Vietnam National University Ho Chi Minh City, University of Science
Department of Information Technology

Overview of Cryptography and Application

Assoc. Prof. Trần Minh Triết
PhD. Trương Toàn Thịnh

fit@hcmus

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Overview

- The course provides students with knowledge related to:
  - Symmetric/asymmetric cryptosystem,
  - Hash function,
  - Digital signature,
  - Public key certification system
- Credits: 4 (3-Cre theory + 1-Cre lab)
- Level: third/fourth-year student
- Allocation-time: 45 theory-class + 30 lab
- Prerequisites: Discrete math, Probability statistics, Data structures and algorithms, Introduction to cryptography

Overview

- Theoretical lecturers
  - Advisor Trần Minh Triết tmtriet@fit.hcmus.edu.vn
  - Advisor Trương Toàn Thịnh ttthinh@fit.hcmus.edu.vn
- Lab lecturers
  - Advisor Lương Vĩ Minh lvminh@fit.hcmus.edu.vn
  - Advisor Mai Anh Tuấn matuan@fit.hcmus.edu.vn
- Grade-scale:
  - Theory: multiple choice questions + exercises (~40%)
  - Midterm & Assignments in the course of study are submitted according to the milestones specified in the semester (~40%)
  - Seminar: Groups of up to 5 students (~20%)

fit@hcmus

Contents

- Topic 1: Overview of Cryptography & Applications
- Topic 2: Classical ciphers
- Topic 3: Shannon theory
- Topic 4: Symmetric modern ciphers (DES, AES…)
- Topic 5: Modes of operation and padding
- Topic 6: Asymmetric cipher
- Topic 7: Digital signature/hash function
- Topic…: Public certificate
- Topic…: Secured Socket Layer
- Topic…: Wireless network protocols (WEP, WPA2…)
- Topic…: Others (Single Sign-On, Kerberos, …)
- …

References

- Vietnamese
  - Mã hóa và ứng dụng (Dương Anh Đức & Trần Minh Triết)
  - Mã hoá thông tin: phương pháp và ứng dụng (Bùi Doãn Khanh & Nguyễn Đình Thúc)
- English
  - Cryptography–Theory and Practice, 2nd edition (Douglas R. Stinson)
  - Cryptography and Network Security: Principles and Practice, 3rd Edition (W. Stallings)
  - Handbook of Applied Cryptography (Menezes, A., Van Oorschot, P., Vanstone, S)
  - Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition (Bruce Schneier)
  - Internet Cryptography (Richard E. Smith)

Introduction

- Cryptography has been around for thousands of years.
- For many centuries, the results of this field were mostly not applied in civilian areas of social life, but were mainly used in the military, political, and diplomatic fields. ...
- Today, information encryption and security applications are being used more and more popularly in different fields around the world, from the fields of security, military, defense... to the fields of civil services such as e-commerce, banking, etc.

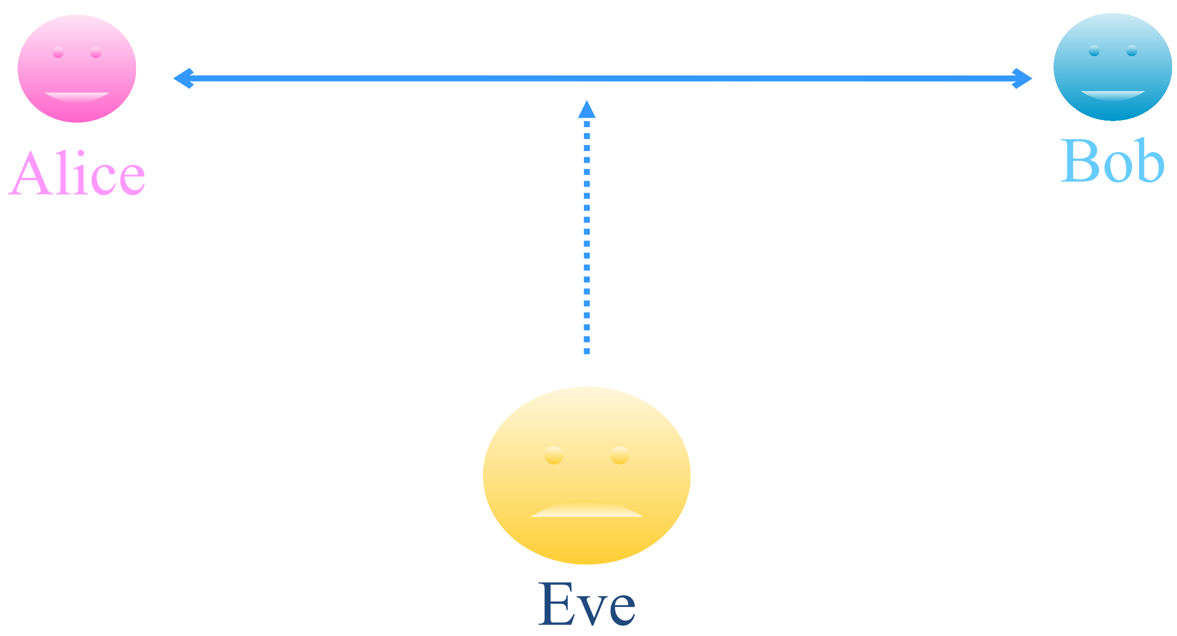
Cryptography

- Cryptography is the science that studies mathematical techniques to provide information protection services.
- W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall
- Terms:
  - Cryptography
  - Cryptanalysis
  - Cryptology = Cryptography + Cryptanalysis
  - Security

Cryptography???

