暨南大學
JINAN UNIVERSITY

Lecture 1: Introduction

-Cryptographic Algorithms and Protocols

Huang, Xiujie (黄秀姐)

Office: Nanhai Building, #411

E-mail: t_xiujie@jnu.edu.cn

Dept. Computer Science

02/24/2022

Outline

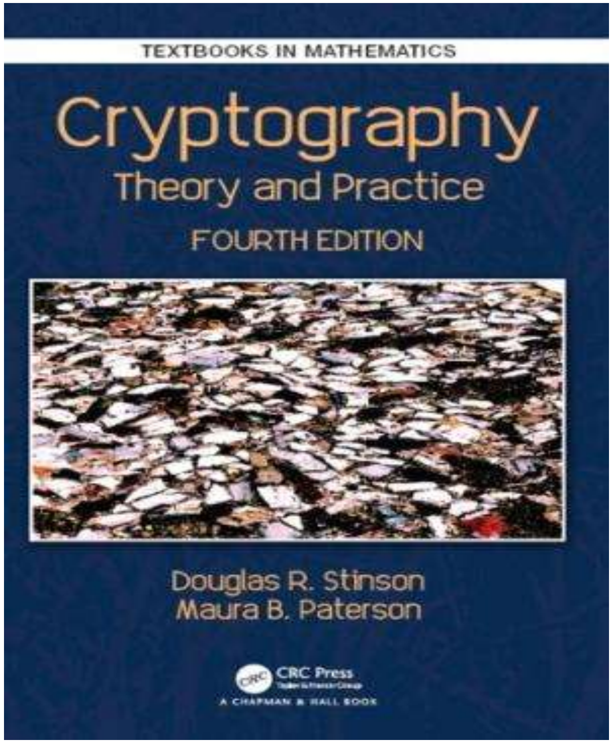
- **1. Course Information**
- **2. Evolution of the Cryptography**
- **3. Intuitions on Cryptographic Algorithms and Protocols**

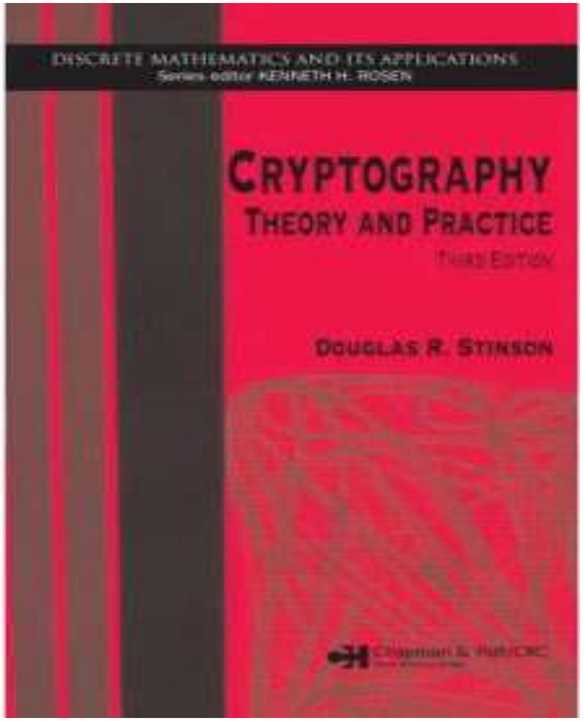
1.1 Books

- **Textbooks:**
  - *Cryptography: Theory and Practice* **(4th ed.)**

    Douglas R. Stinson and Maura B. Paterson

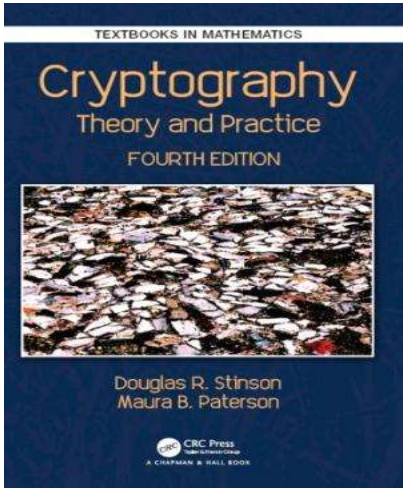
    2018, CRC Press





1.2 Main Contents & Calendar

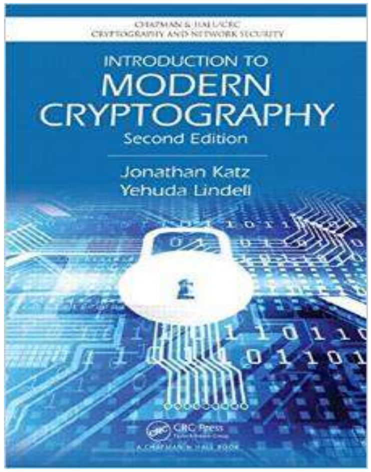
- **1. Introduction: week 1**
- **2. Classical Cryptography: week 2**
- **3. Shannon’s Theory: week 3**
- **4. Block Ciphers: weeks 4-5**
- **5. Hash Functions: weeks 6-8**
- **6. The RSA Cryptosystem: weeks 9-10**
- **7. The ElGamal-like Cryptosystems: weeks 11-12**
- **8. Signature Schemes: weeks 13-14**
- **9. Applications and New Directions: weeks 15-16**

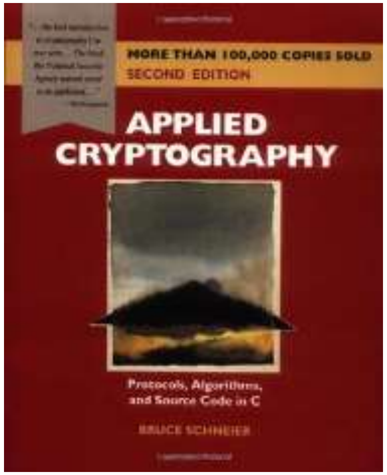


1.3 References

- **<u>Prerequisites:</u>**
  - **Probability, Number Theory, Linear Algebra, Abstract Algebra**
- **References:**

- “Introduction to Modern Cryptography”, 2nd ed., by J. Katz and Y. Lindell, 2014, CRC Press.
- “Applied Cryptography”, 2nd ed., by B. Schneier, 1995, Wiley Press




MORE THAN 100,000 COPIES SOLD
SECOND EDITION
APPLIED
CRYPTOGRAPHY
Protocols, Algorithms, and Source Code in C
BRUCE SCHNEIER

1.4 Teaching Goals

- **Understand how basic cryptographic algorithms and protocols work**
  - **Basic concepts, basic principles, key terms**
  - **Classic Schemes and Designs**
  - **Common designs and security discussions**
- **Be able to use algorithms and protocols correctly and analyze their security**
  - **Can analyze the security of cryptographic constructions**
  - **Can break insecure constructions**

1.5 Evaluation Rules

- **Grading:**
  - **Attendance and Class behaviors: 20% (3 Absences = 0 !!!)**
  - **Homeworks and Quiz: 20%**
  - **Final exam: 60% (closed book)**

- **Office hours:**
  - **at 10am-11am on every Thursday in N124**
  - **Please make an appointment by Email (t_xiujie@jnu.edu.cn) or QQ in advance**

