Course

- ❑ Title : Modern Cryptology (ICE605)
- ❑ Credit/Hour : 3/3
- ❑ Prof : Kwangjo Kim
- ❑ TA : Byongcheon Lee
- ❑ Hour : Tue. / Thu., PM 3:00 - 4:30
- ❑ Web page :

http://garden.icu.ac.kr/course/2001/spring/ice605

Syllabus

1. Course Description

With the adventment of information infrastructure, the side-effects such as illegal wiretapping, modification, or insersion, etc of information are rapidly increased.

This course focuses the student to be capable of designing the theoretical and practical countermeasures against such malicious acts for building secure information society.

2. Textbook

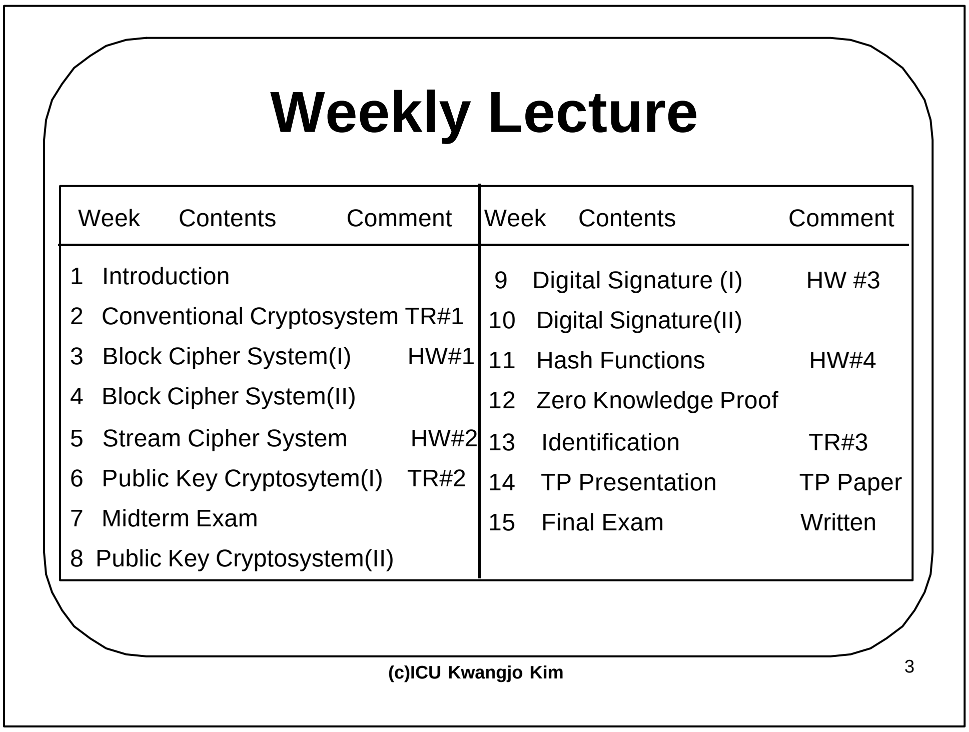
- Main Textbook : Douglas R. Stinson, *Cryptography-Theory and Practice*, CRC Press, 1995, pp.448, ISBN 0-8493-5821-0
- Recommended Reading Material :

Menezes et al, *Handbook of Applied Cryptography*, CRC Press, 1997, ISBN 0-8493-8523-7

