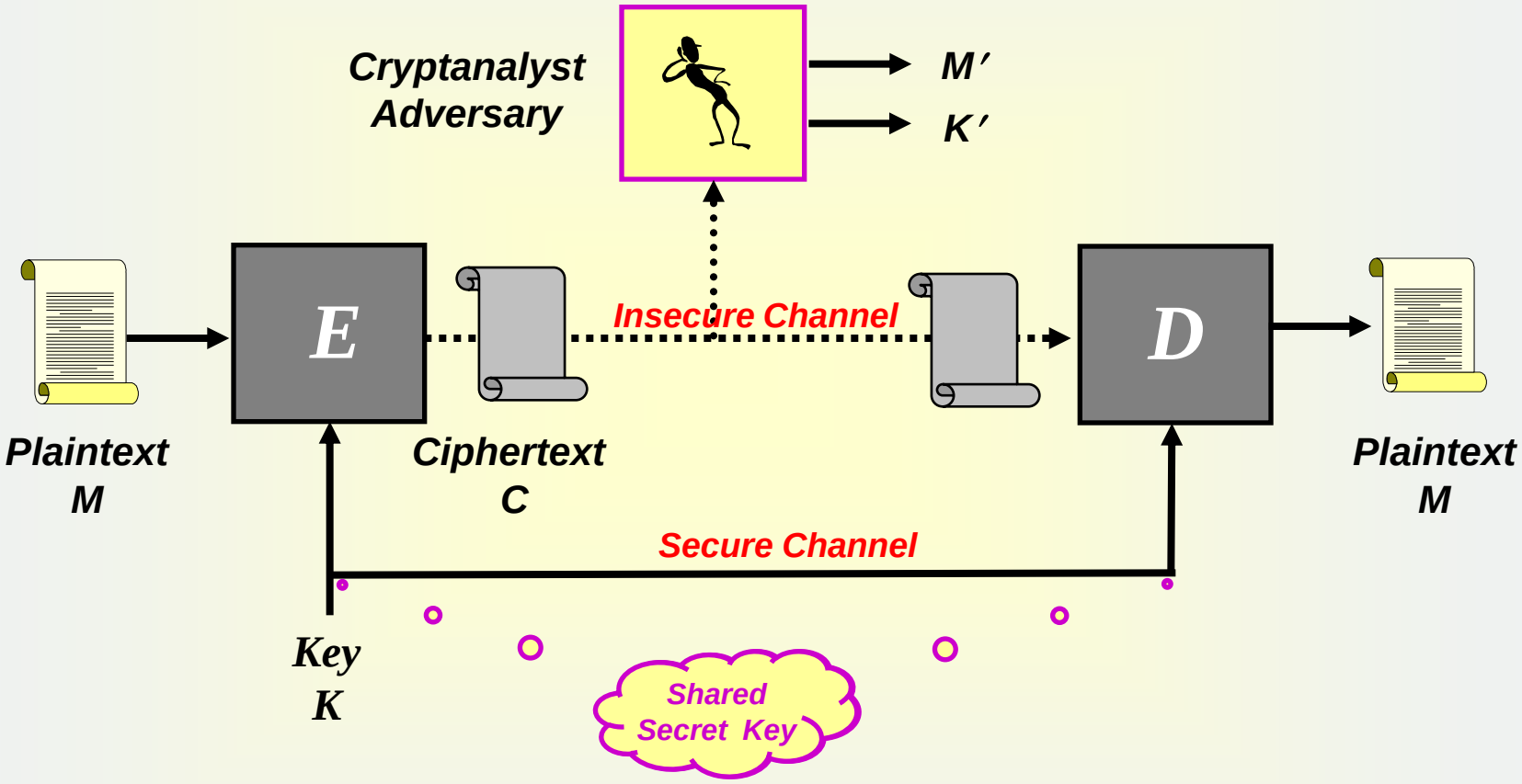
- Cipher: Block cipher, Stream cipher, Public key cipher
- Plaintext/Cleartext (평문), Ciphertext (암호문)
- Encryption/Encipherment(암호화)
- Decryption/Decipherment(복호화)
- Key (or Cryptographic key)
  - Secret key
  - Private key / Public key
- Hashing (해쉬)
- Authentication (인증)
  - Message authentication
  - User authentication
- Digital signature (전자서명)

Cryptographic Primitives

- **Block / Stream Cipher**
  - 3DES, AES, SEED, RC2, RC5, … / RC4, SEAL …
- **Hash Function**
  - MD5, SHA1/SHA2, HAS160, RMD160, Tiger …
- **Message Authentication Code (MAC)**
  - HMAC, CBC-MAC, UMAC

- **Public Key Encryption**
  - RSA, ElGamal
- **Digital Signature**
  - RSA, DSA/ECDSA, KCDSA/EC-KCDSA …
- **Key Exchange**
  - Diffie-Hellman, ECDH, RSA key transport

Symmetric Encryption Model

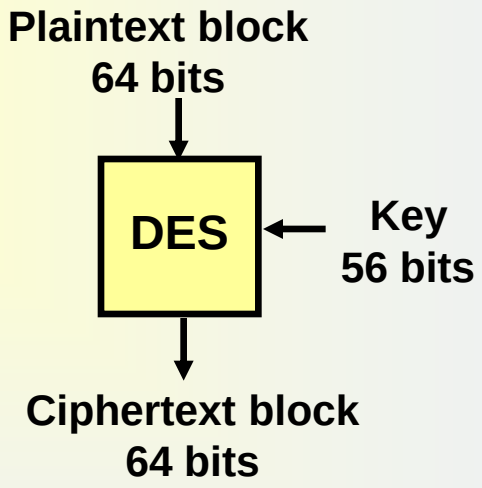


Data Encryption Standard (DES)