Outline

- **1. Course Information**

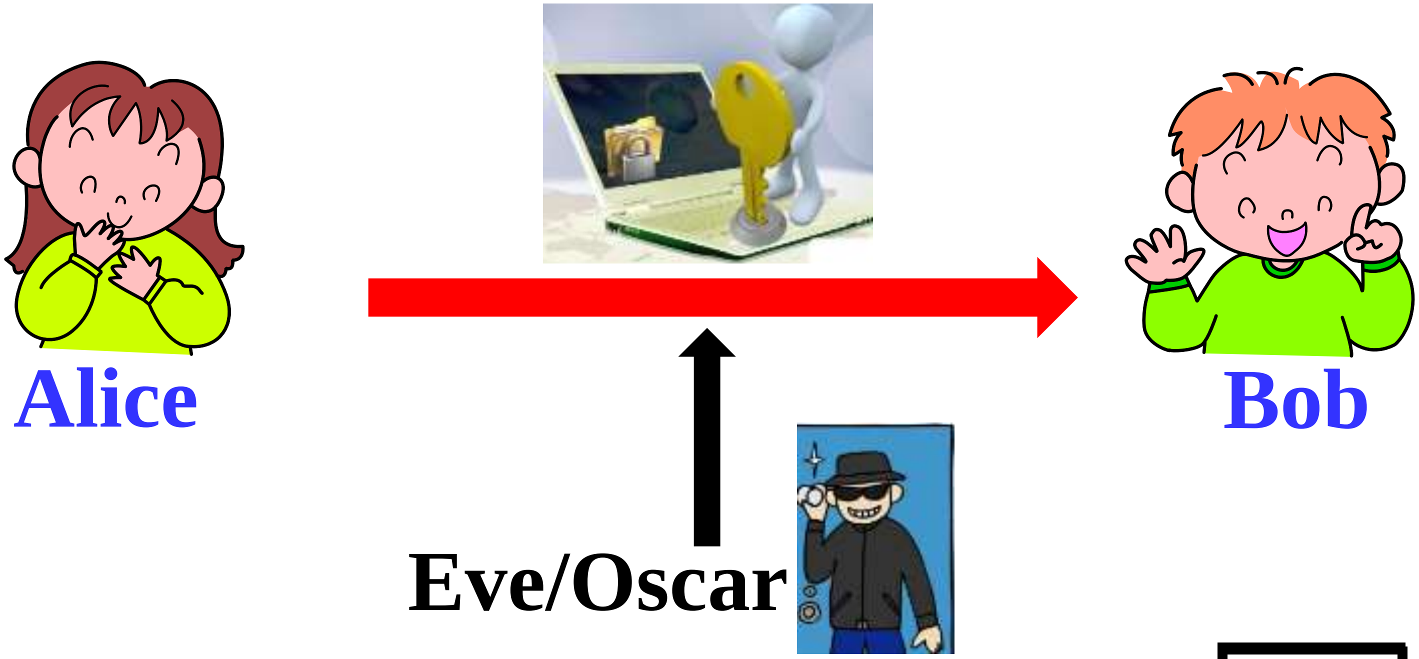
- **2. Evolution of the Cryptography**

- **3. Intuitions on Cryptographic Algorithms and Protocols**

Password is not Cryptography

Cryptography can do much more！

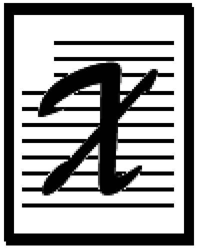
Goals of Cryptography



Alice

Bob

Eve/Oscar

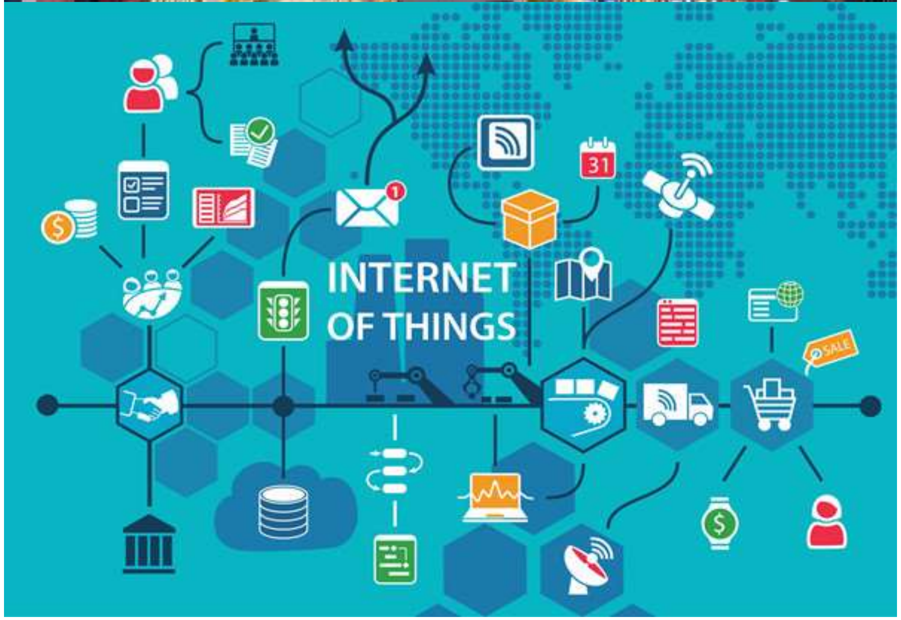


ciphertext

- Goal 1: Protect Good from Bad
- Solution: Make message Meaningless
- Goal 2: Be able to Distinguish between Good and Bad
- Solution: Identification

Cryptography is everywhere

- **Secure communications**
  - web traffics: HTTPS
  - wireless traffics: 802.11i WPA2,



- **Encrypting files on disk:**

  EFS, TrueCrypt

- **Content protection:**

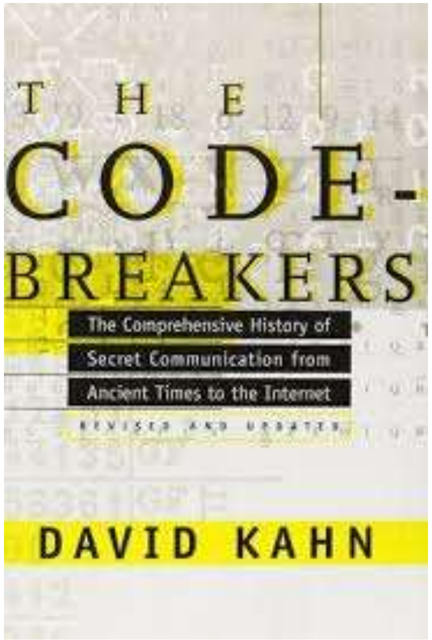
  CSS (DVD), AACS (Blu-ray disk)

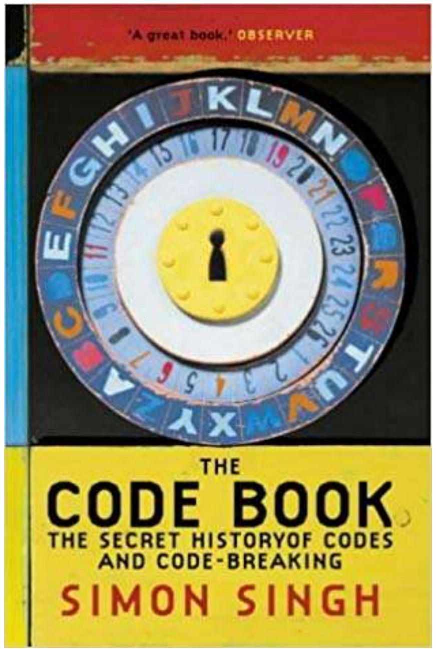
- **User authentication**

  ……

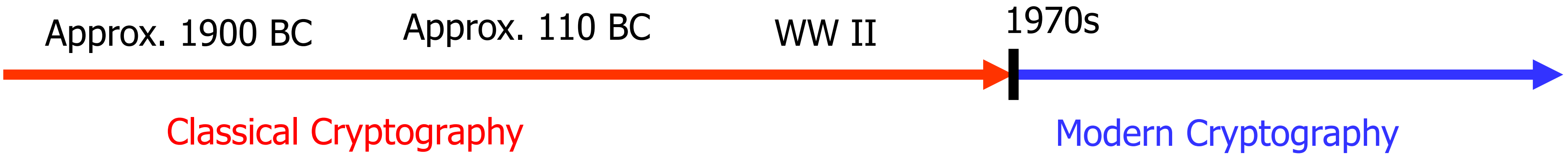
History

- David Kahn, “The Code Breakers” (1996)
- Simon Singh, “The Code Book” (1999)


THE
CODE-
BREAKERS
The Comprehensive History of
Secret Communication from
Ancient Times to the Internet
REVISED AND UPDATED
DAVID KAHN