Handouts, etc

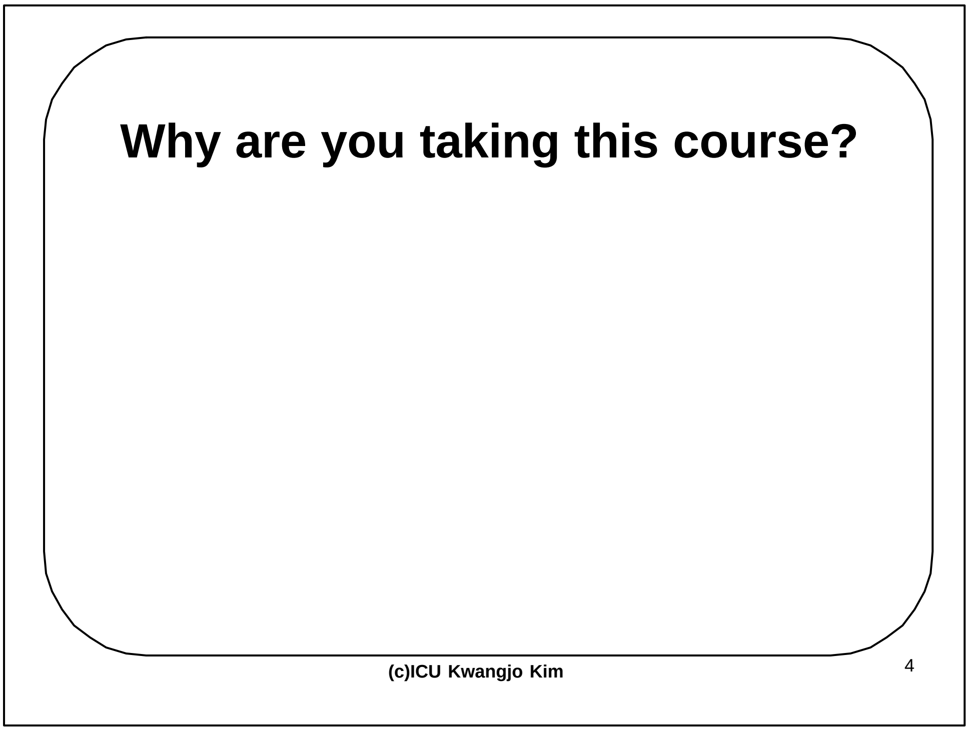
3. Test and Evaluation

- Midterm Exam: 15% - Quiz:5% - Final Exam:25% - Homework: 15% - Term Project : 15%
- Term Paper: 20% - Attendance : 5%



Weekly Lecture

Week	Contents	Comment	Week	Contents	Comment
1	Introduction		9	Digital Signature (I)	HW #3
2	Conventional Cryptosystem	TR#1	10	Digital Signature(II)	
3	Block Cipher System(I)	HW#1	11	Hash Functions	HW#4
4	Block Cipher System(II)		12	Zero Knowledge Proof	
5	Stream Cipher System	HW#2	13	Identification	TR#3
6	Public Key Cryptosytem(I)	TR#2	14	TP Presentation	TP Paper
7	Midterm Exam		15	Final Exam	Written
8	Public Key Cryptosystem(II)				



Why are you taking this course?

Term Projects

- ❑ Cryptographic application of your majoring field
- ❑ Designing of a Block Cipher
- ❑ Evaluation of AES (Rijndael)
- ❑ Design of a stream cipher for IMT2000
- ❑ Application of digital signature
- ❑ Cryptographic hash function
- ❑ Implementation of Fiat-Shamir Protocol in Java
- ❑ Design cryptographic protocol based on elliptic curve cryptosystem
- ❑ Implementation of RSA in a smart card
- ❑ etc

Prerequisite

- Mathematics
  - Number Theory
  - Group, Ring & Field Theory
  - Linear algebra
  - Elliptic curve
- Probability
- Information Theory / Coding Theory
- Computational Complexity
  - algorithm, Turing machine
  - NP-completeness
- Chaos Theory / Quantum Computing, etc

Background

- ❑ Information Society as promulgation of Computer & Network
- ❑ Information Security is becoming a core technique for building E-commerce system from traditional domestic and military applications
- ❑ Defense for Illegal hacking (cracking) for building NII, DII and GII
- ❑ Self-defense cryptology and Information Security Techniques not depending on advanced countries
- ❑ Civilian forces to self-guard (‘ 99.1)

N(D, G) II : National (Defence, Global) Information Infrastructure

EC (Electronic Commerce)

Who are interested in cryptology ?