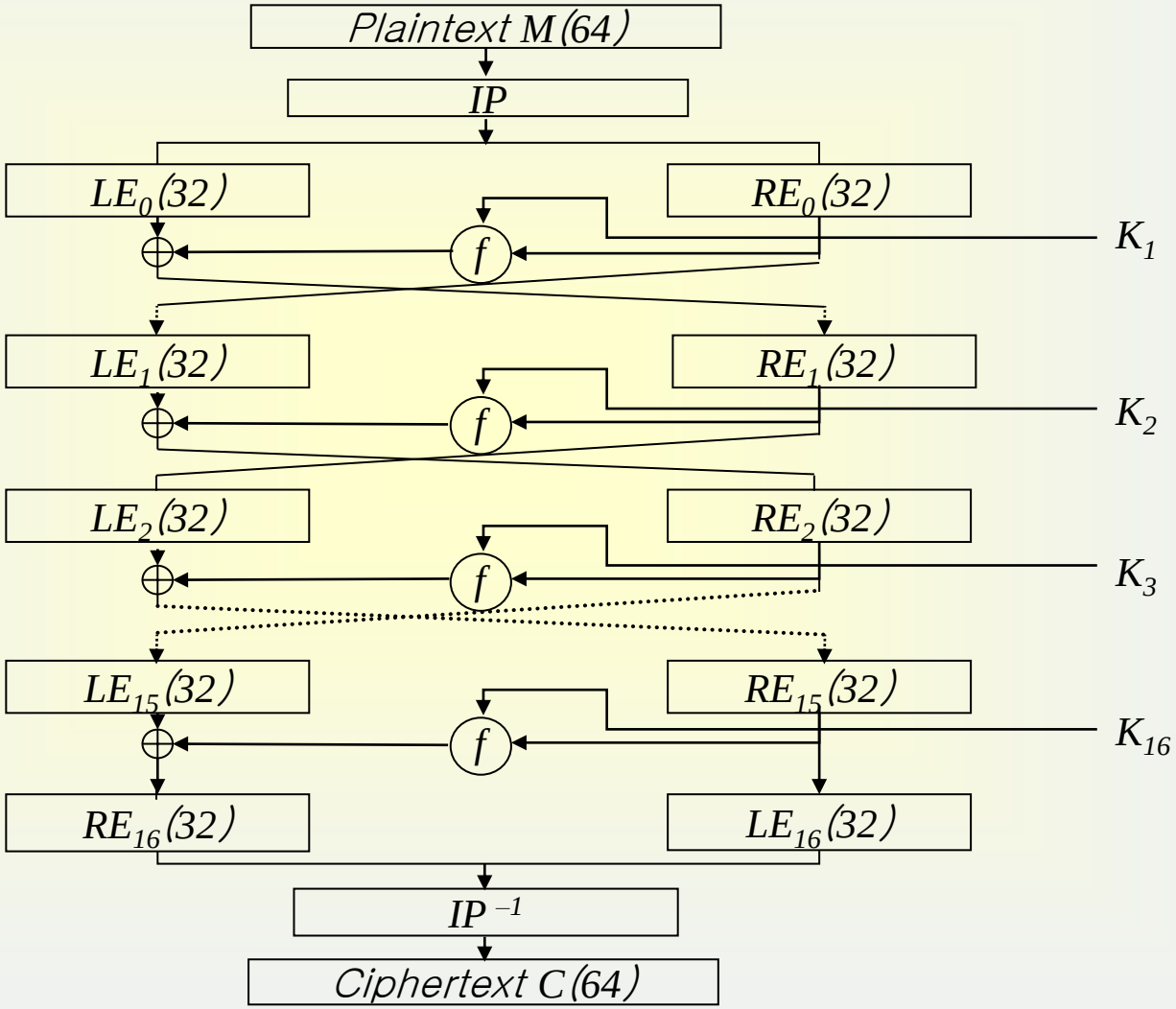
- **DES - History**
  - ✓ 1976 – adopted as a federal standard
  - ✓ 1977 – official publication as FIPS PUB 46
  - ✓ 1983, 1987, 1993 – recertified for another 5 years

* Federal Information Processing Standards

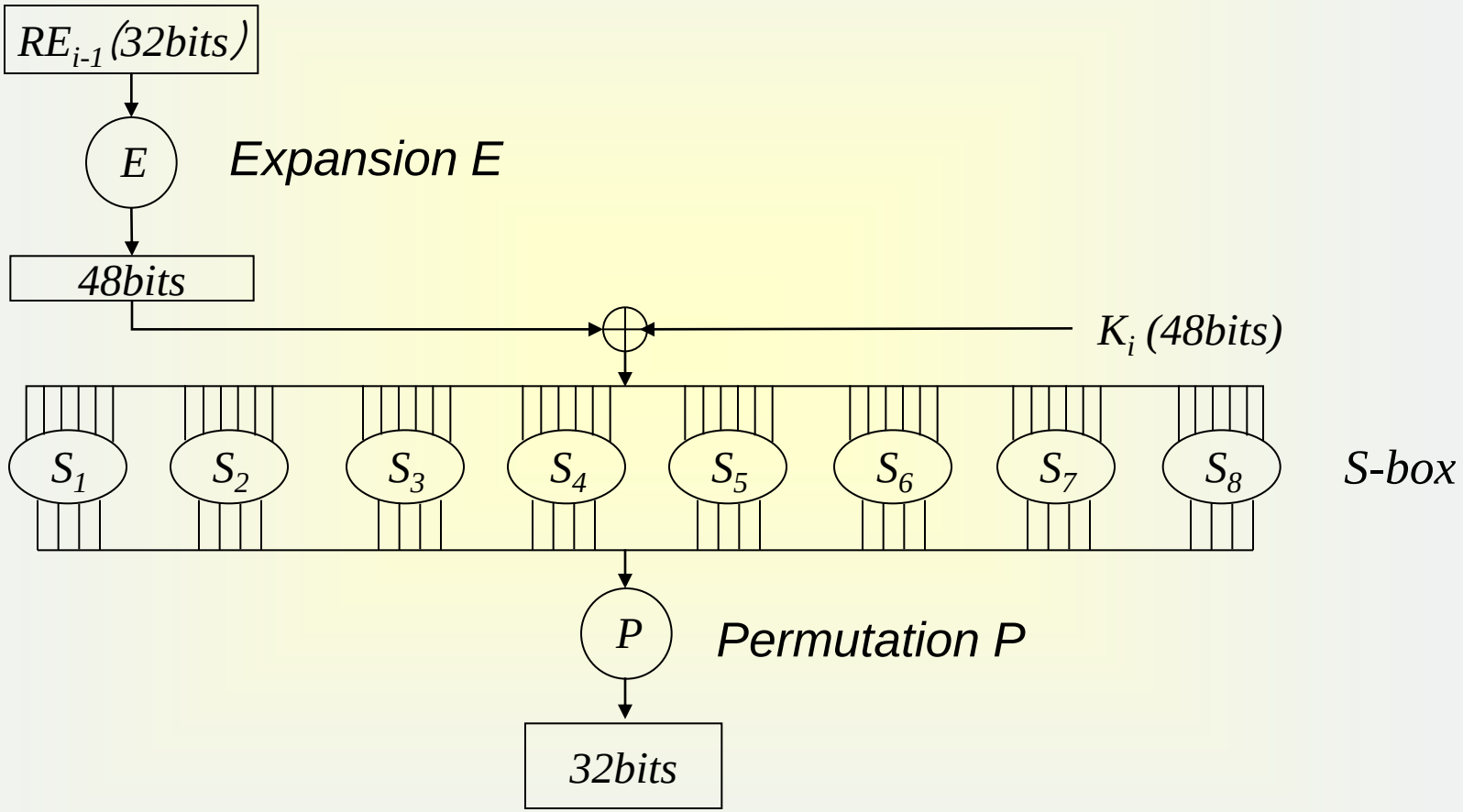
- **Design Criteria of DES**
  - ✓ Provide a high level of security
  - ✓ Completely specify and easy to understand
  - ✓ Security must depend on hidden key, not algorithm
  - ✓ Available to all users
  - ✓ Adaptable for use in diverse applications
  - ✓ Economically implementable in electronic device
  - ✓ Able to be validated
  - ✓ Exportable