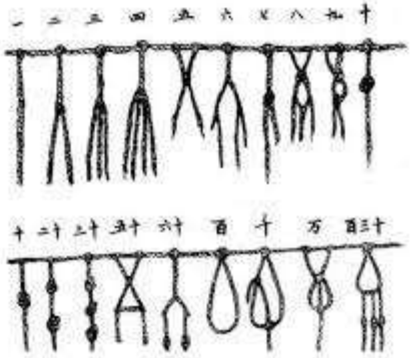


Evolution of the Cryptography



Applications

Secure Communications


一 二 三 四 五 六 七 八 九 十
十 二十 三十 五十 六十 百 千 万 百三十

Art

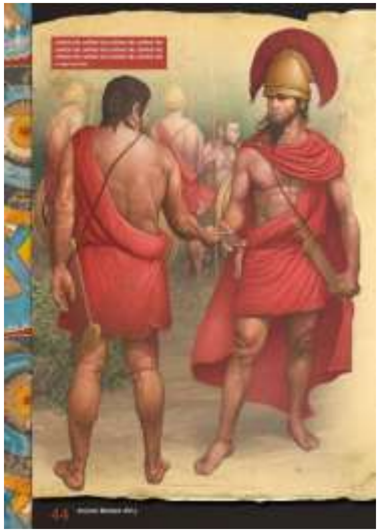
Secure Communications
E-cash
Secure Information Retrieval
E-election, E-auction
Secure Storage, Secret Sharing, Broadcast
Secure outsourcing to Cloud
Secure Computations
……

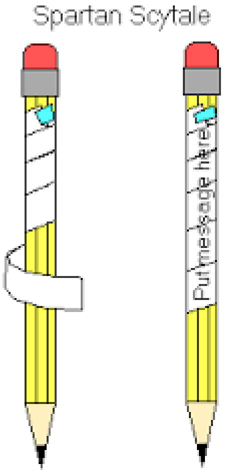
Science

Classical Cryptography

2.1 Scytale cipher

- **Around 400 B.C. used in Spartan military**





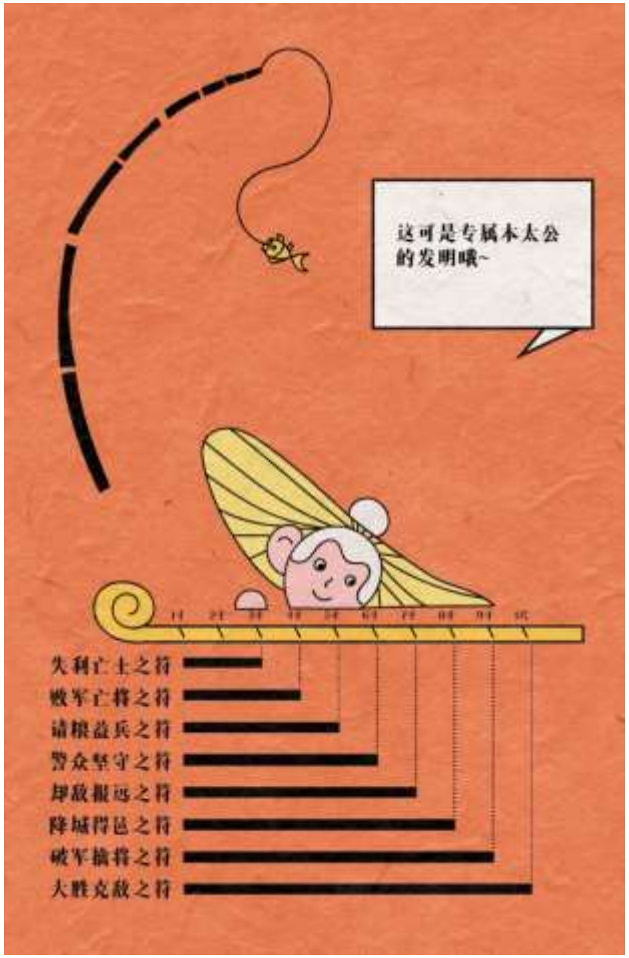
IEUARNMIIANVTJEEIRANSCAIHNTY

IAMATEACHERINJINANUNIVERSITY

2.2 One Ancient Cryptography in China – 阴符密码

- **Around 1100 B.C.**
- **invented by Jiang Taigong in the time of King Wu of Zhou (周武王)**
- **阴符:**
  - **大胜克敌符，长一尺；破军擒将符，长九寸；**
  - **降城得邑符，长八寸；却敌报远符，长七寸；**
  - **警众坚守符，长六寸；请粮益兵符，长五寸；**
  - **败军亡将符，长四寸；失利亡士符，长三寸。**

  (a substitution cipher)

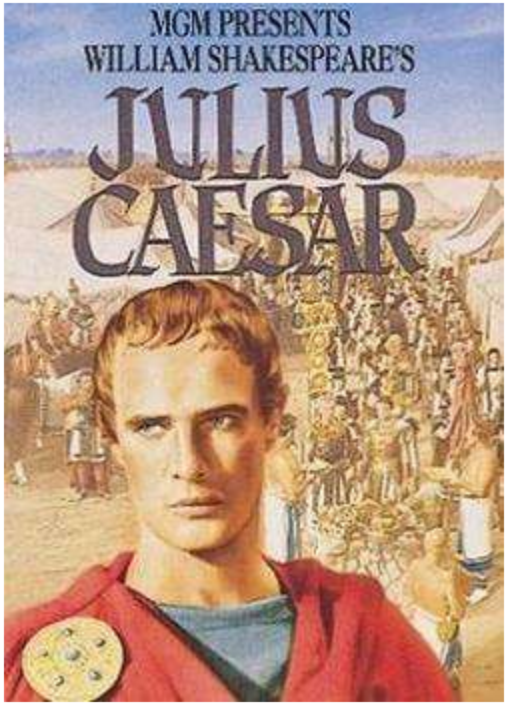


- **阴书：“一合而再离，三发而一知”**

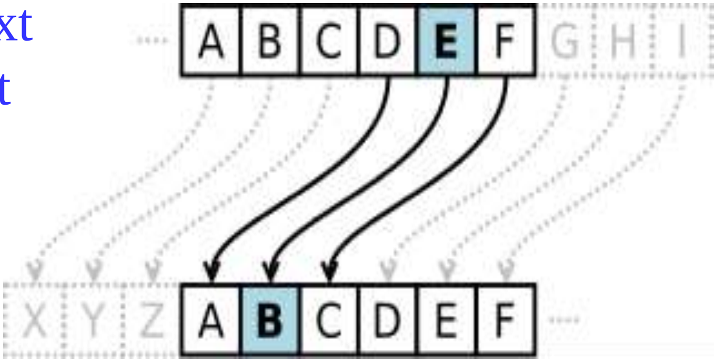
  (a permutation cipher)

2.3 Caesar Cipher

- **around 50 B.C.**
- **named after Julius Caesar**



Ciphertext alphabet



Plaintext alphabet

WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

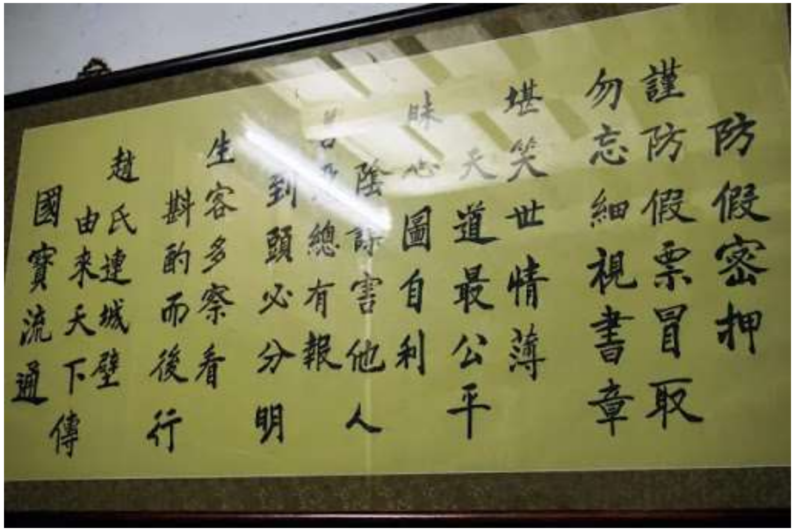
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