Traditional understanding: keep the content of the exchange secret

Alice and Bob talk to each other while Eve tries to “eavesdrop”.

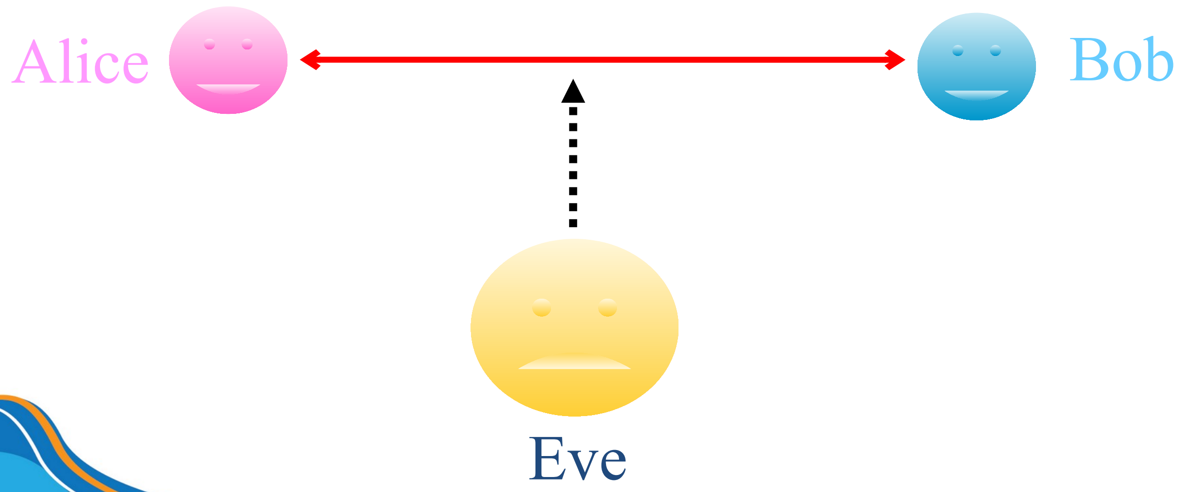


Some information problems

- Confidentiality: ensuring information is kept confidential.
- Integrity: ensures the integrity of information in communications or helps detect that information has been modified.
- Authentication: authenticate the partners in the communication and authenticate the information content in the communication.
- Non-repudiation: ensure that any partner in the system cannot deny responsibility for the action that he has taken

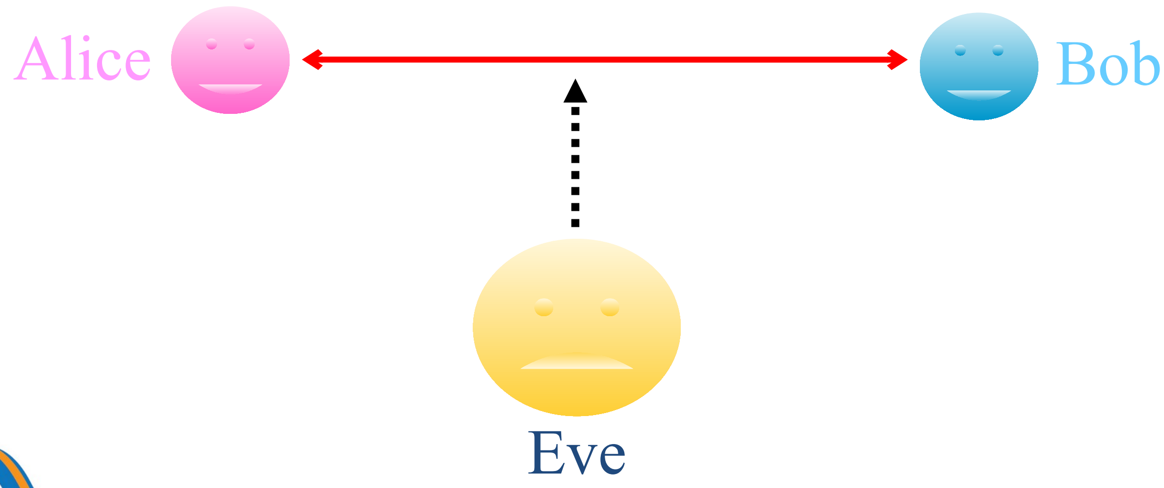
Authentication

- Example:
  - Bob waits Alice for “confirmation” until the working-time
  - Need to make sure that Eve doesn't interfere to create fake “confirmations”
- Two cases: online and offline
  - Data origin authentication for offline
  - Identification/Entity authentication for online



Integrity

- Example:
  - Bob needs to make sure he received exactly what Alice sent
  - It is necessary to ensure that Eve does not intervene to correct the message that Alice sent to Bob
- Integrity

