Week 2-1 : Introduction II

Are you ready to begin?

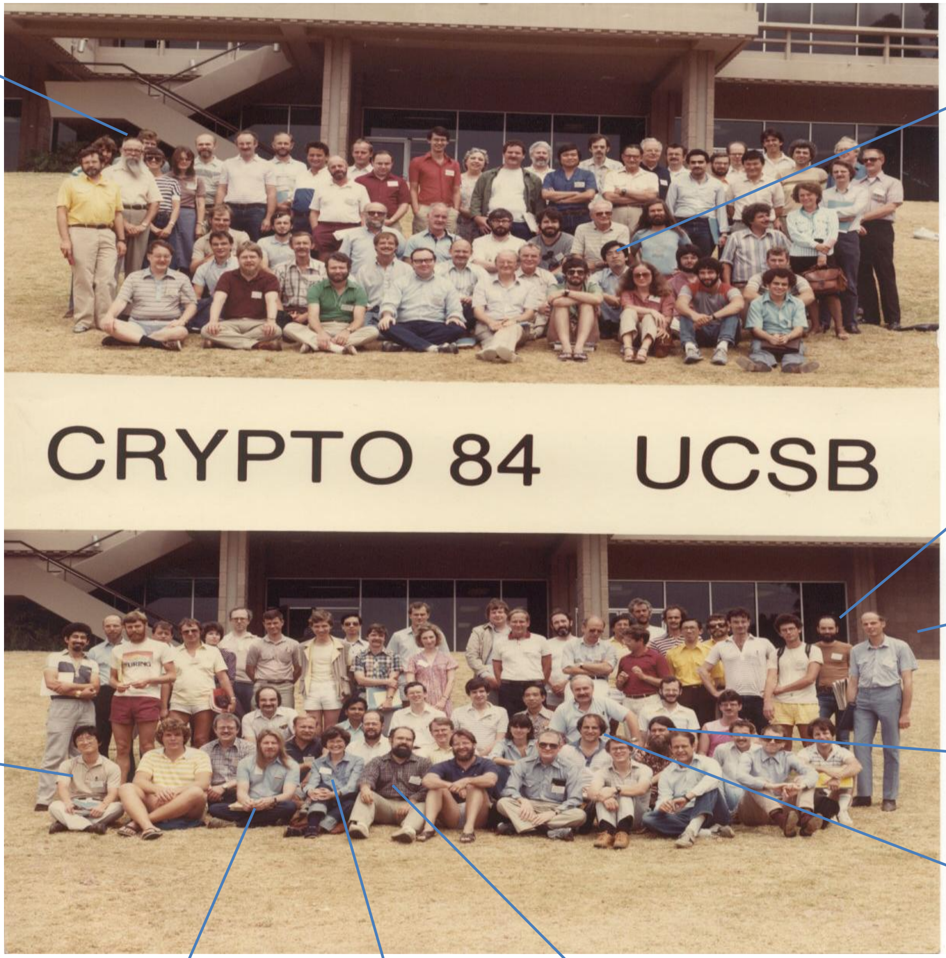
IACR

- International Associations for Cryptologic Research, http://www.iacr.org
- Non-profit organization registered in the USA, 1981
- Purposes : To advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare.
- J. of Cryptology by Springer and IACR Newsletter
- Cryptology eprint Archive: e-print.iacr.org

IACR Conferences

- Crypto (81~), UCSB, Aug, USA
- Crypto 2011: 14-18 Aug., UCSB, Santa Barbara
  Tom Shrimpton/Phil Rogaway+Rei Safavi-Naini
- Eurocrypt (82~), May to June, Europe
- Eurocrypt 2011: 15-19 May, Tallinn, Estonia
  Helger Lipmaa/Kenny Paterson+David Pointcheval