2.4 Jin merchants' Cryptography

- **Used in Money Orders**
- **During Ming and Qing Dynasties**

2.4 Jin merchants' Cryptography

- **Used in Money Orders**
- **During Ming and Qing Dynasties**



防假密押

謹防假票冒取

勿忘細視書章

堪笑世情薄

天道最公平

昧心圖自利

陰謀害他人

善惡終有報

到頭必分明

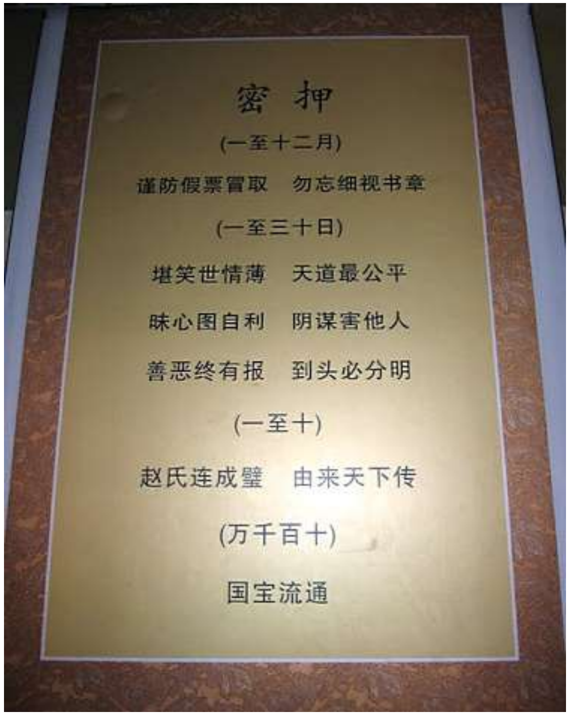
生客多察看

斟酌而後行

趙氏連城璧

由來天下傳

國寶流通



密 押

(一至十二月)

谨防假票冒取　勿忘细视书章

(一至三十日)

堪笑世情薄　天道最公平

昧心图自利　阴谋害他人

善恶终有报　到头必分明

(一至十)

赵氏连成璧　由来天下传

(万千百十)

国宝流通

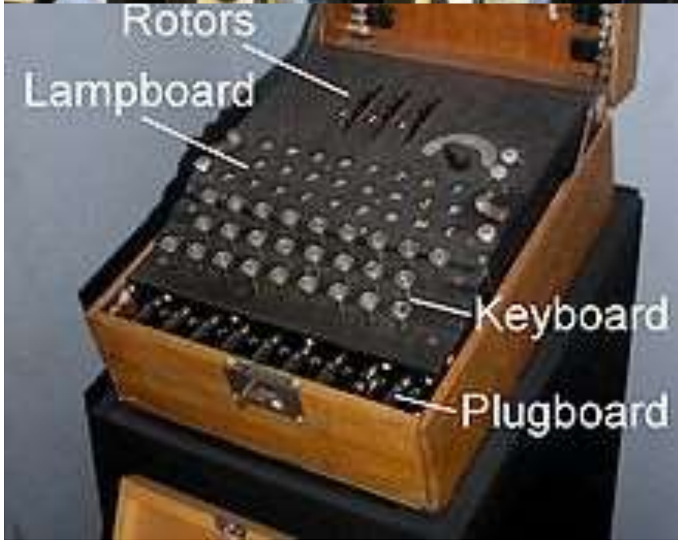
1	2	3	4	5	6	7	8	9	0
赵	氏	连	城	璧	由	来	天	下	传

万	千	百	两
国	宝	通	流

三百两　　连通流

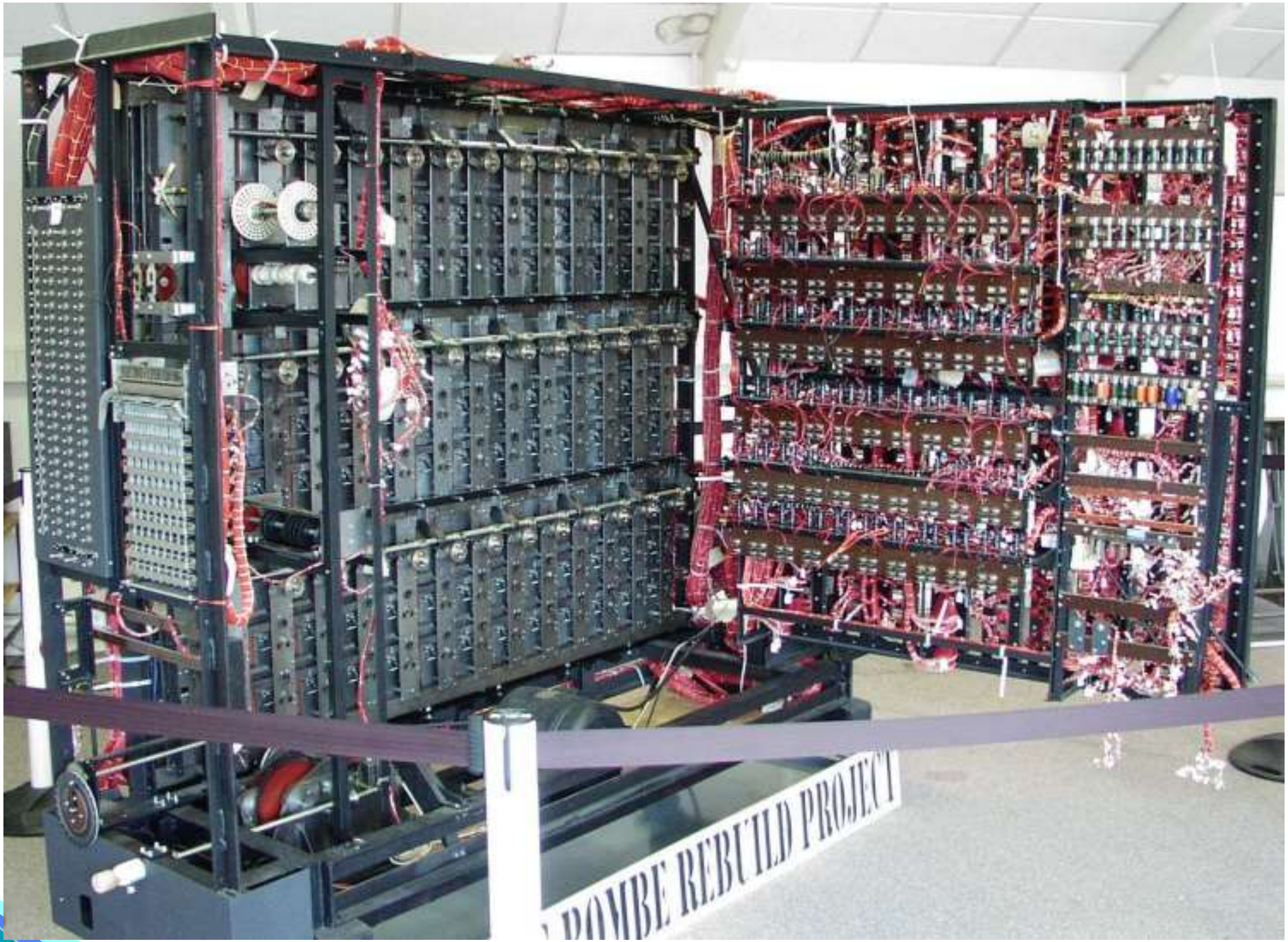
2.5 Enigma Machine (Mechanical Cryptography)

- **Invented by the German engineer Arthur Scherbius in 1918**
- **Used** by the German military **before and during World War II**



- **Cryptanalysis of Enigma**
  - **The Bombe designed by Alan Turing**

Bombe



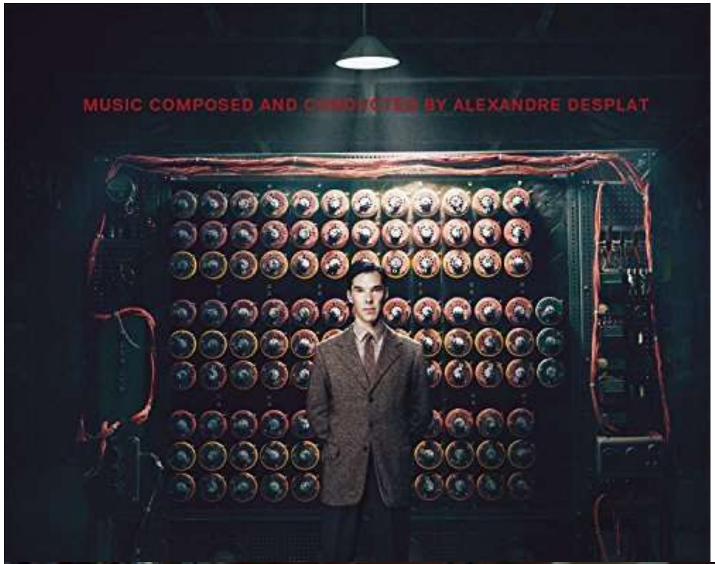
Alan Turing （1912-1954）

- one of its “100 Most Important People of the 20th century” by *Time* magazine (1999)
- Designs of Turing Machine & Turing Test
- A founding father of artificial intelligence and of modern cognitive science