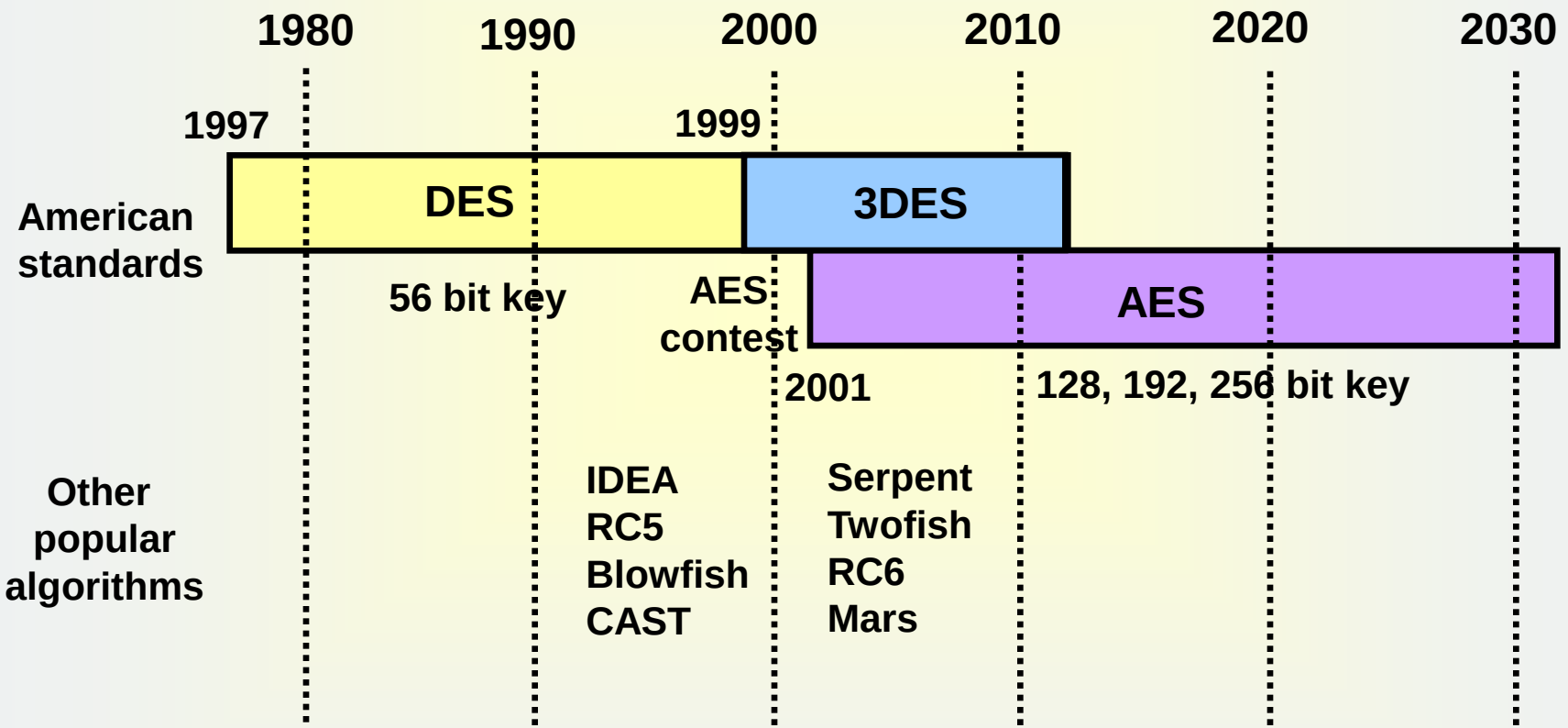
DES Overview



Nonlinear Function $f(k_i, RE_{i-1})$

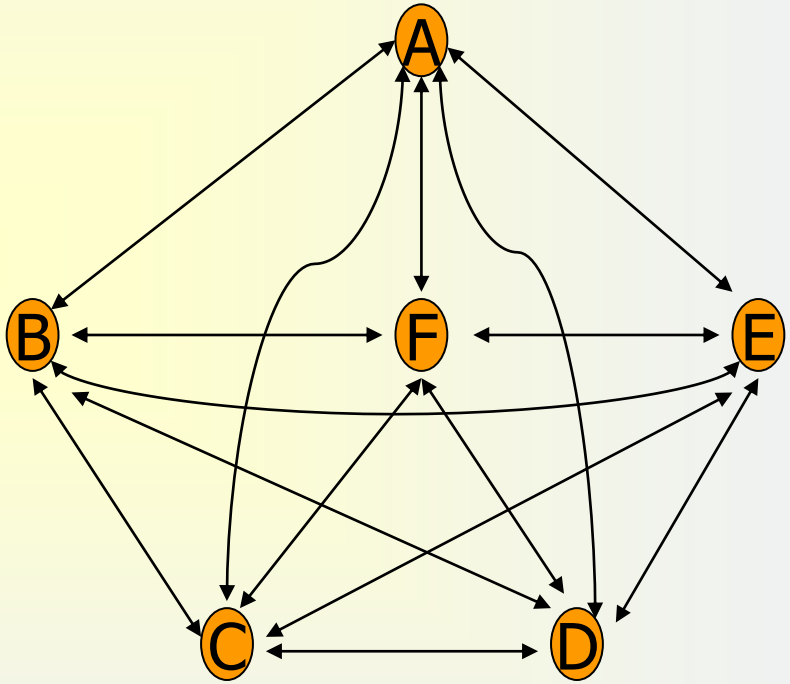


History of Symmetric Ciphers



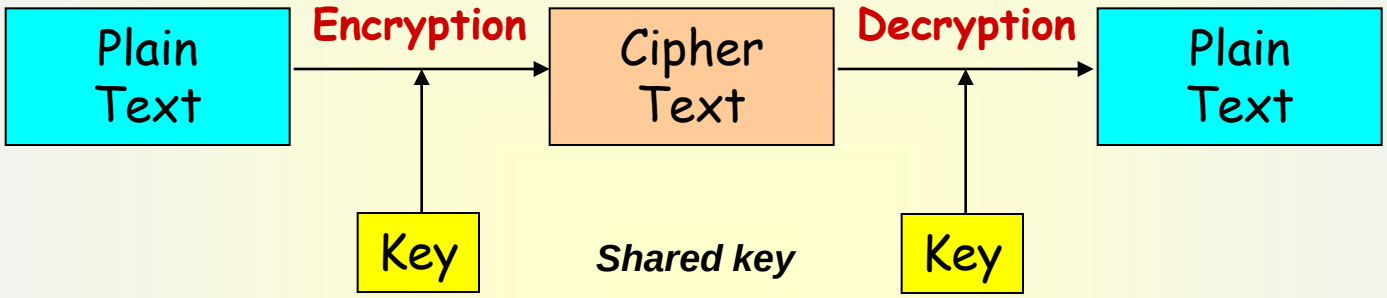
Key Distribution Problem

- **Symmetric Key Cryptosystem**
  - ✓ $_nC_2 = n(n-1)/2$ secret keys are required
  - ✓ How to keep them securely?

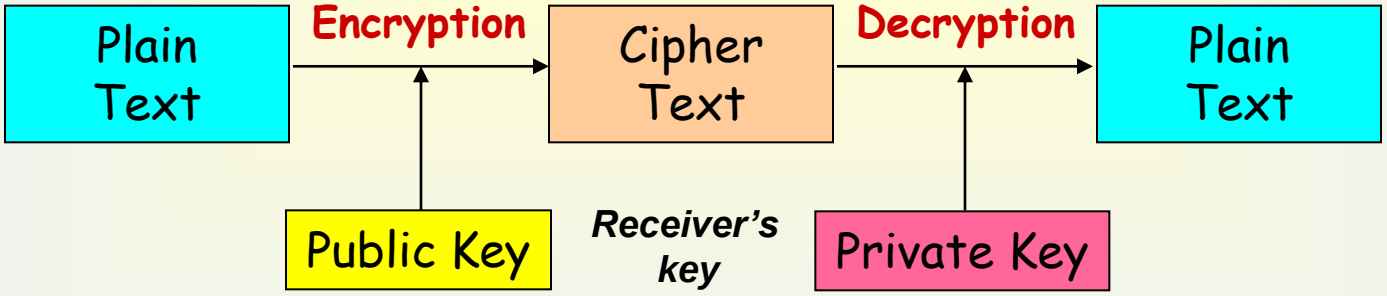