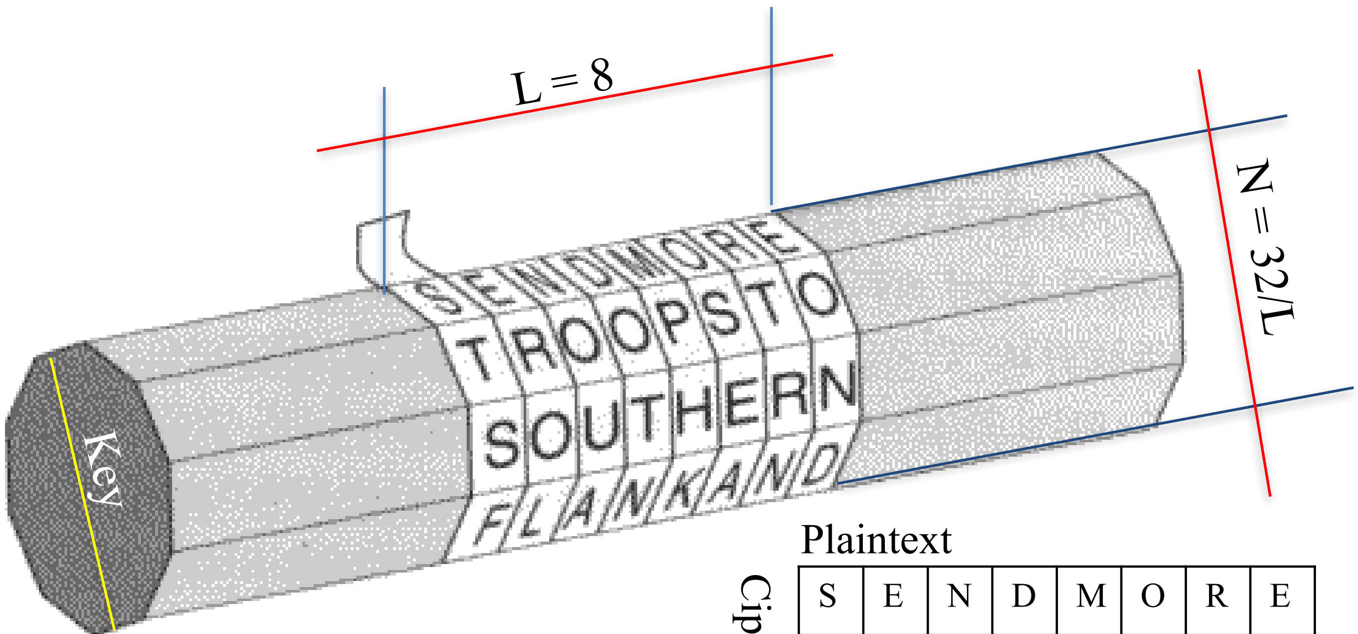


Non-repudiation

- Example:
  - Bob receives a message that Alice sent
  - Alice cannot "refute" not to send this message to Bob
- Non-repudiation

Brief history of the development of cryptography

- Seals are used to seal important documents
- Password is used to identify people in the organization…



Plaintext

Ciphertext

S	E	N	D	M	O	R	E
T	R	O	O	P	S	T	O
S	O	U	T	H	E	R	N
F	L	A	N	K	A	N	D

https://asecuritysite.com/encryption/rust_scy

Ancient ciphers

- **Atbash** method:
  - Used in ancient Hebrew “ששך = בבל”

ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

- **Caesar** method:

A	B	C	…	X	Y	Z
D	E	F	…	A	B	C

  - Anyone know this encryption rule to easily decrypt the message

Ancient ciphers

- The Caesar method is a special case of the Shift Ciphers method.
- Shift Cipher method: characters are rotated to K positions in the alphabet. K is considered the key for decryption

A	B	C	…	X	Y	Z
D	E	F	…	A	B	C

- Both the Atbash and Shift Cipher methods are special cases of the general method used in antiquity: the "mono-alphabetic substitution cipher" method.

Ancient ciphers

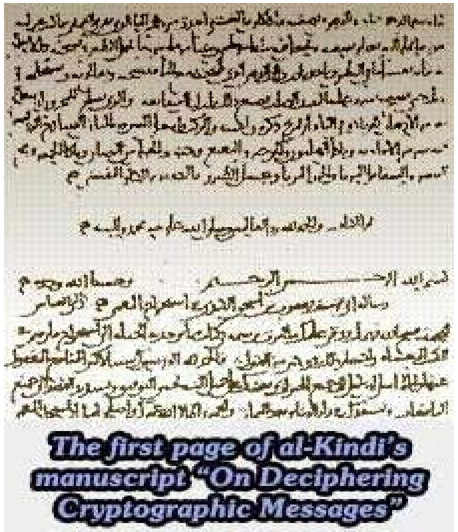
- Not all ancient coding methods used the substitution method.
- First encoder: Spartan scytale (encryption stick)

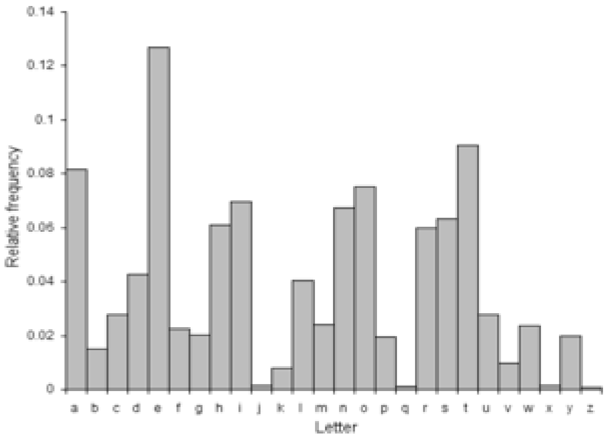
https://plus.maths.org/content/os/issue34/features/ekert/index

- Using this device, the letters in the message are not changed, but only the position of the messages appear (Transposition).