Turing Award (since 1966)

“Nobel Prize” in Computer Science

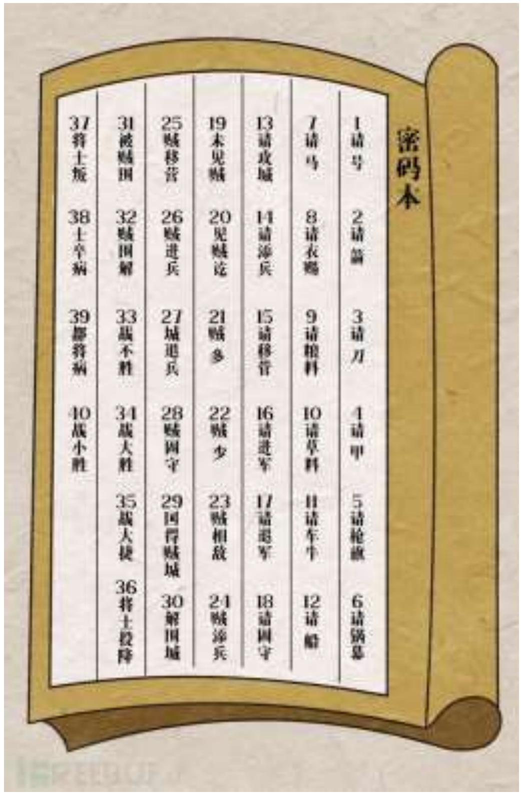
A related film – The Imitation Game



送杜少府之任蜀州

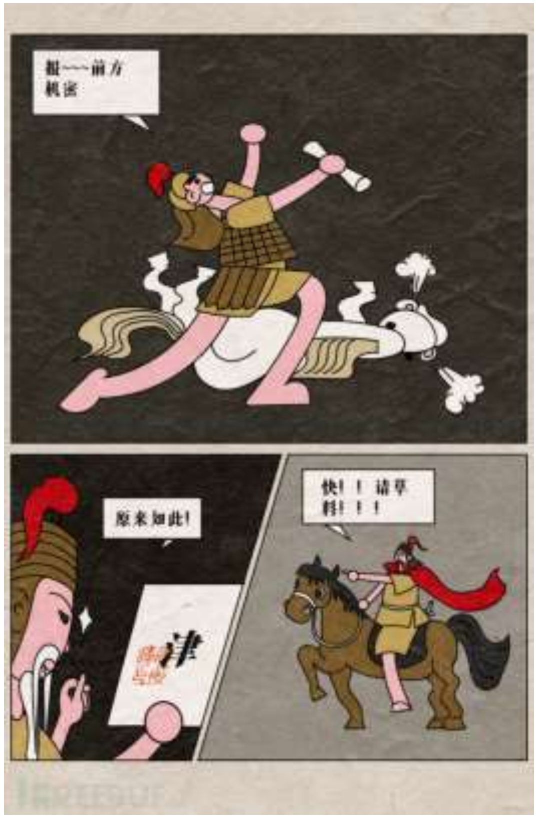
唐/王勃

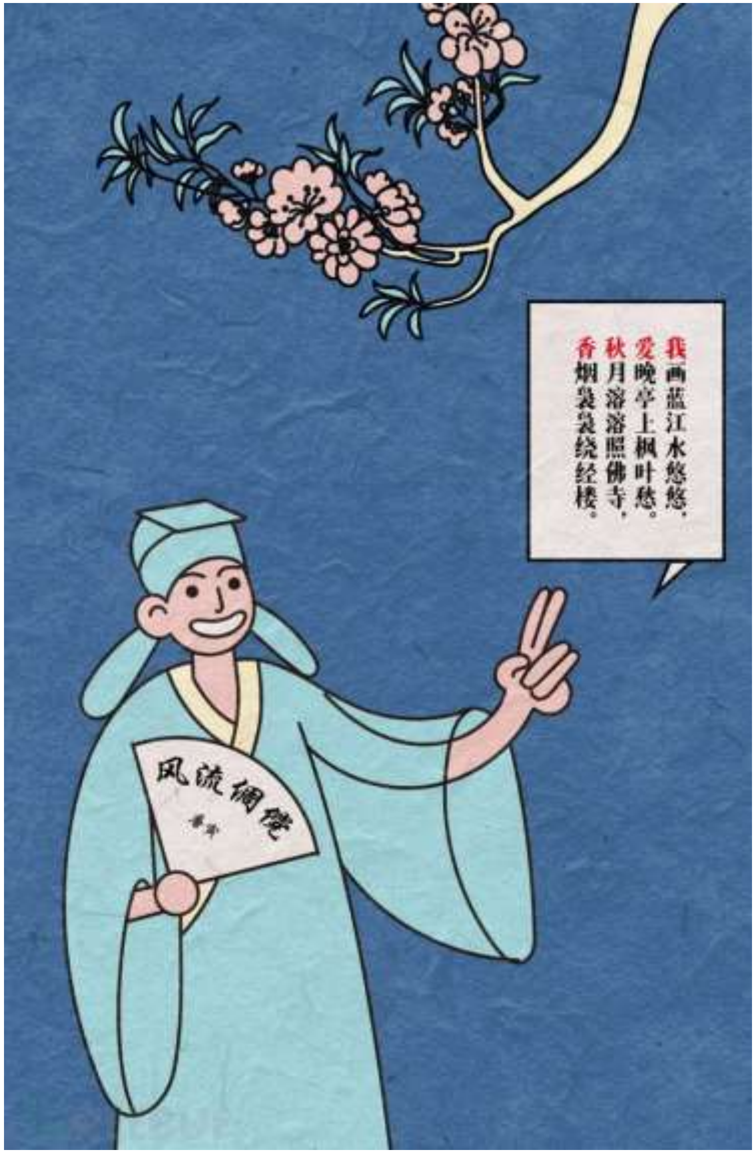
城阙辅三秦，风烟望五津。
与君离别意，同是宦游人。
海内存知己，天涯若比邻。
无为在歧路，儿女共沾巾。