- Government/Diplomatic
- Military
- Academic
- Standard
- Politician
- Police
- Financial
- Porno Vendor

- Industrial
- Criminal
- Business/Electronic Commerce
- Common Carrier
- Nuclear Control
- Copyright Protection
- Digital Watermark
- Visual Cryptography
- Secret Sharing

Academic Research

- **USA**
  - IACR (International Association for Cryptologic Research)
    : Crypto(‘ 81-) http://www.iacr.org/
  - IEEE(Symposium on Privacy and Security)
  - ACM(Foundation Of Computer Science)
- **Europe**
  - Eurocrypt(‘ 82-)
  - ESORICS(European Symposium on Research in Computer Security)
- **Asia**
  - Asiacrypt(‘ 91-) / Auscrypt(‘ 90-), ICICS(‘ 97-)
  - IEICE‘ s ISEC Group (‘ 84-) : SCIS(‘ 84-)/PKC(‘ 98-)
  - KIISC (Korea Institute of Information Security and Cryptology)
    (‘ 89-) http://www.kiisc.or.kr/

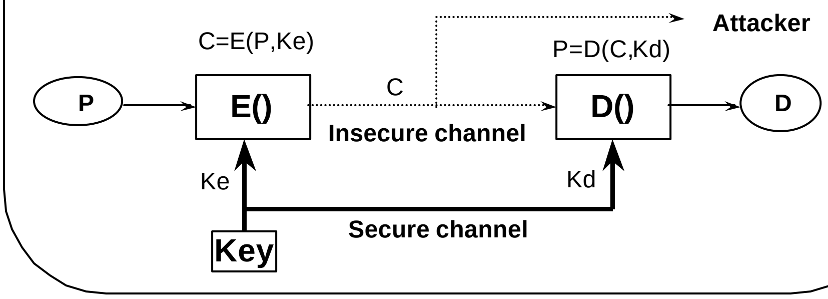
Basic Concepts(I)

❑ **Cryptology**

= Crypto(Hidden) + Logos (word)

= Cryptography + Cryptanalysis
= Code Writing + Code Breaking

❑ **Encryption(Decryption),Key,Plaintext,Ciphertext, Deciphertext**



Basic Concept(II)

- ❑ 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

Basic Concepts(III)

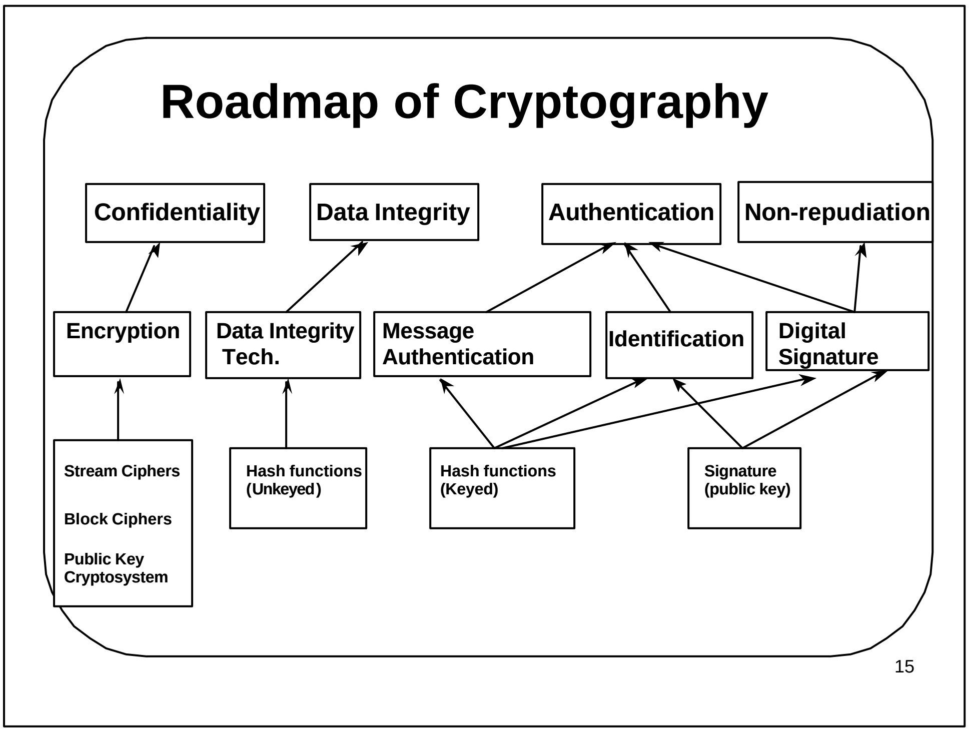
- ❑ Classification of cryptoalgorithms
  - – by date
    - ✓ Traditional(~19C) : Ceaser
    - ✓ Mechanical(WW I, II) : Rotor Machine, Purple
    - ✓ Modern(‘ 50~) : DES, IDEA, AES
  - – by number of keys
    - ✓ Conventional : {1,single,common} key, symmetric
    - ✓ Public key cryptosystem : {2,dual}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