Secret Key vs. Public Key Systems

- **Symmetric Key Cryptosystem**

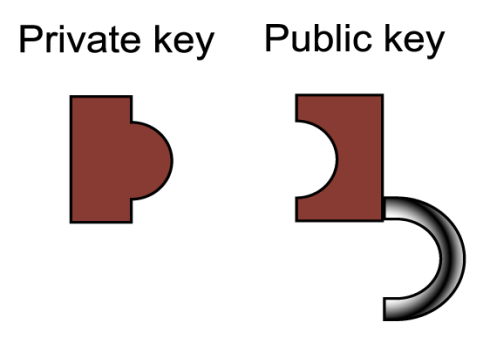


- **Public Key Cryptosystem**



Public Key Cryptography - Concept

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

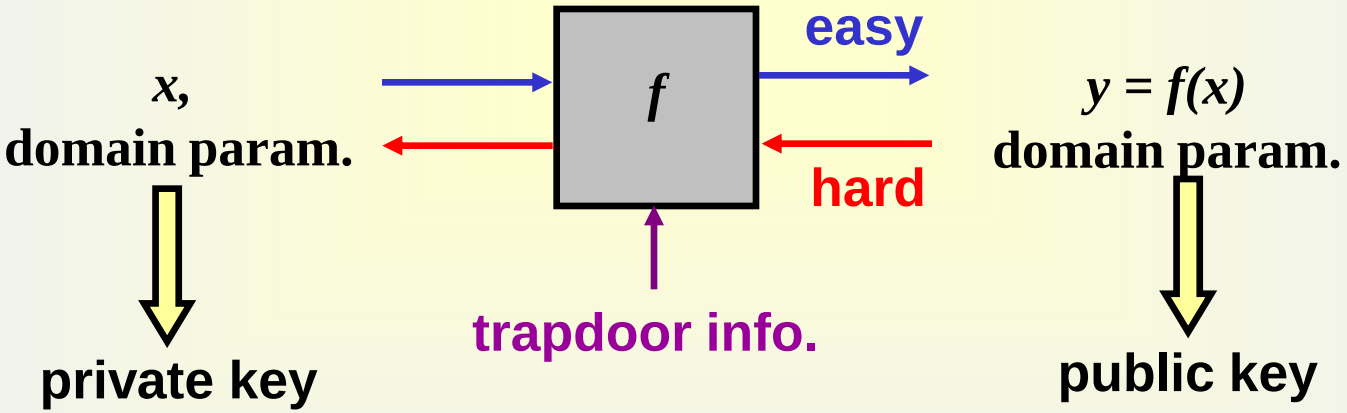
- **Only the signer can sign (using the private key)**
- **Anyone can verify (using the public key)**