Crypto'84@UCSB



G. Simmons (passed away)

E.Okamoto

A.Shamir

J.Quisquater

K. Kim

D. Chaum

R. Rivest

W. Diffie

D.Denning

T. Berson

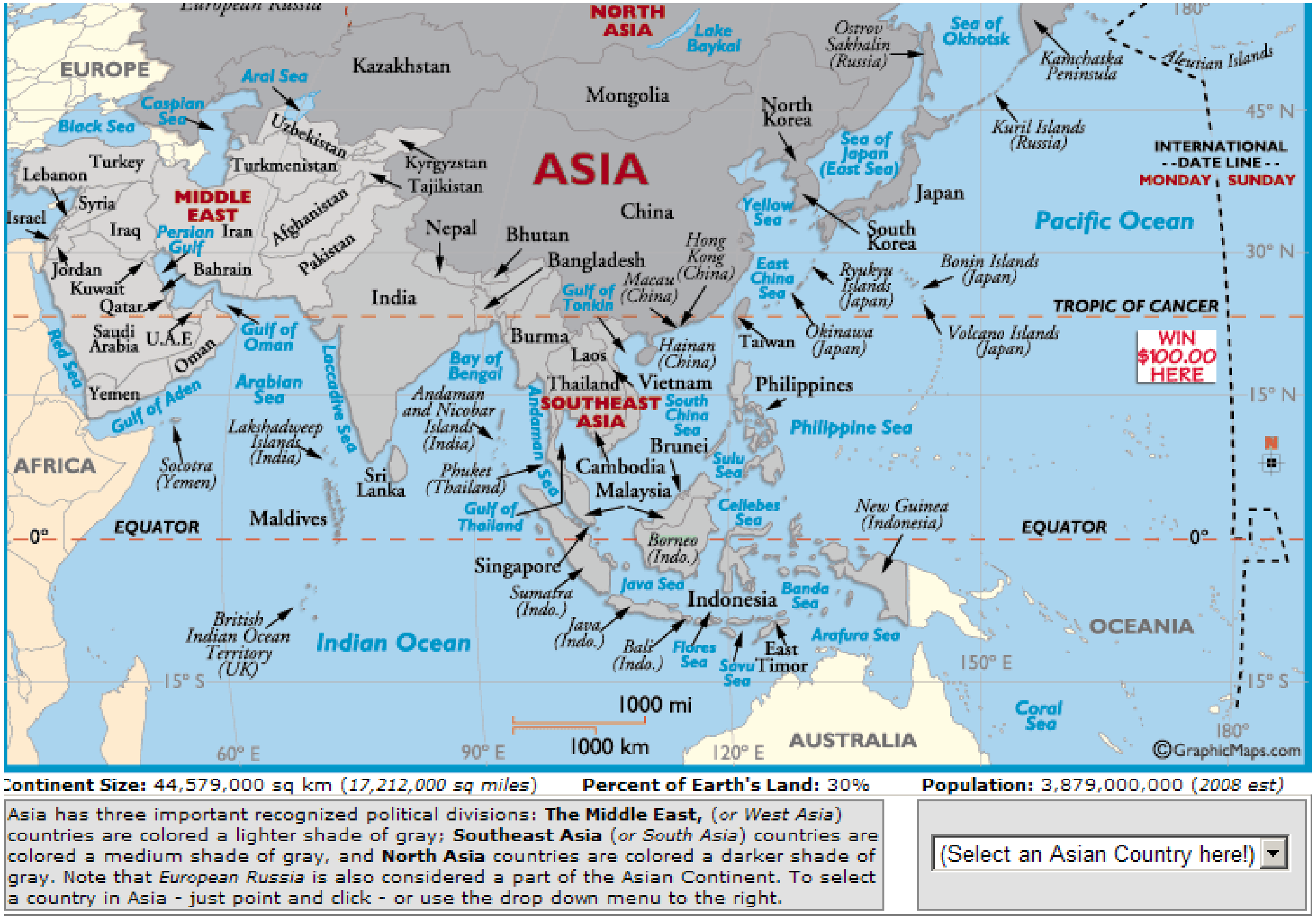
Crypto’97@UCSB

Joke*: Can you find K. Kim?*

ASC

- Asiacrypt Steering Committee
- Promote Cryptographic Research in Asian Countries
- 9 Member Countries
  - Australia, China, India, Japan, Korea, Malaysia, New Zealand, Singapore, Taiwan
  - 2 ~ 3 representatives per each country
- Propose venue of coming Asiacrypt’s by voting and its General Chair to IACR
- Annual meeting during Crypto and Asiacrypt

Where is Asia?