Ancient ciphers

- According to recorded documents, the method of frequency analysis has been used since the 9th century





https://plus.maths.org/content/os/issue34/features/ekert/index *https://en.wikipedia.org/wiki/Caesar_cipher*

- Coding in Europe had almost no development from antiquity to the 14th century!!!

Renaissance ciphers

- In Italy, as in other European countries, cryptography began to be developed again
- Countries and cities began looking for experts in cryptography and code breaking to encrypt and decrypt messages.
- The encryption method of this stage is usually “Poly-alphabetic substitution cipher”.
- Many cryptographic tools are made and used

Renaissance ciphers

- Multi-character substitution encoding can be viewed as using multiple consecutive single-character substitutions.
- Usually use the Cipher Disk tool, or use the lookup table to help encrypt and decrypt
- The main (classical) technique used to break the Multi-Character Replacement cipher system consists of 2 steps:
  - Find out the length of the cycle
  - Apply analytical techniques (for single-character substitution encoding) + information obtained from previous characters

The 19th and early 20th centuries ciphers

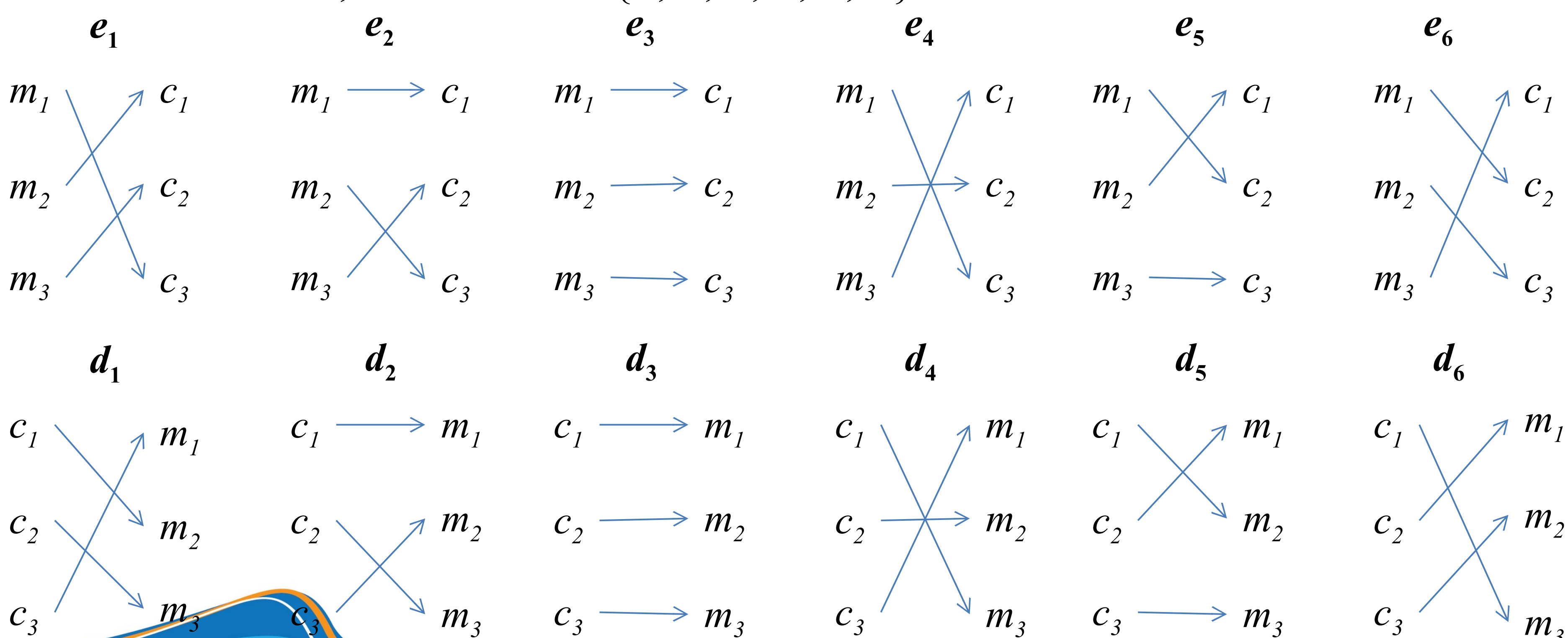
- Encryption was widely used during World War I
- The development of radio waves and radios made communication in the military easier and more common.
- Requires devices that support encryption and decryption => encoders are born
- World War II: the war on science, including cryptography.
- Enigma (Germany) cipher machine decrypted by British military
- Japanese ‘Purple’ encoder decrypted by US military