Public Key Cryptography

- Keys
  - ✓ A pair of (Public Key, Private Key) for each user
  - ✓ Public keys must be publicly & reliably available
- Public Encryption
  - ✓ Encrypt with peer's Public Key; Decrypt with its own Private Key
  - ✓ RSA, ElGamal
- Digital signature
  - ✓ Sign with its own Private Key; verify with peer's Public Key
  - ✓ RSA, DSA, KCDSA, ECDSA, EC-KCDSA …
- Key exchange
  - ✓ Key transport or key agreement for secret-key crypto.
  - ✓ RSA; DH(Diffie-Hellman), ECDH

Public Key Cryptography

- Invented by Diffie and Hellman in 1976
- Solve the secret key sharing problem in symmetric cryptosystems
- Two keys used: public key & private key
- Also known as two-key cryptography or asymmetric cryptography
- Based on (trapdoor) one-way function



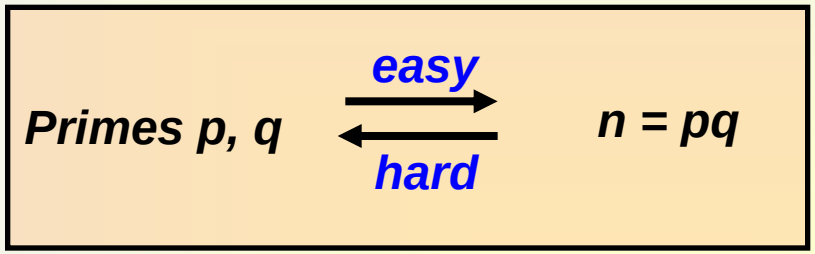
But, easy if trapdoor info. is given.

Public Key Cryptosystems – History

- 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
- ElGamal scheme (1985)
- Elliptic Curve Cryptosystem (1985): Koblitz, Miller
- Non-Abelian group Cryptography (2000): Braid group

Integer Factorization Problem (IFP)

- **Problem: Given a composite number n, find its prime factors**



- **Application: Used to construct RSA-type public key cryptosystems**

- **Algorithms to solve IFP (probabilistic sub-exponential algorithms)**
  - **Quadratic sieve**
  - **General Number Field Sieve**

Discrete Logarithm Problem (DLP)

- **Problem:**
  Given g, y, and prime p, find an integer x, if any, such that
  $y = g^x \bmod p$ ($x = \log_g y$)

Given g, x, p	*easy* →	$y = g^x \bmod p$
$x = \log_g y$	← *hard*	*Given g, y, p*

- **Application: Used to construct Diffie-Hellman & ElGamal-type public key systems: DH, DSA, KCDSA …**

- **Algorithms to solve DLP:**
  - **Shank's Baby Step Giant Step**
  - **Index calculus**

RSA Challenge Solution

RSA-160

Date: Tue, 1 Apr 2003 14:05:10 +0200
From: Jens Franke
Subject: RSA-160

We have factored RSA160 by gnfs. The prime factors are:
p=4542789285848139407168619064973883 1\ 656137145778469793250959984709250004157335359
q=4738809060383201619663383230378895 1\ 973268922921040957944741354648812028493909367

http://www.loria.fr/~zimmerma/records/rsa160

RSA-200

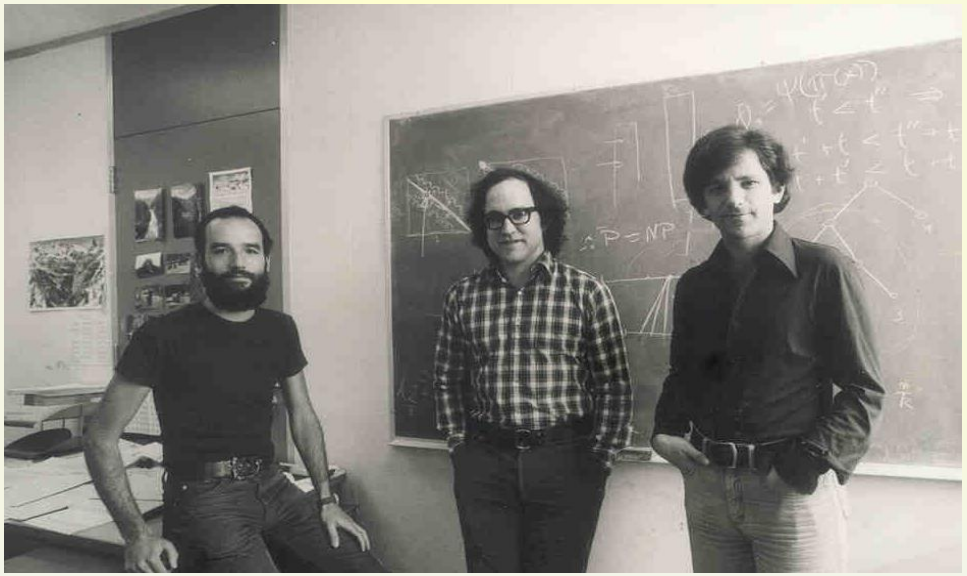
Date: Mon, 9 May 2005 18:05:10 +0200 (CEST)
From: Thorsten Kleinjung
Subject: rsa200

We have factored RSA200 by GNFS. The factors are
p=35324619344027701212726049781984643686711974001976\ 25023649303468776121253679423200058547956528088349
and
q=79258699544783330333470858414800596877379758573642\ 19960734330341455767872818152135381409304740185467

http://www.loria.fr/~zimmerma/records/rsa200

RSA Public Key Systems

- RSA is the first public key cryptosystem
- Proposed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT
- It is believed to be secure and still widely used
- Patent : *US Patent 4,405,829, expired on 21 September 2000*