Continent Size: 44,579,000 sq km (*17,212,000 sq miles*) **Percent of Earth's Land:** 30% **Population:** 3,879,000,000 (*2008 est*)

Asia has three important recognized political divisions: **The Middle East,** (*or West Asia*) countries are colored a lighter shade of gray; **Southeast Asia** (*or South Asia*) countries are colored a medium shade of gray, and **North Asia** countries are colored a darker shade of gray. Note that *European Russia* is also considered a part of the Asian Continent. To select a country in Asia - just point and click - or use the drop down menu to the right.

Asiacrypt (1/3)

- Before IACR Sponsorship
  - Auscrypt90: Sydney, Australia, Jennifer Seberry/Josef Pieprzyk, Rainer Rueppel, Scott Vanstone
  - Asiacrypt91: Fujiyoshida, Japan, Shigeo Tsujii/Hideki Imai, Ron Rivest
  - Auscrypt92: Queensland, Australia, William Caelli/Jennifer Seberry (Merged into Asiacrypt)
  - Asiacrypt94: Wollongong, Australia, Jennifer Seberry/Josef Pieprzyk
  - Asiacrypt96: Kyongju, Korea, Man Young Rhee/Kwangjo Kim, Tsutomu Matsomuto
  - Asiacrypt98: Beijing, China, Keqin Feng/Kazuo Ohta, Dingyi Pei
  - Asiacrypt99: Singapore, Chao Ping Xing /Kwok Yan Lam, Eiji Okamoto

Asiacrypt (2/3)

- After IACR-Sponsorship
  - Asiacrypt2000: Kyoto, Japan, Tsutomu Matsumoto/Tatsuaki Okamoto
  - Asiacrypt2001: Gold Coast, Australia, Ed Dawson/Colin Boyd
  - Asiacrypt2002: Queenstown, New Zealand, Henry Wolfe/Yuliang Zheng
  - Asiacrypt2003: Taipei, Taiwan, Chin Chen Chang/Chi Sung Laih
  - Asiacrypt2004: Jeju Island, Korea, Kwangjo Kim/Pil Joong Lee
  - Asiacrypt2005: Chennai, India, C. Pandu Rangan/Bimal Roy
  - Asiacrypt2006: Shanghai, China, Dingyi Pei/Xuejia Lai
  - Asiacrypt2007: Sarawak, Malaysia, Raphael Phan/Kaoru Kurosawa
  - Asiacrypt2008: Melbourne, Australia, Lynn Batten/Josef Pieprzyk
  - Asiacrypt2009: Tokyo, Japan, Eiji Okamoto/ Mitsuru Matsui
  - Asiacrypt2010: Singapore, Ling San/Masayuki Abe

Asiacrypt (3/3)

- Asiacrypt2011: 4-8 Dec. Seoul, Korea
  Hyong-Joong Kim/ Dong Hoon Lee+Xiaoyun Wang

- Asiacrypt2012: 2-6 Dec. Beijing, China
  Xuejia Lai/Xioyun Wang

- Asiacrypt2013: Dec.1-5, Abu Dhabi, UAE

Korean Academic Society

- KIISC (Korea Institute for Information Security and Cryptology) established in 1990, http://www.kiisc.or.kr
- Domestic conference : CISC-S, CISC-W
- 3 local branches: ChungChung(M), YoungNam(LS), Honam (LW)
- International Annual Conferences:
  ICISC('97-), WISA('00-), IWDW('02-)
- More than 30 universities and 200 professors

Korean Security Institutes

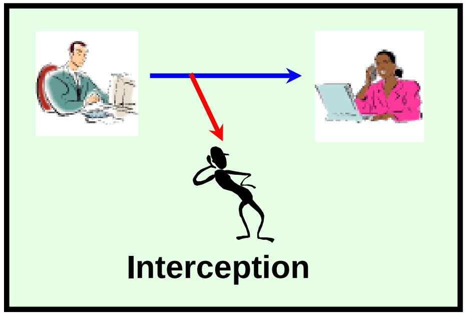
- NIS (National Intelligence Service)
  - NCSC (National Cyber Security Center)
- KISA (Korea Information & Internet Agency)
  - KrCERT (Computer Emergency Response Team)
  - ROOT CA (Certificate Authority)
- Research Institutes
  - ETRI (Electronics & Telecommunications Research Institute)
- Financial Security
  - FSA (Financial Security Agency)
- KISIA (Korea Information Security Industry Association)
- etc.