Information Security Objectives (I)

- *Privacy (or 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*
- *Signature : a means to bind information to an entity*
- *Access control* **: restricting access to resources to privileged entities.**
- *Non-repudiation :* **Preventing the denial of previous commitment or actions.**

Information Security Objectives(II)

- **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**
- **Timestamping : 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**



Roadmap of Cryptography

Confidentiality

Data Integrity

Authentication

Non-repudiation

Encryption

Data Integrity Tech.

Message Authentication

Identification

Digital Signature

Stream Ciphers

Block Ciphers

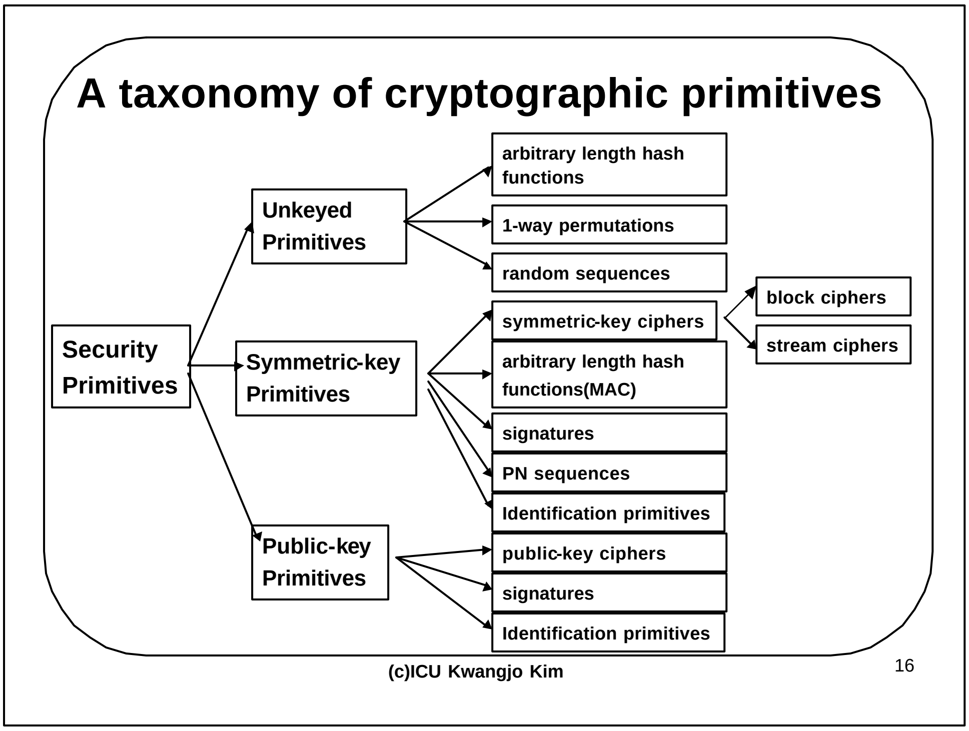
Public Key Cryptosystem

Hash functions (Unkeyed)

Hash functions (Keyed)

Signature (public key)

15



A taxonomy of cryptographic primitives

Security Primitives

Unkeyed Primitives

- arbitrary length hash functions
- 1-way permutations
- random sequences

Symmetric-key Primitives

- symmetric-key ciphers
  - block ciphers
  - stream ciphers
- arbitrary length hash functions(MAC)
- signatures
- PN sequences
- Identification primitives