Shamir *Rivest* *Adleman*

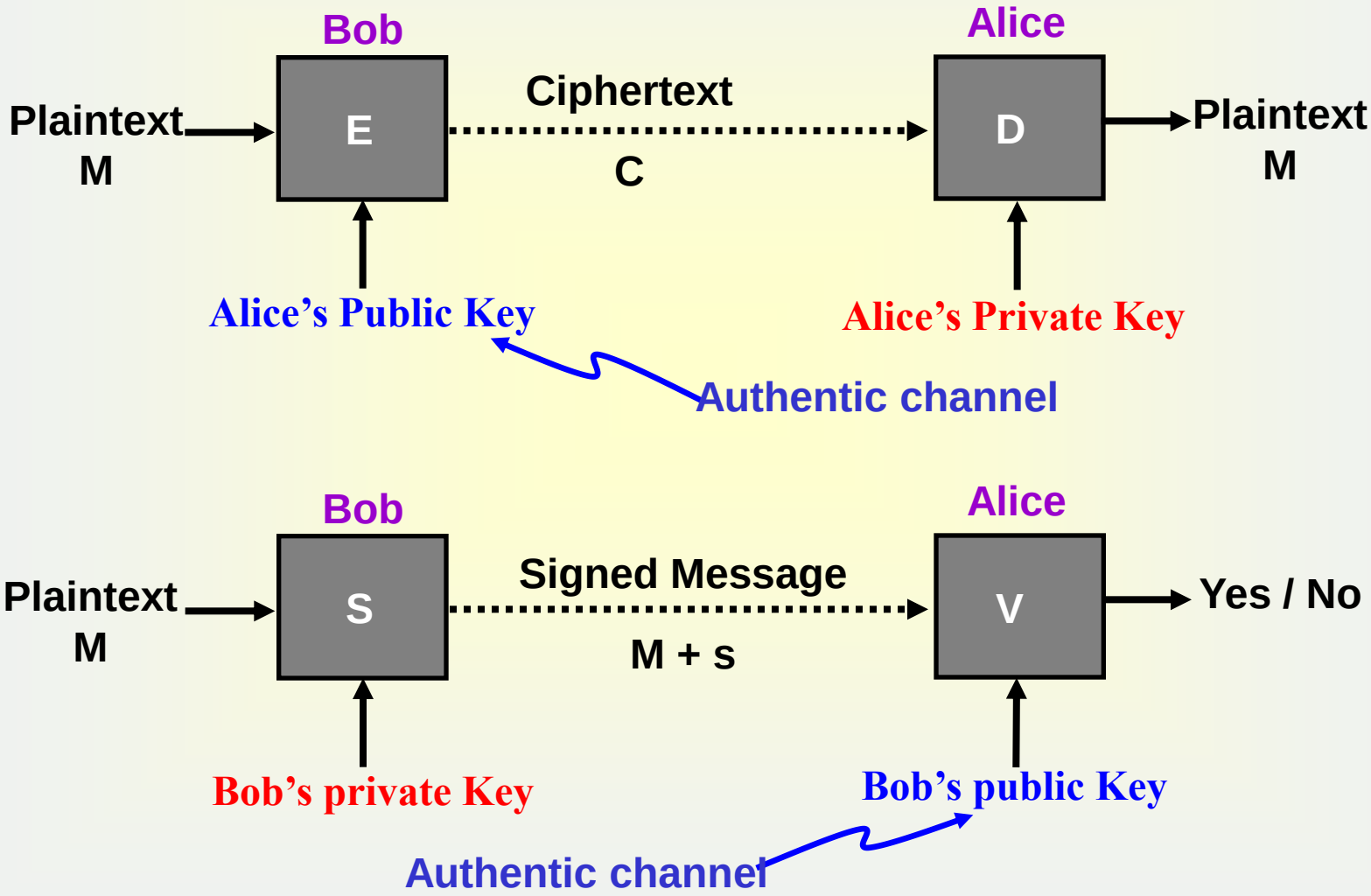
RSA Public Key Systems

- **Key generation**
  - Choose two large (512 bits or more) primes p & q
  - Compute modulus n = pq, and $\phi(n) = (p-1)(q-1)$
  - Pick an integer e relatively prime to $\phi(n)$, $\gcd(e, \phi(n))=1$
  - Compute d such that $ed = 1 \bmod \phi(n)$
  - **Public key (n, e)** : publish
  - **Private key d** : keep secret (may discard p & q)

- **Special Property**
  - $(m^e \bmod n)^d \bmod n = (m^d \bmod n)^e \bmod n$ for $0 < m < n$

- **Encryption / Decryption**
  - E: $c = m^e \bmod n$ for $0 < m < n$
  - D: $m = c^d \bmod n$
  - Proof) $C^d = (M^e)^d = M^{ed} = M^{k\phi(n)+1} = M\{M^{\phi(n)}\}^k = M$

Public Key Encryption vs. Signature



Digital Signature

- Digital Signature
  - Electronic version of handwritten signature on electronic document
  - Signing using private key (only by the signer)
  - Verification using public key (by everyone)

- Hash then sign: sig(h(m))
  - Efficiency in computation and communication

Digital Signature

- **Security requirements for digital signature**
  - **Unforgeability (위조 방지)**
  - **User authentication (사용자 인증)**
  - **Non-repudiation (부인 방지)**
  - **Unalterability (변조 방지)**
  - **Non-reusability (재사용 방지)**

- **Services provided by digital signature**
  - **Authentication**
  - **Data integrity**
  - **Non-Repudiation**