Week 2-2: Basic Terms

Lots of new terminologies in every new fields…

Security Requirements(1/2)

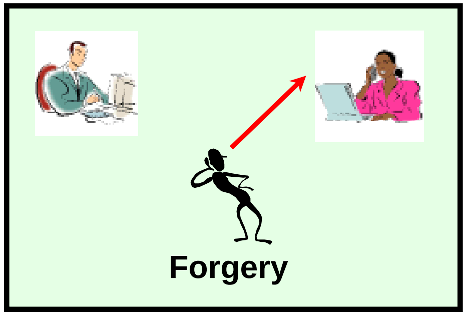
Confidentiality



Interception

Is Private?

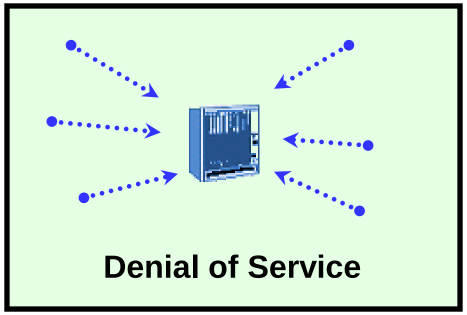
Authentication



Forgery

Who am I dealing with?

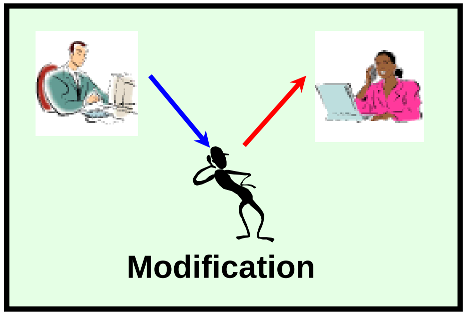
Availability



Denial of Service

Wish to access!!

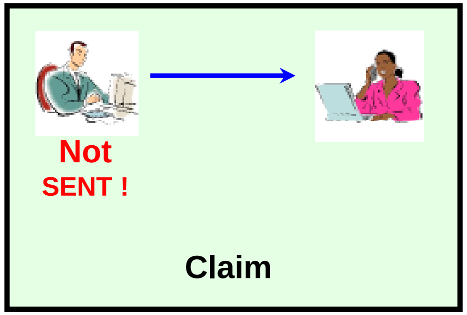
Integrity



Modification

Has been altered?

Non-Repudiation

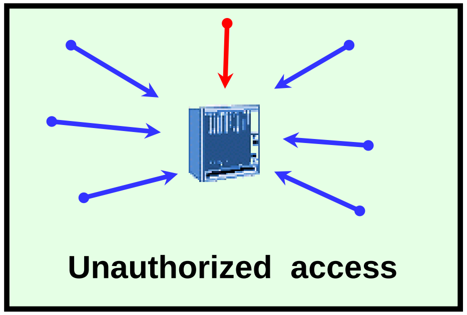


Not SENT !

Claim

Who sent/received it?

Access Control



Unauthorized access

Have you privilege?

Security Requirements (2/2)

- ❑ Security services
  - ➢ A service that enhances information security using one or more security mechanisms

- ❑ Confidentiality/Secrecy (기밀성) ↔ Interception
- ❑ Authentication (인증성) ↔ Forgery
- ❑ Integrity (무결성) ↔ Modification
- ❑ Non-repudiation (부인방지) ↔ Denial of facts

- ❑ Access control (접근제어) ↔ Unauthorized access
- ❑ Availability (가용성) ↔ Interruption