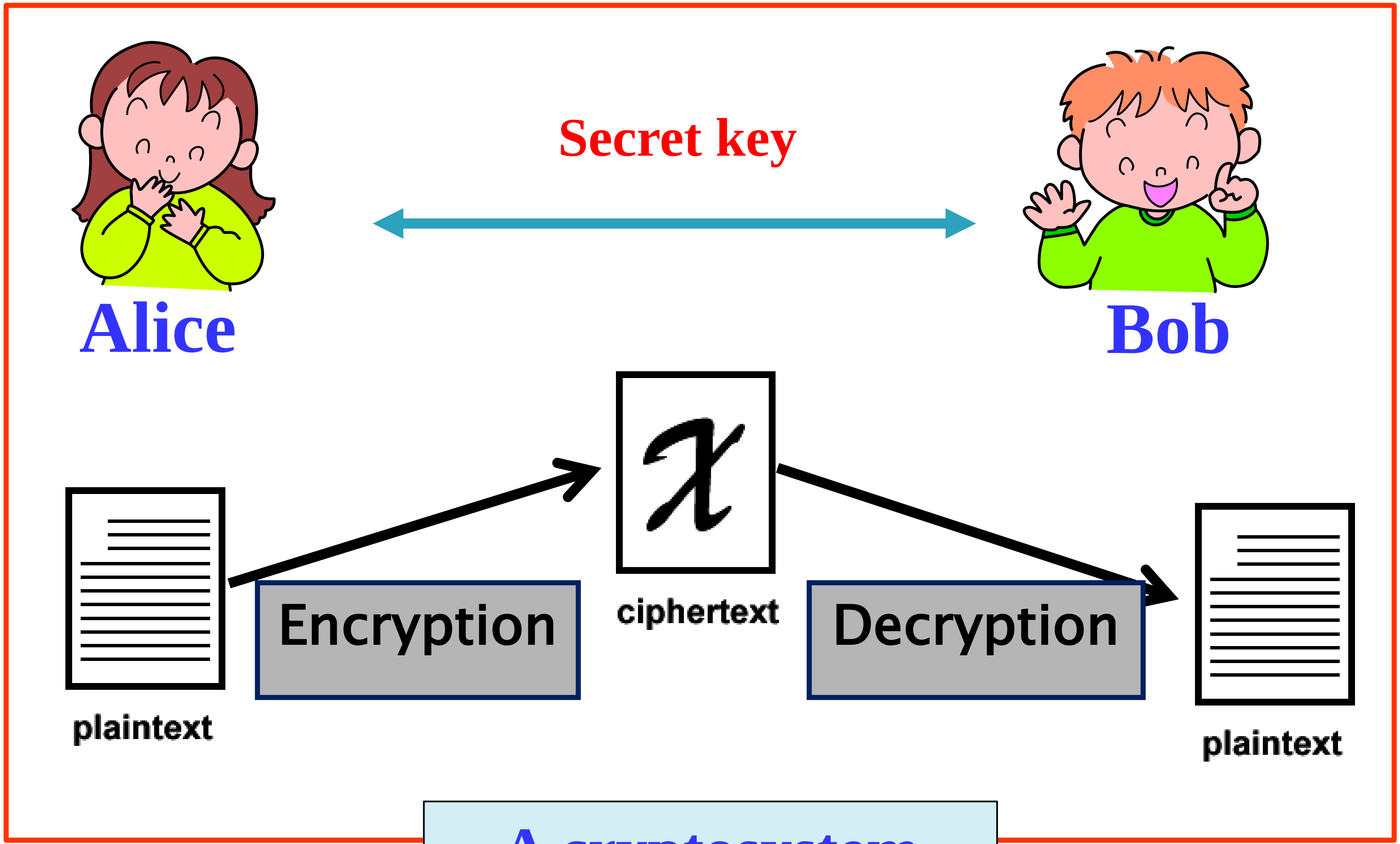
密码本

1请弓	2请箭	3请刀	4请甲	5请枪旗	6请锅幕
7请马	8请衣赐	9请粮料	10请草料	11请车牛	12请船
13请攻城	14请添兵	15请移营	16请进军	17请退军	18请固守
19未见贼	20见贼讫	21贼多	22贼少	23贼相敌	24贼添兵
25贼移营	26贼进兵	27贼退兵	28贼固守	29围得贼城	30解围城
31被贼围	32贼围解	33战不胜	34战大胜	35战大捷	36将士投降
37将士叛	38士卒病	39都将病	40战小胜		




我画蓝江水悠悠，
爱晚亭上枫叶愁。
秋月溶溶照佛寺，
香烟袅袅绕经楼。
风流倜傥

Basics of the Cryptography



A cryptosystem

Our Study

- **Classical Cryptography**
  - **Substitution Ciphers & Permutation Ciphers**

    ……

- **Modern Cryptography**
  - **Block Ciphers**
  - **Public-Key Cryptography**

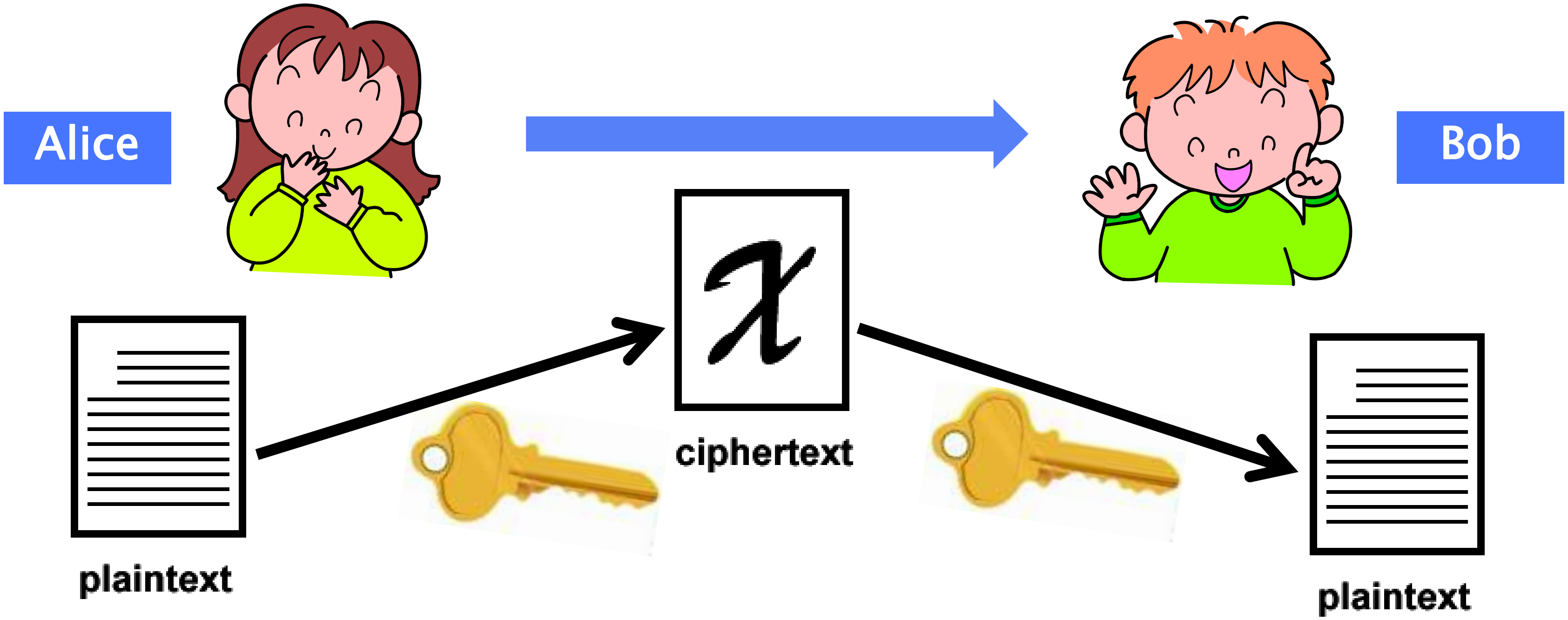
    ……

Modern Cryptography

- **Symmetric-Key Cryptosystem (SKC):**
  - **Block Ciphers: DES, AES**
  - **Steam Ciphers**
  - **Hash Functions and MACs**
  - **…**
- **Public-Key Cryptography (PKC):**
  - **RSA**
  - **ElGamal**
  - **Signature Schemes**
  - **…**

1) Symmetric-Key Cryptosystem

SKC



- **Long history:** Scytale Cipher, Caesar Cipher, 阴符密码, 晋商汇票, …
- **Security and Cryptanalysis**
- **Drawback**