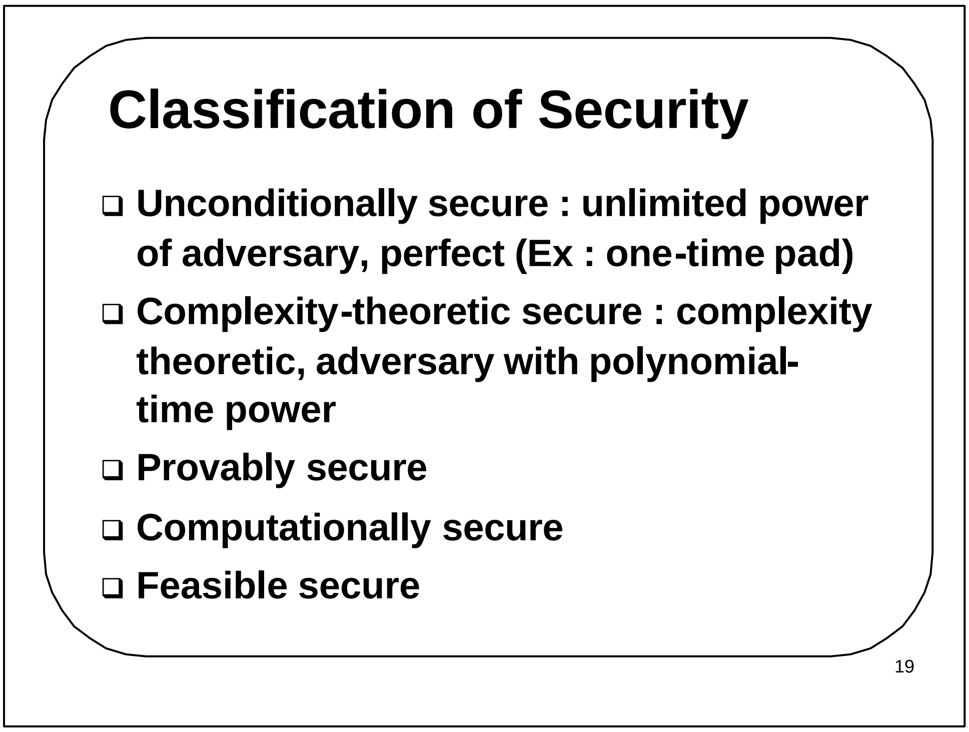
Public-key Primitives

- public-key ciphers
- signatures
- Identification primitives

(c)ICU Kwangjo Kim

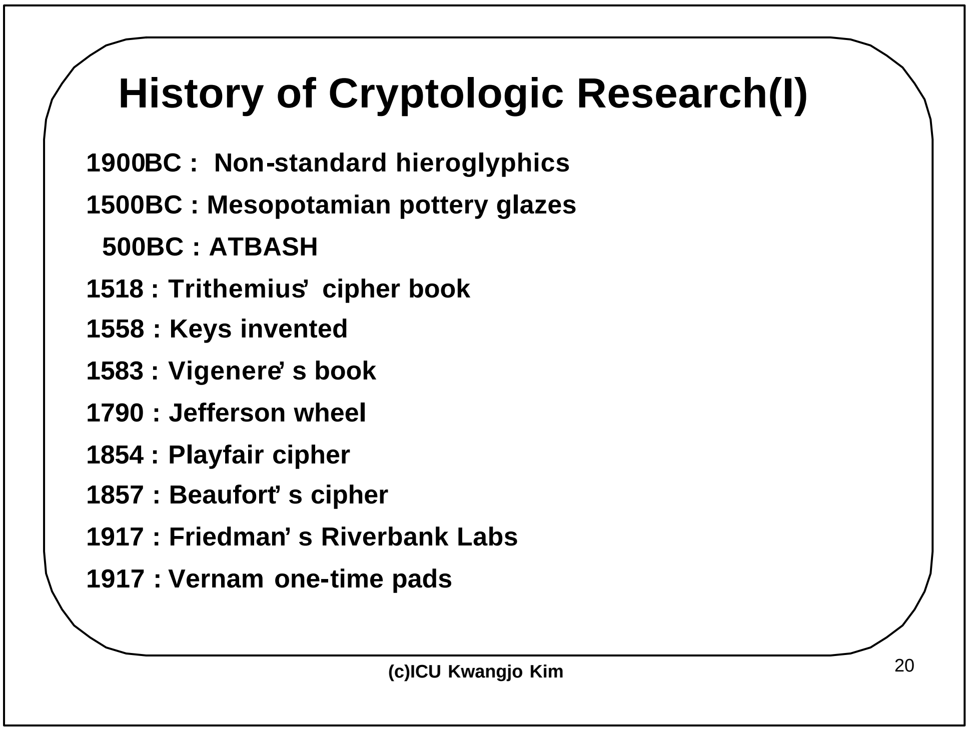
16

17



Classification of Security

- ❑ Unconditionally secure : unlimited power of adversary, perfect (Ex : one-time pad)
- ❑ Complexity-theoretic secure : complexity theoretic, adversary with polynomial-time power
- ❑ Provably secure
- ❑ Computationally secure
- ❑ Feasible secure



History of Cryptologic Research(I)

1900BC : Non-standard hieroglyphics

1500BC : Mesopotamian pottery glazes