Cryptology = Cryptography + Cryptanalysis

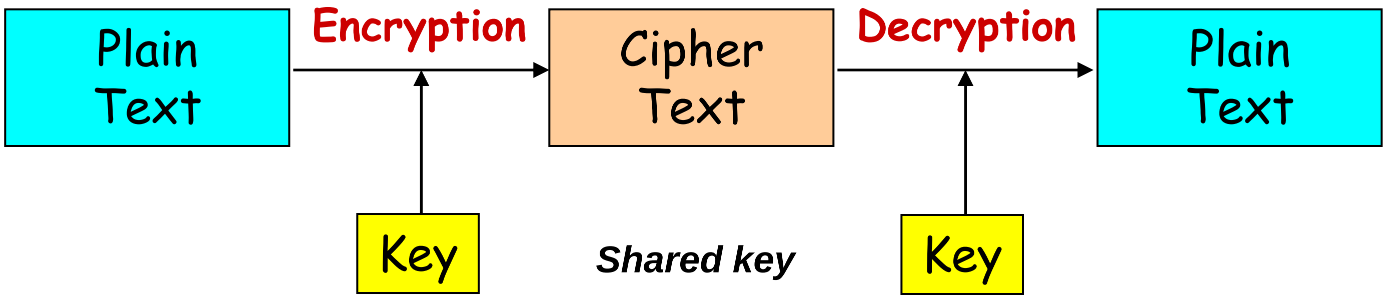
- Cryptography : designing secure cryptosystems
  - Cryptography (from the Greek kryptós and gráphein, “to write”) was originally the study of the principles and techniques by which information could be concealed in ciphers and later revealed by legitimate users employing the secret key.

- Cryptanalysis : 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.

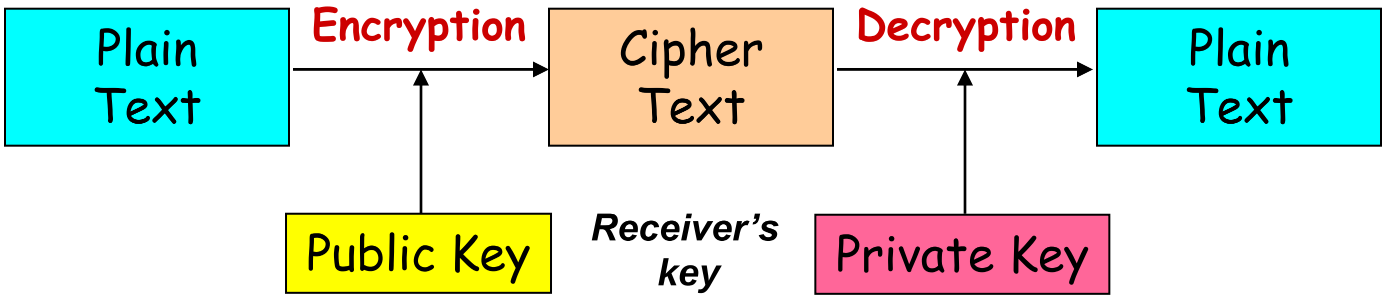
- Cryptology : science dealing with information security
  - Science concerned with data communication and storage in secure and usually secret form. It encompasses both cryptography and cryptanalysis.
  - Basic tools for information security

Secret Key vs. Public Key Systems

- Symmetric Key Cryptosystem



- Public Key Cryptosystem



Common Terms (1)

- ❑ Cryptography(암호설계): The study of mathematical techniques related to aspects of information security
- ❑ Cryptanalysis(암호분석): The study of mathematical techniques for attempting to defeat cryptographic techniques
- ❑ Cryptology(암호학): The study of cryptography and cryptanalysis
- ❑ Cryptosystem(암호시스템): A general term referring to a set of cryptographic primitives used to provide information security
  - ➢ Symmetric key primitives; Public key primitives
- ❑ Steganography: The method of concealing the existence of message

❖ Cryptography is not the only means of providing information security, but rather one set of such techniques (physical / human security)

Common Terms (2)

- ❑ 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)

Attacks

- ❑ Attacks
  - ➢ An efficient algorithm that, for a *given* cryptographic design, enables some protected elements of the design to be computed "substantially" quicker than specified by the designer.
  - ➢ Finding overlooked and realistic threats for which the design fails
- ❑ Attacks on encryption algorithms
  - ➢ Exhaustive search (brute force attack) : Theoretical possible to any algorithm
  - ➢ Ciphertext-only attack : c^n -> k
  - ➢ Known-plaintext attack : $(kp, c)^n$ -> k
  - ➢ Chosen-plaintext attack : *given* E(), $(cp, c)^n$ -> k
  - ➢ Chosen-ciphertext attack : *given* D(), $(cc, p)^n$ ->k