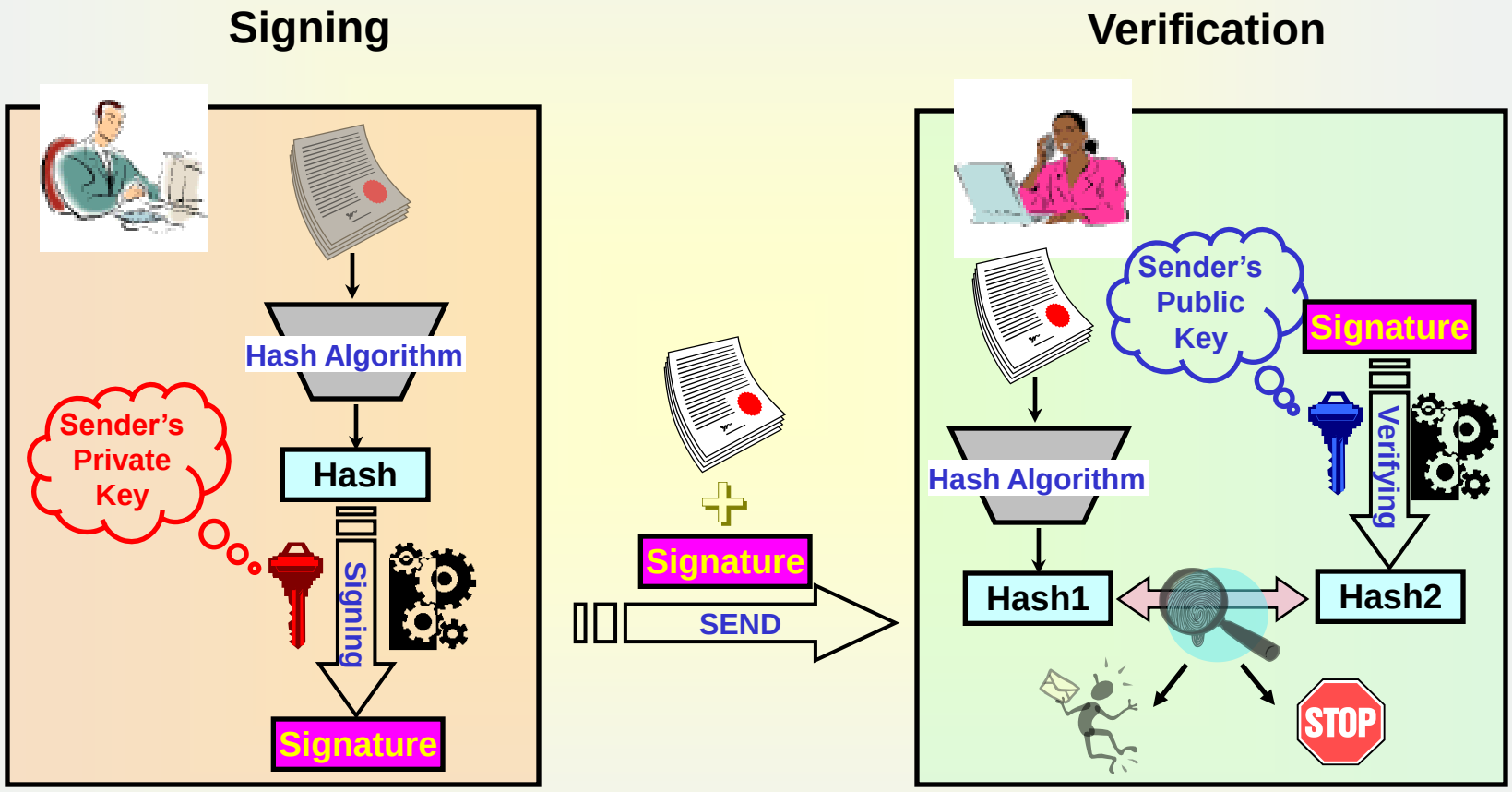
RSA Signature

- **Key generation**
  - Choose two large (512 bits or more) primes p & q
  - Compute modulus n = pq, and $\phi(n) = (p-1)(q-1)$
  - Pick an integer e relatively prime to $\phi(n)$, $\gcd(e, \phi(n))=1$
  - Compute d such that $ed = 1 \bmod \phi(n)$
  - **Public key (n, e)** : publish
  - **Private key d** : keep secret (may discard p & q)

- **Signing / Verifying**
  - S: $s = m^d \bmod n$ for $0 < m < n$
  - V: $m =? s^e \bmod n$
  - S: $s = h(m)^d \bmod n$ --- hashed version
  - V: $h(m) =? s^e \bmod n$

- **RSA signature without padding**
  - Deterministic signature, no randomness introduced