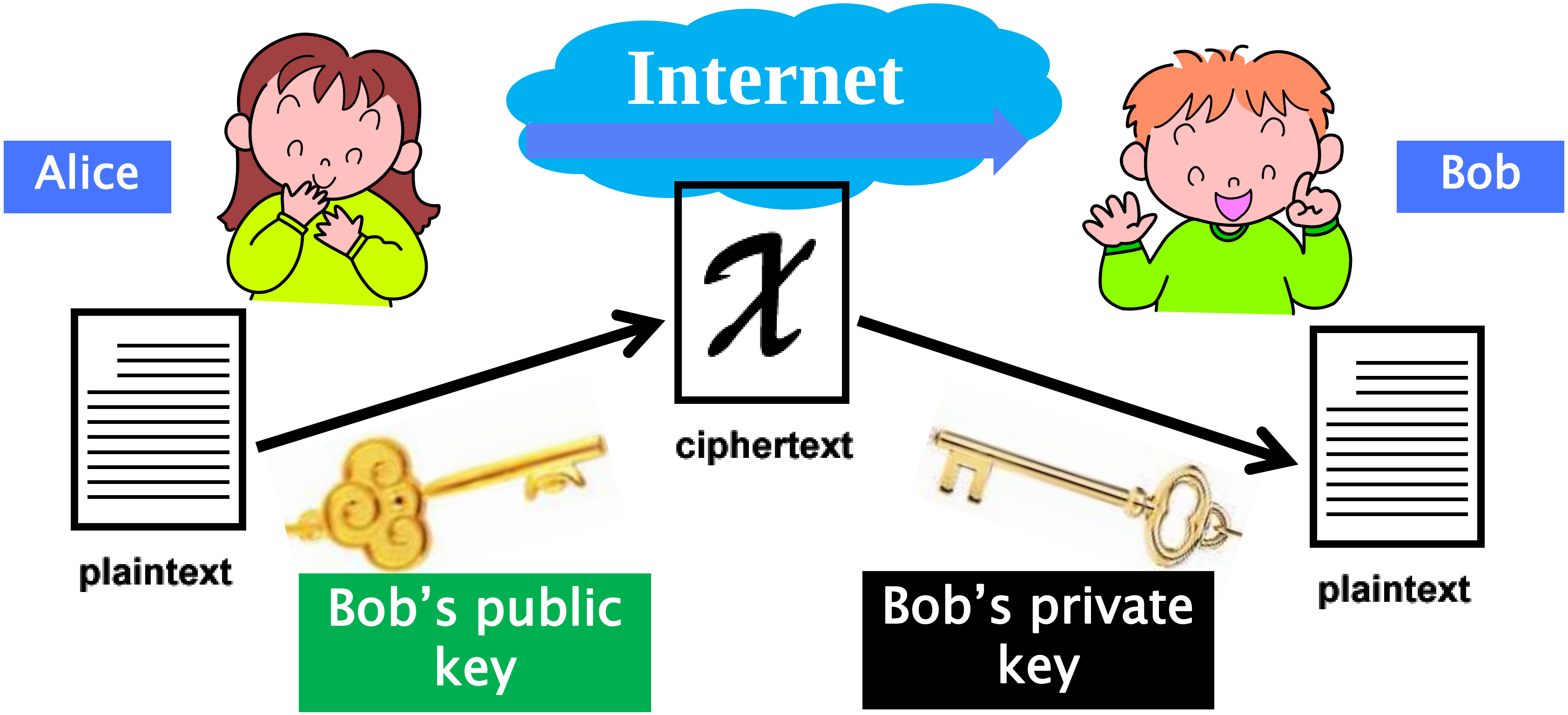
1) SKC

- **Block Cipher**
  - **Each block (fixed-sized chunk) is encrypted**

- **Stream Cipher**
  - **Keystream: has same length as the plaintext**

2) Public-Key Cryptography

- PKC (Asymmetric-key)
  - since 1976, Diffie-Hellman



- Advantages and Disadvantages:

2) PKC

- **PKCs can be seen as invariably Block Ciphers**
  - **RSA**
  - **ElGamal**
  - **ID-based Cryptography**
  - **Signatures**
  - **…**

3) Hybrid Cryptography

- **A combination of SKC and PKC**
  - **SKC: faster, to encrypt a “long” message**
    - **To encrypt the plaintext**
  - **PKC: slower, to encrypt small amounts of data**
    - **To encrypt the secret key**

4) Applications: Message Integrity

- **Message Integrity**
  - **Integrity of data**
  - **Secrecy (confidentiality)**
  - **Passive adversary v.s. Active adversary**

- **Methods:**
  - **Message authentication codes (MACs): SKC**
  - **Signature schemes: PKC**
  - **Hash functions**

4) Applications: Message Integrity

- **MACs: SKC**
  - **Secret key, tag**
  - **Encrypt-then-MAC**
  - **Deniable**
- **Signature schemes: PKC**
  - **Signing algorithm, signature, verification algorithm**
  - **Sign-then-encrypt**
  - **Nonrepudiation**

4) Applications: Message Integrity

- **Hash Functions: (SKC)**
  - **Cryptographic has function**
  - **Message digest**
  - **Hash-then-sign**
  - **Hash-then-sign-then-encrypt**
- **Certificates: PKC**

Cryptanalysis

5) Cryptanalysis: Security

- **Attack models: Kerckhoffs' Principle**
  - **Known ciphertext attack**
  - **Known plaintext attack**
  - **Chosen plaintext attack**
  - **Chosen ciphertext attack**
- **Adversarial goals**
- **Security levels:**
  - **Computational security**
  - **Provable security (reductionist security)**
  - **Unconditional security**

Goal: The adversary cannot achieve a weak adversarial gol in a strong attack model, given significant computational resources.