Models for Evaluating Security

- ❑ **Unconditional Security**

- ❑ **Computational Security**
  - ➢ **Limitation on Space (Memory) or Time**
  - ➢ **Time-Memory Tradeoff**
  - ➢ **Feasible (Practical) Security**

- ❑ **Provable Security**

  (e.g.) Under assumption *A*, prove that "*Breaking X is equiv. to solving of well-known difficult problem.*"

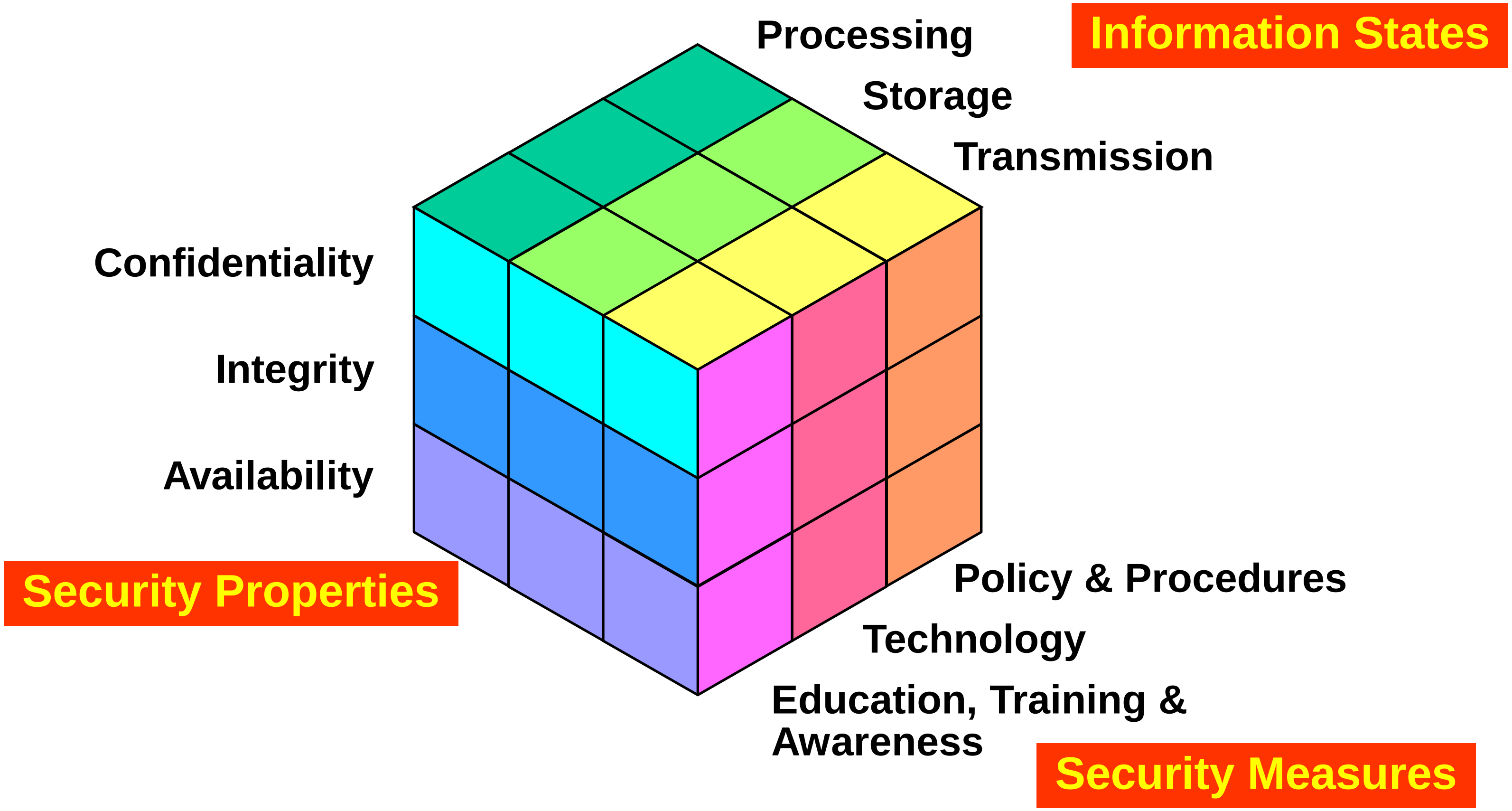
Information Security : C.I.A.