Digital Signature

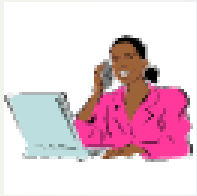


Digital Enveloping : Key Transport + Encryption

Bob's Public Key/Private Key

Alice's Public Key

Randomly Generated Session Key



Hash Algorithm

Hash

Signing

Signature

Signature

Encryption

Encrypted Message

Symmetric Key Cryptosystem

Encrypted Session Key

Encrypted Message

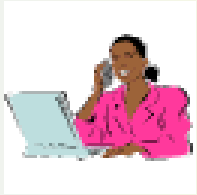
SEND

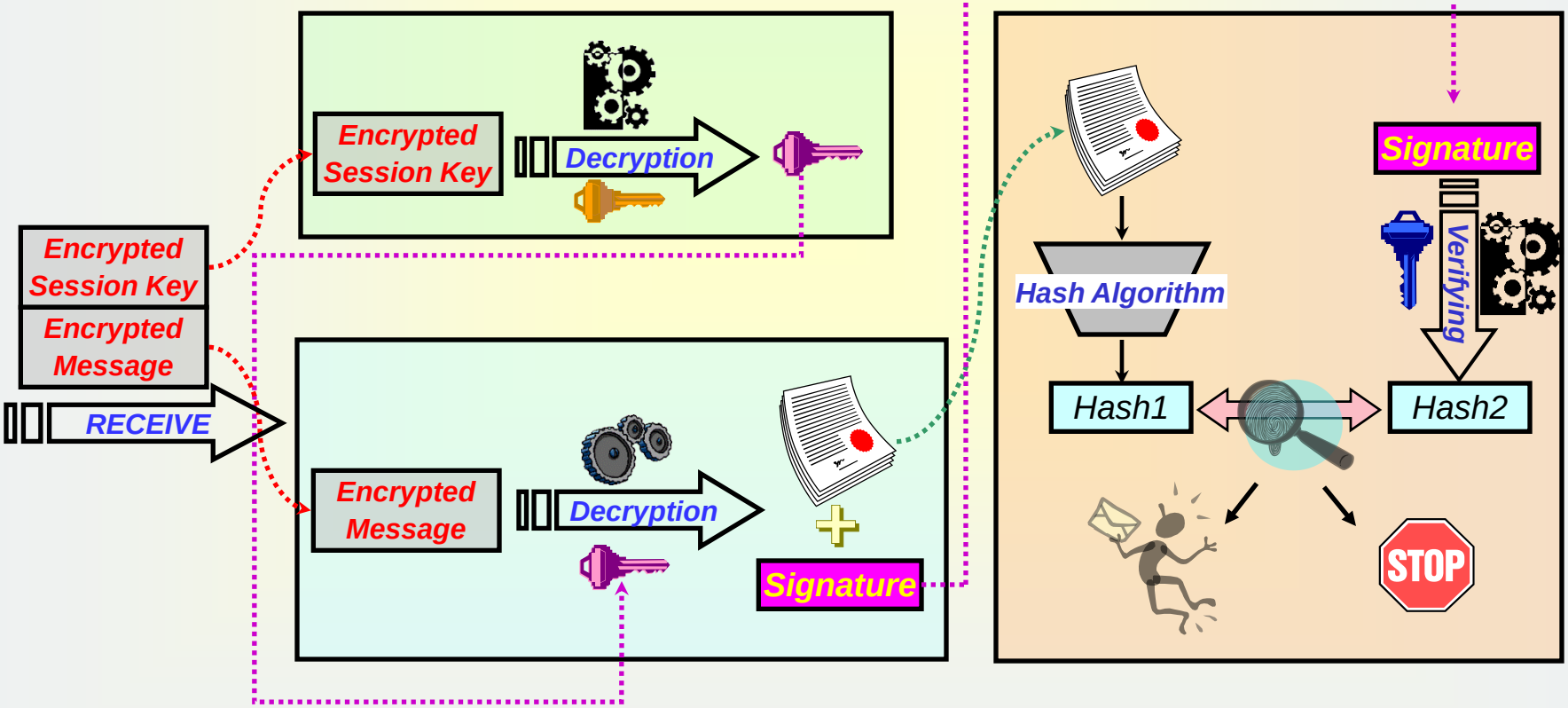
Encryption

Encrypted Session Key

Public Key Cryptosystem

Digital Enveloping : Key Recovery + Decryption

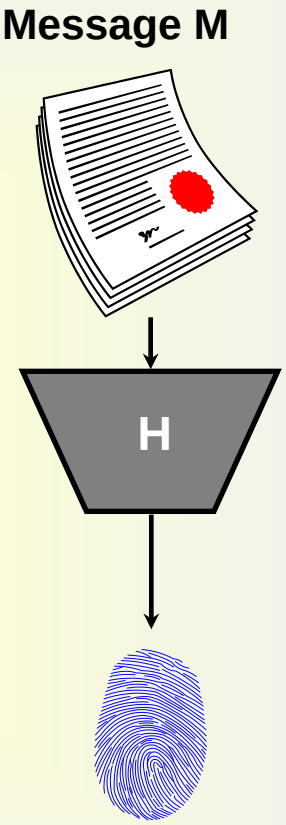




Hash Functions

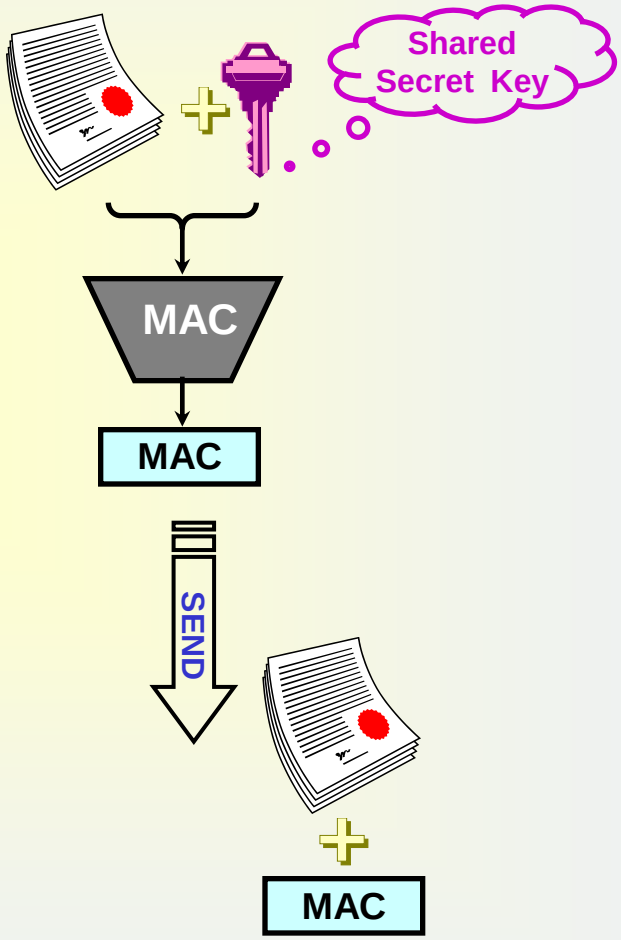
- **Hash Function**
  - ✓ Generate a fixed length "Fingerprint" for an arbitrary Message
  - ✓ No Key involved
  - ✓ One Way Function
  - ✓ MD5, SHA1, SHA2, HAS160

- **Applications**
  - ✓ Keyed hash: used to generate/verify MAC(Message Authentication Code) or Integrity Check Value(ICV) → HMAC
  - ✓ Unkeyed hash: used to produce Digital Signature



Message Authentication Code (MAC)

- **Purposes**
  - ✓ Secure tag for authentication
  - ✓ Message origin authentication
  - ✓ User authentication
  - ✓ Message integrity
- **Schemes**
  - ✓ Keyed hash: HMAC
  - ✓ Block cipher: CBC-MAC, XCBC-MAC
  - ✓ Dedicated MAC: UMAC



Q & A

Thank you!