500BC : ATBASH

1518 : Trithemius' cipher book

1558 : Keys invented

1583 : Vigenere' s book

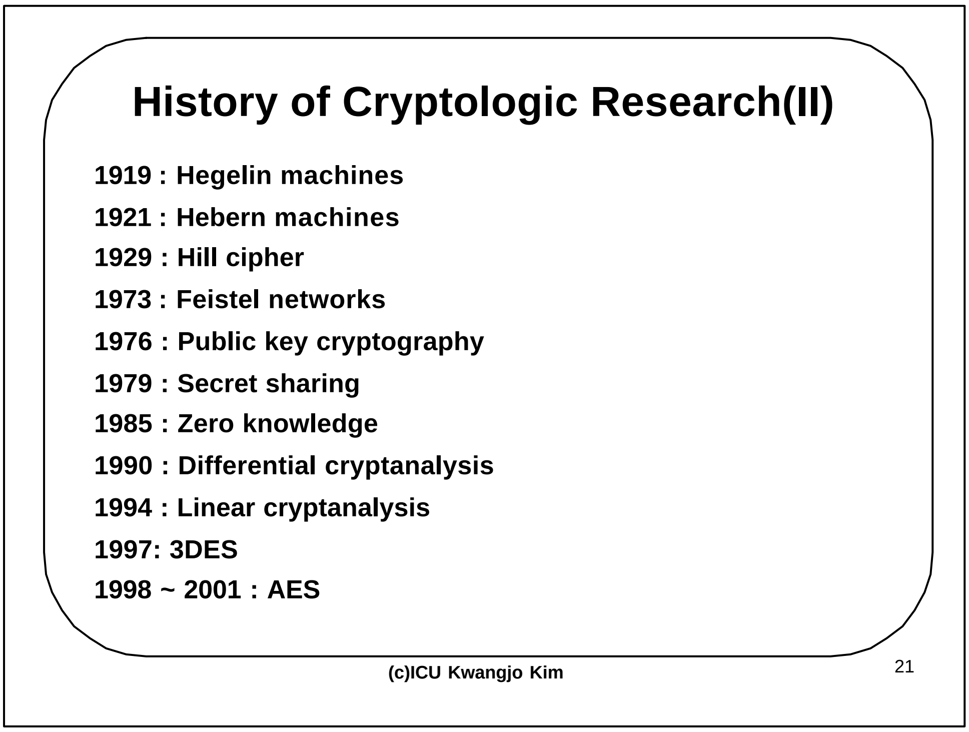
1790 : Jefferson wheel

1854 : Playfair cipher

1857 : Beaufort' s cipher

1917 : Friedman' s Riverbank Labs

1917 : Vernam one-time pads



History of Cryptologic Research(II)

1919 : Hegelin machines

1921 : Hebern machines

1929 : Hill cipher

1973 : Feistel networks

1976 : Public key cryptography

1979 : Secret sharing

1985 : Zero knowledge

1990 : Differential cryptanalysis

1994 : Linear cryptanalysis

1997: 3DES

1998 ~ 2001 : AES