- 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

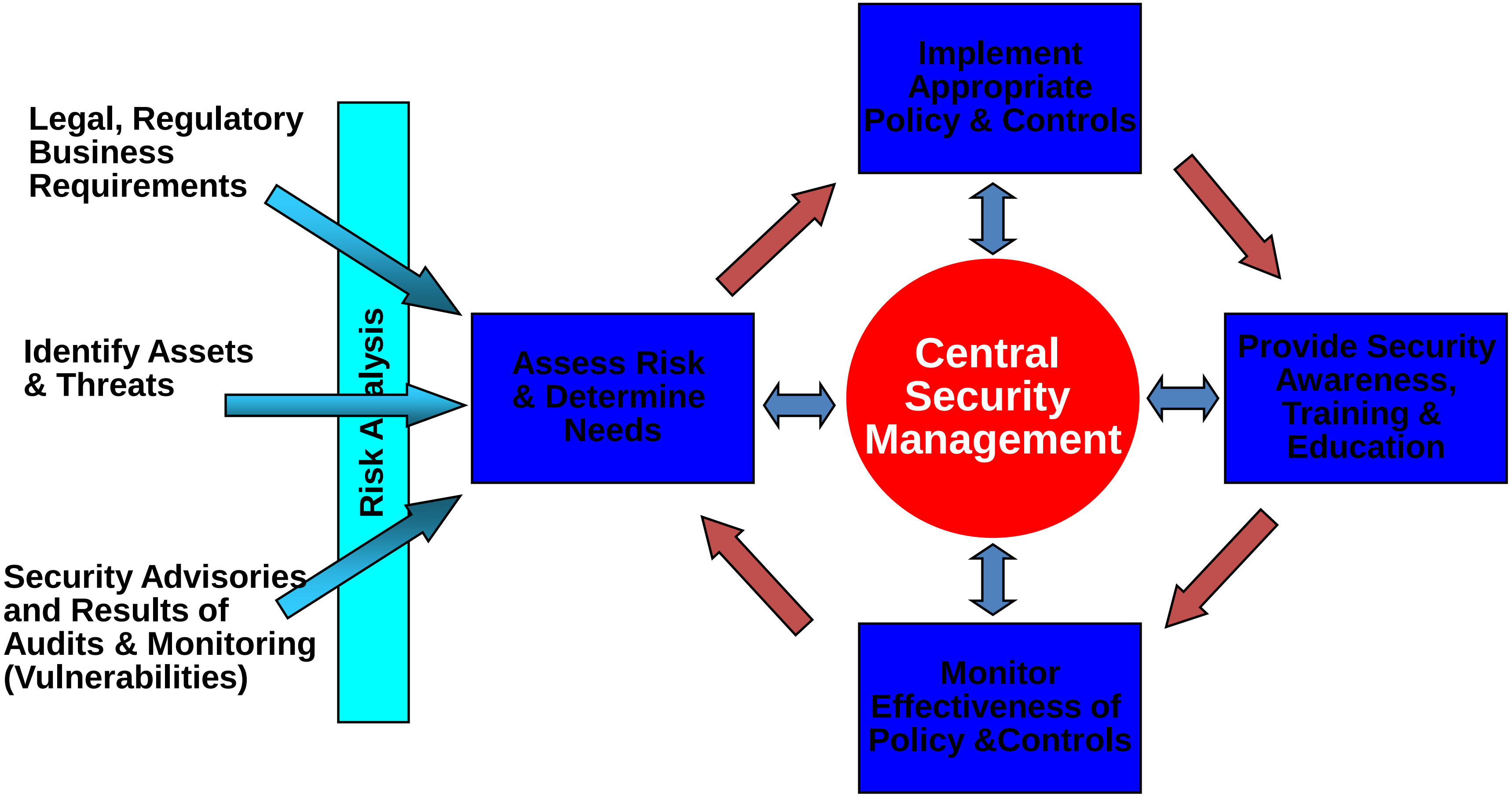
- How to Achieve Information Security
  - Policies : what should do, what should not do, etc., for information security
  - Technologies: implementing the policies
  - Operations: assessment & improvement on the implemented technologies