Cryptography system

- A cryptosystem is a set of five (P, C, K, E, D) that satisfy the following conditions:
  - Source set P is the finite set of all possible source messages to be encrypted
  - Target set C is the finite set of all possible messages after encryption
  - Key set K is a finite set of keys that can be used
  - E and D are the encryption and decryption rules, respectively. For each $k \in K$, there exists an encryption rule $e_k \in E$ and a decryption rule $d_k \in$ D. Encryption rule $e_k: P \to C$ and decryption rule $e_k: C \to P$ are two functions satisfying $d_k(e_k(x)) = x$, $x \in P$
- **Ensure that a message x encrypted with the encryption rule e_k can be correctly decrypted with the rule d_k**

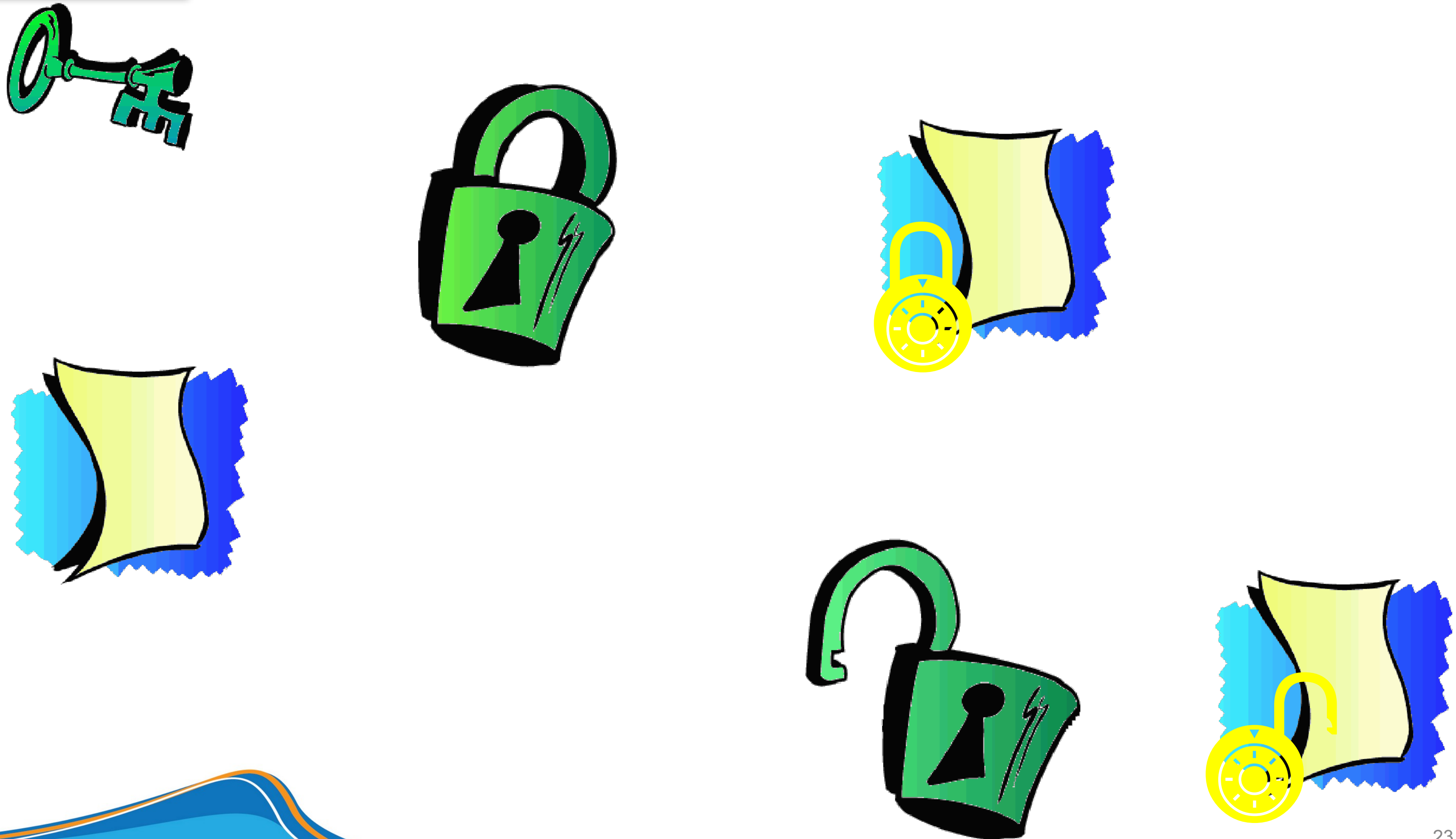
Cryptography system

- Example of a cryptosystem:
  - Let $P = \{m_1, m_2, m_3\}$, $C = \{c_1, c_2, c_3\}$ ⇒ 3 × 2 × 1 = 6 bijections: $P \rightarrow C$. So, we have $K = \{1, 2, 3, 4, 5, 6\}$