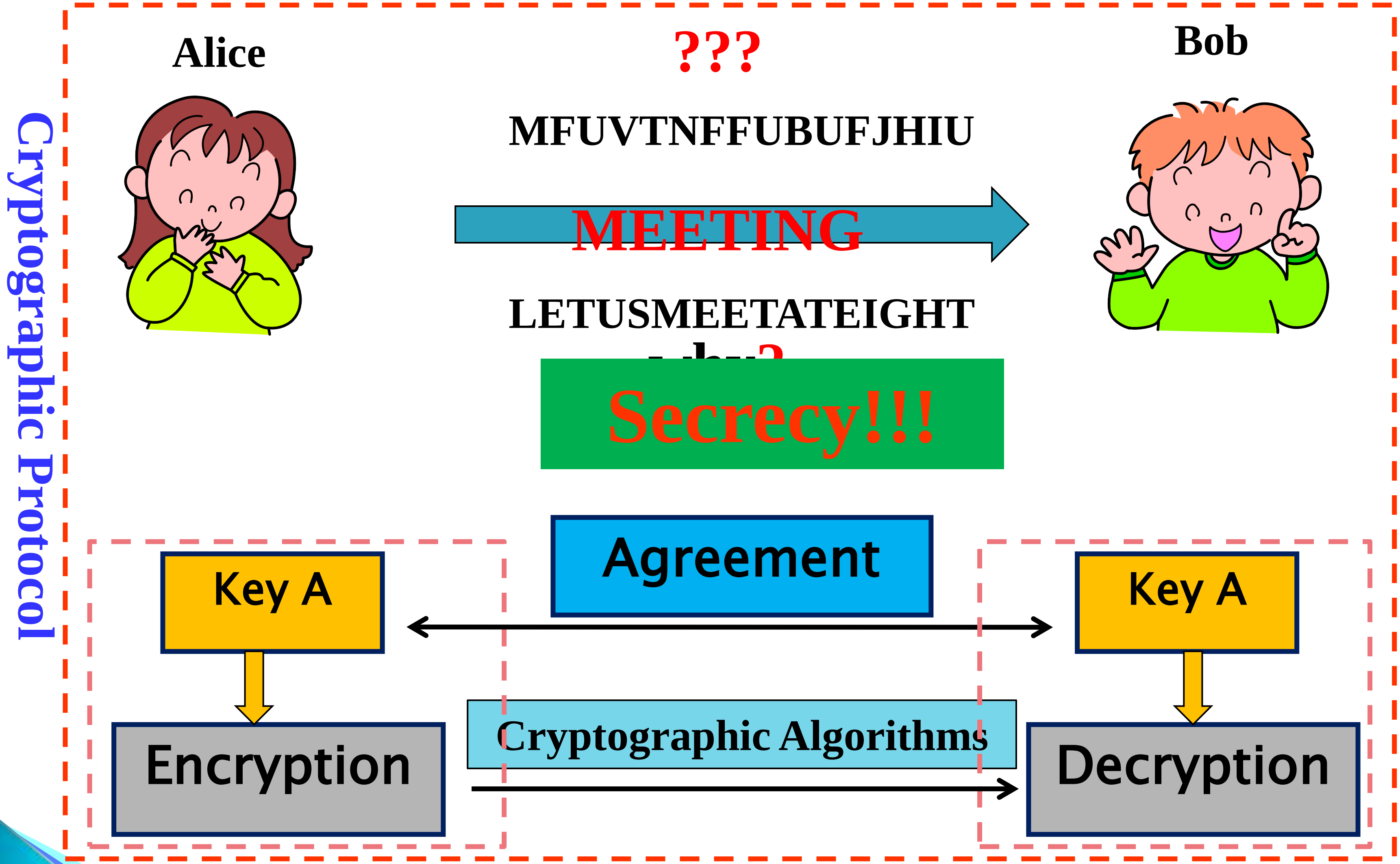
Outline

- **1. Course Information**

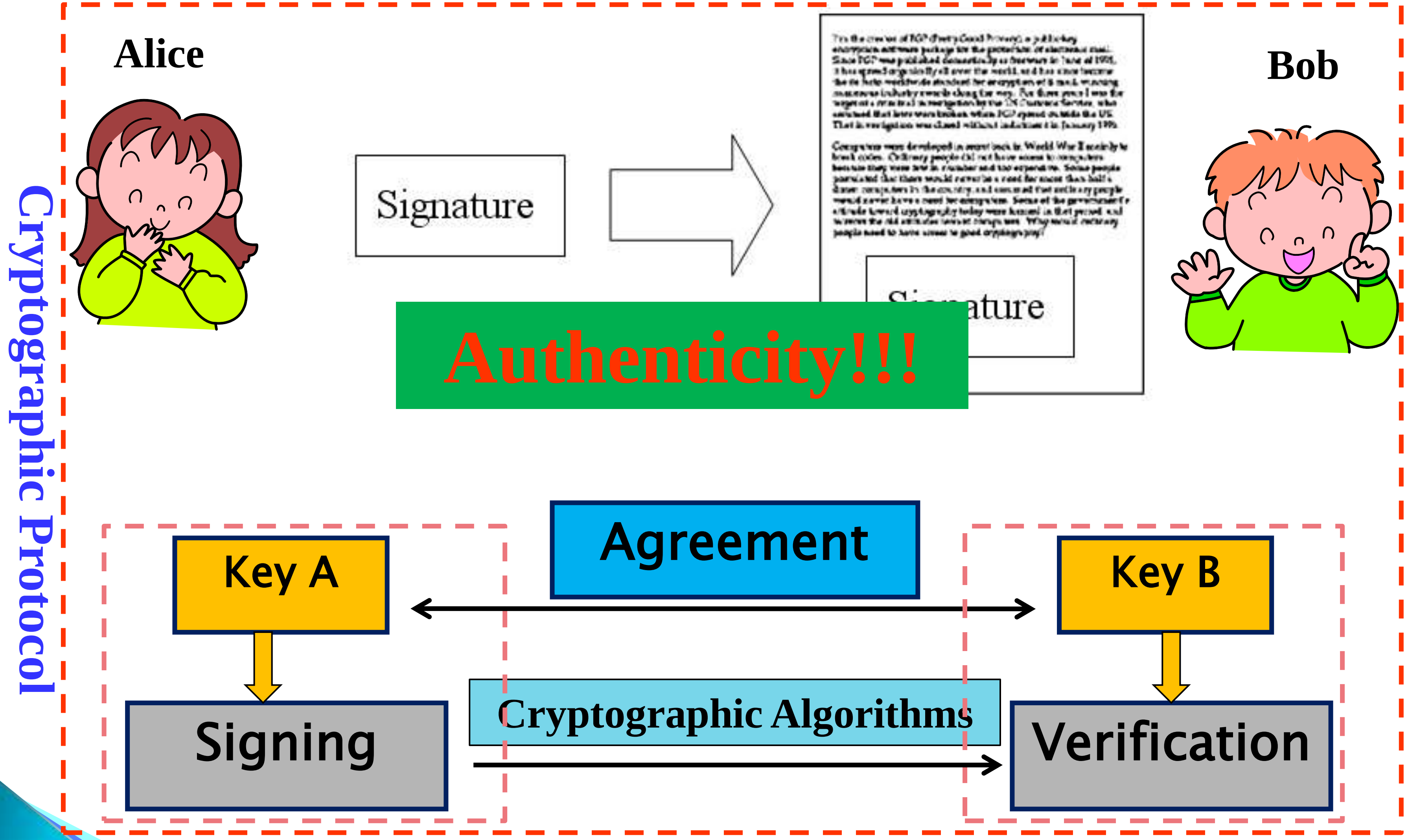
- **2. Evolution of the Cryptography**

- **3. Intuitions on Cryptographic Algorithms and Protocols**

3.1 Simple Example1



3.2 Simple Example 2



Cryptographic Protocol

Alice

Bob

Signature

Authenticity!!!

Agreement

Key A

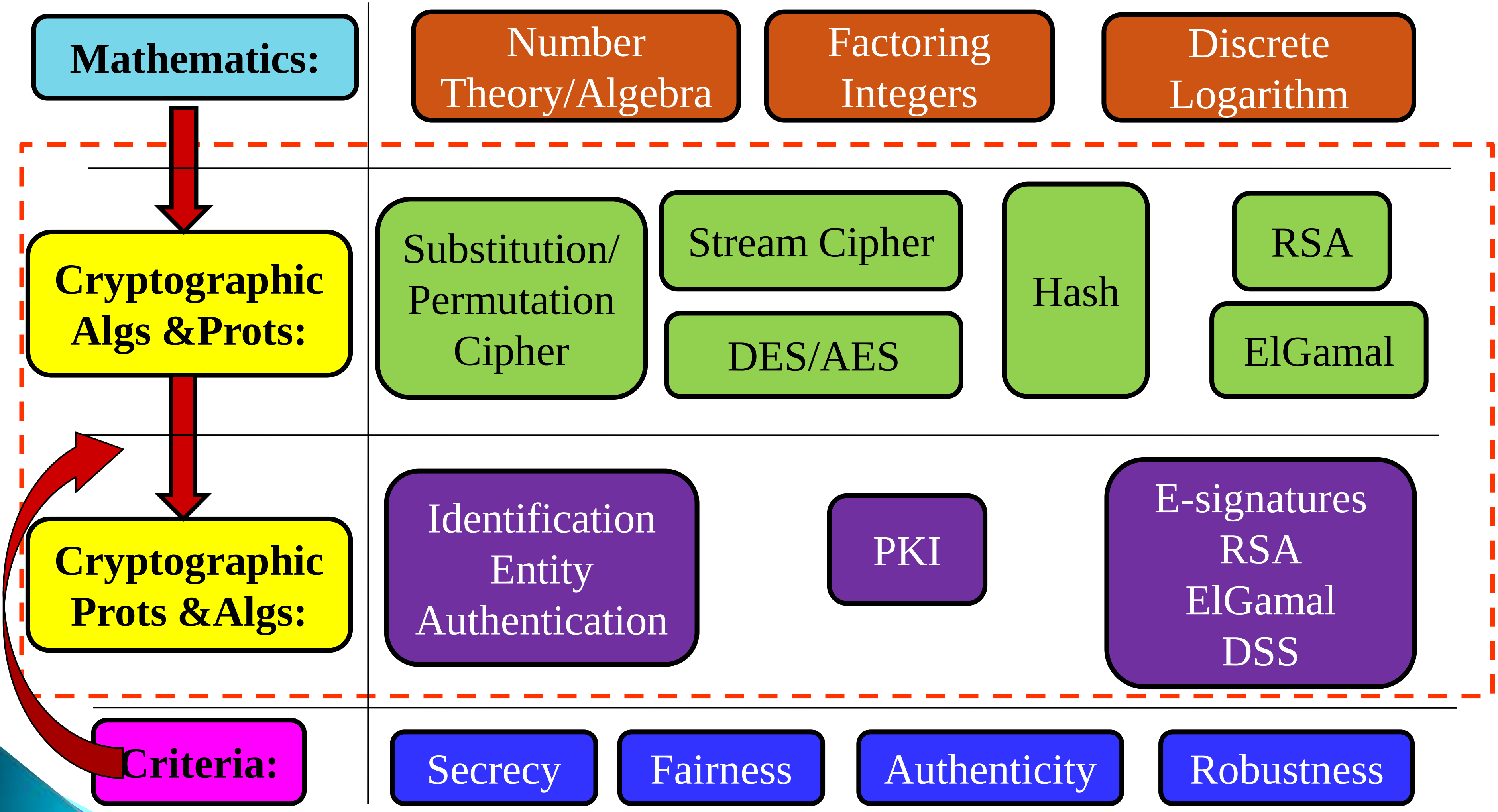
Key B

Signing

Cryptographic Algorithms

Verification

Course Structures



Mathematics:

Number Theory/Algebra

Factoring Integers

Discrete Logarithm

Cryptographic Algs &Prots:

Substitution/ Permutation Cipher

Stream Cipher

DES/AES

Hash

RSA

ElGamal

Cryptographic Prots &Algs:

Identification Entity Authentication

PKI

E-signatures
RSA
ElGamal
DSS

Criteria:

Secrecy

Fairness

Authenticity

Robustness

Questions?

Challenging and Engaging

Cherishable and Enjoyable