Field of Information Security



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

Managing Security



Legal, Regulatory
Business
Requirements

Identify Assets
& Threats

Security Advisories
and Results of
Audits & Monitoring
(Vulnerabilities)

Risk Analysis

Assess Risk
& Determine
Needs

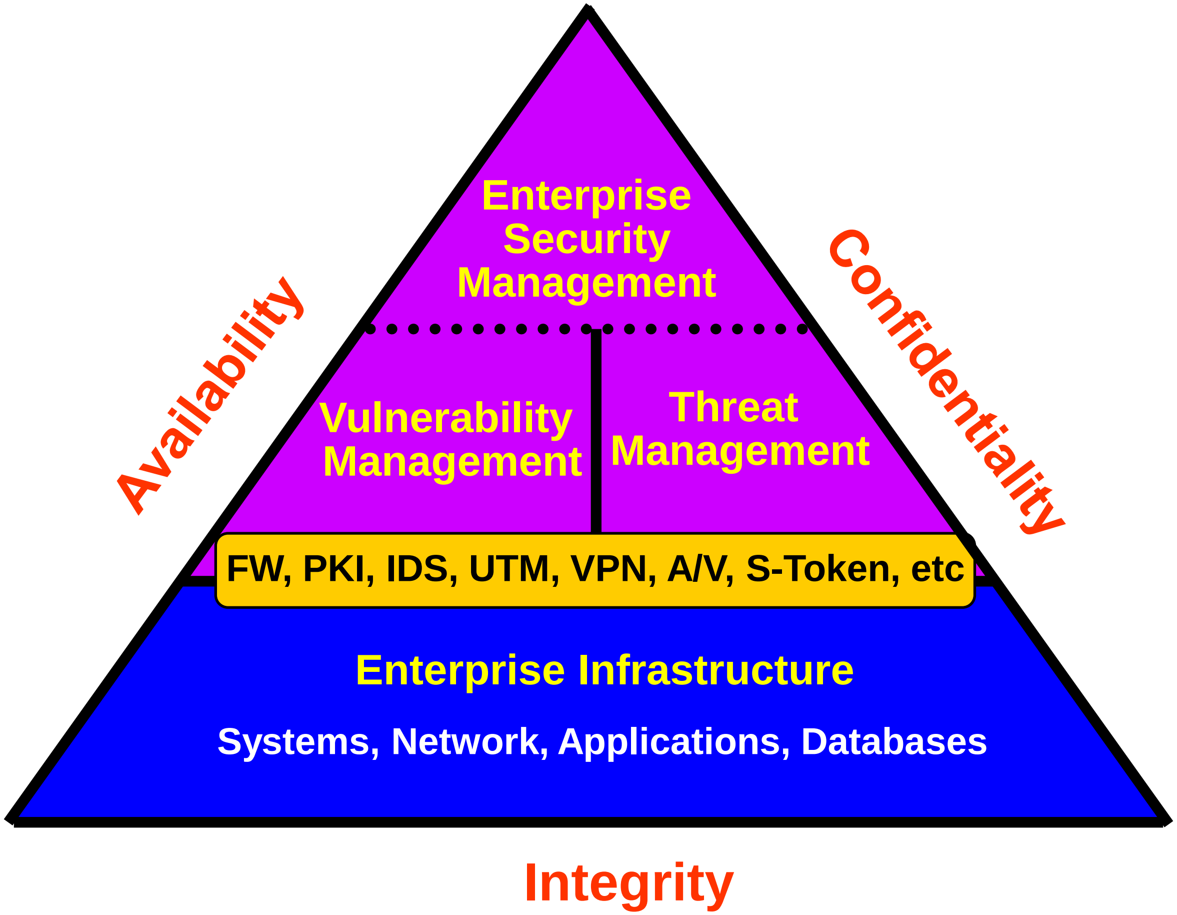
Implement
Appropriate
Policy & Controls

Central
Security
Management

Provide Security
Awareness,
Training &
Education

Monitor
Effectiveness of
Policy &Controls

Enterprise Security Management


Enterprise Security Management
Availability
Confidentiality
Vulnerability Management
Threat Management
FW, PKI, IDS, UTM, VPN, A/V, S-Token, etc
Enterprise Infrastructure
Systems, Network, Applications, Databases
Integrity