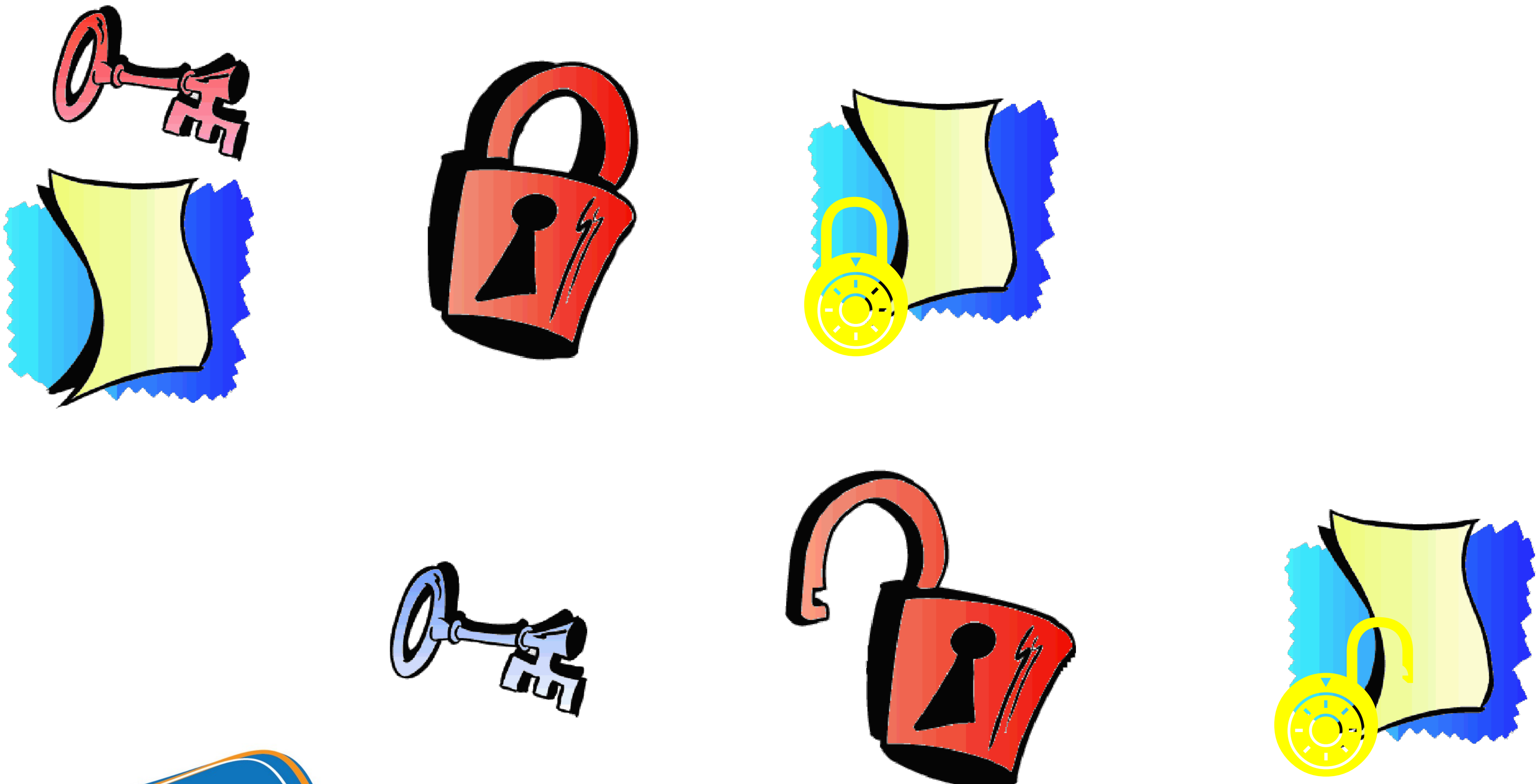


fit@hcmus

Symmetric cipher

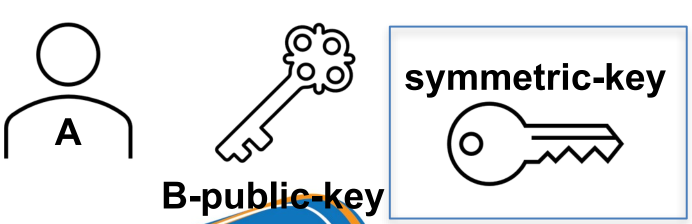


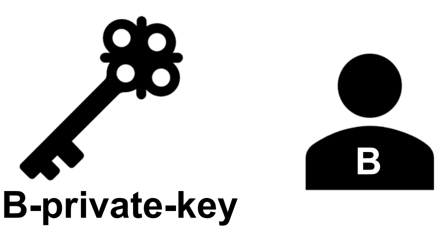
Asymmetric cipher



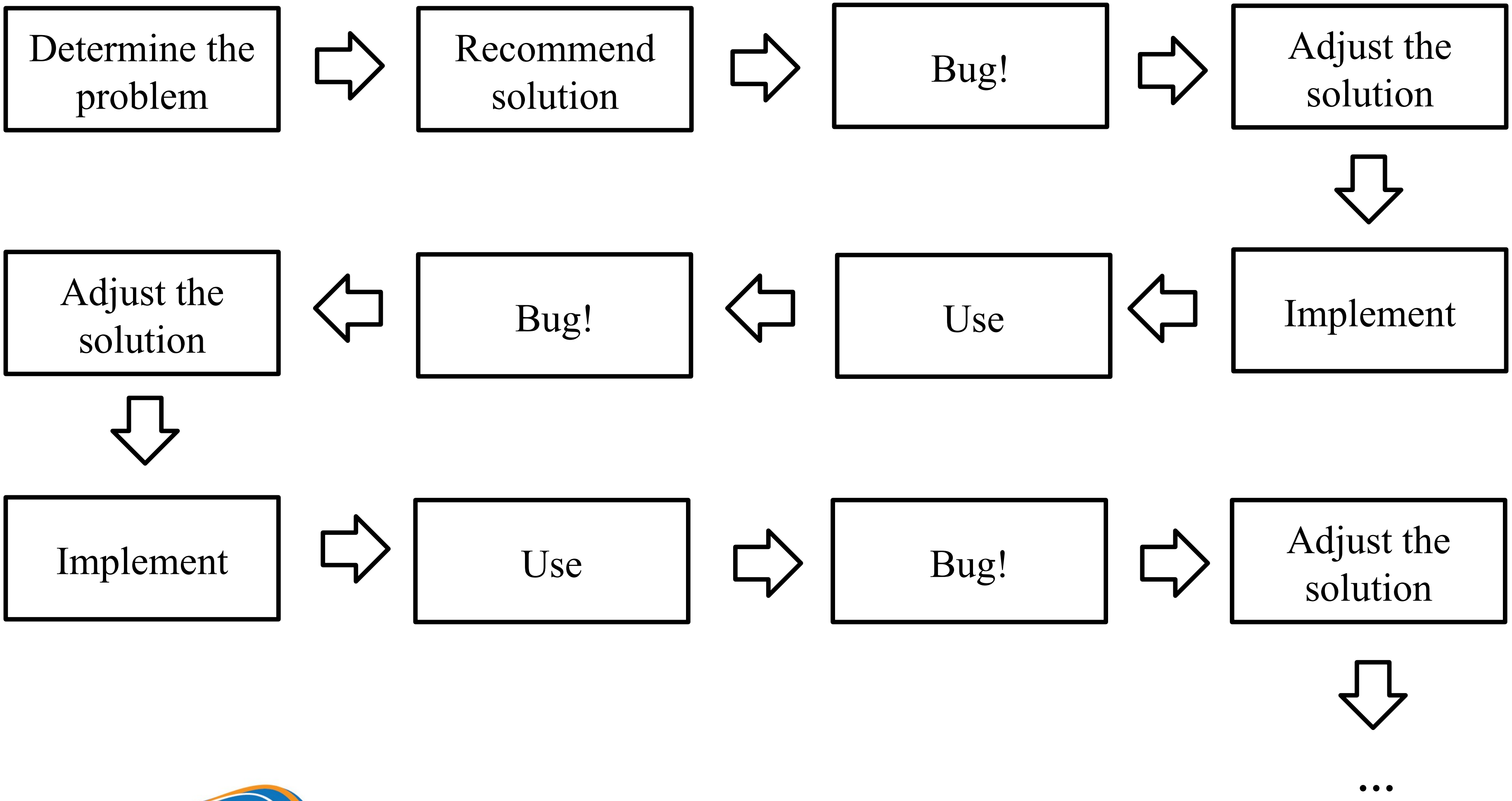
Compare Symmetric & Asymmetric ciphers

Fast processing	Slow processing
Short key-length	Long key-length
Difficult to exchange keys	Easy to exchange keys

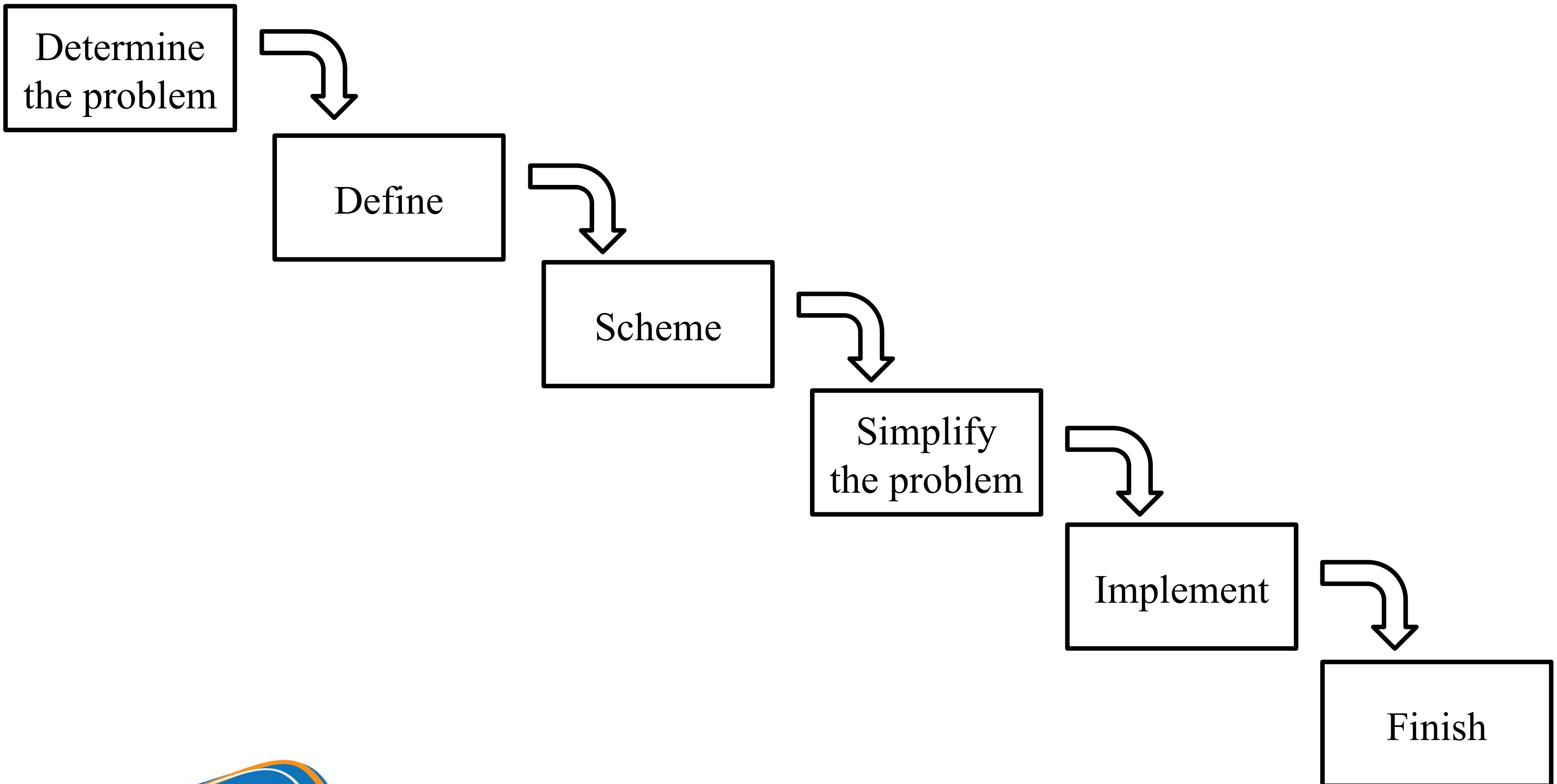




Design in the direction of cryptographic analysis



Provable-Security approach



Concept of Z_m

- Z_m is a set of $\{0, 1, \ldots, m\text{-}1\}$, equipped with addition operator (denote $+$) and multiplication operator (denote $\cdot$).
- Addition and multiplication in Z_m are similar to Z, except for the result modulo m.
- Example:
  - Assume we need compute in Z_{16}.
  - In Z, we have $11 \cdot 13 = 143$
  - Because $143 \equiv 15 \pmod{16}$, so $11 \cdot 13 = 15$ in Z_{16}.

Properties of Z_m

- Addition of Z_m
  - Closure: $a, b \in Z_m$, $a + b \in Z_m$
  - Commutativity: $a, b \in Z_m$, $a + b = b + a$
  - Associativity: $a, b, c \in Z_m$, $(a + b) + c = a + (b + c)$
  - Z_m has a neutral element 0, $a, b \in Z_m$, $a + 0 = 0 + a = a$
  - For each $a \in Z_m$, there is an opposing element $(m – a) \in Z_m$
- Multiplication of Z_m
  - Closure: $a, b \in Z_m$, $a \times b \in Z_m$
  - Commutativity: $a, b \in Z_m$, $a \times b = b \times a$
  - Associativity: $a, b, c \in Z_m$, $(a \times b) \times c = a \times (b \times c)$
  - Z_m has a unit element 1, $a, b \in Z_m$, $a \times 1 = 1 \times a = a$
  - Distribution of '$\times$' with '+': $a, b, c \in Z_m$, $(a + b) \times c = a \times c + b \times c$

Extended Euclide algorithm

- Consider 2 prime numbers *a* and *b*, let's build
  - $r_0 = a$ $\qquad r_1 = b$
  - $s_0 = 1$ $\qquad s_1 = 0$
  - $t_0 = 0$ $\qquad t_1 = 1$
- So, we have:
  - $r_2 = r_0 - q_0 r_1$
  - $s_2 = s_0 - q_0 s_1$
  - $t_2 = t_0 - q_0 t_1$
  - …
  - $r_{i+1} = r_{i-1} - q_i r_i \ (i \ge 1)$
  - $s_{i+1} = s_{i-1} - q_i s_i$
  - $t_{i+1} = t_{i-1} - q_i t_i$

Algorithm stops when $r_{k+1} = 0$ & $r_k = gcd(a, b) = a s_k + b t_k$

Extended Euclide algorithm

- Example $a = r_0 = 240$ and $b = r_1 = 46$

i	q_{i-1}	r_i	s_i	t_i
0		240	1	0
1		46	0	1
2	240 / 46 = 5	240 − 5 × 46 = 10	1 − 5 × 0 = 1	0 − 5 × 1 = −5
3	46 / 10 = 4	46 − 4 × 10 = 6	0 − 4 × 1 = −4	1 − 4 × −5 = 21
4	10 / 6 = 1	10 − 1 × 6 = 4	1 − 1 × −4 = 5	−5 − 1 × 21 = −26
5	6 / 4 = 1	6 − 1 × 4 = 2	−4 − 1 × 5 = −9	21 − 1 × −26 = 47
6	4 / 2 = 2	4 − 2 × 2 = 0	5 − 2 × −9 = 23	−26 − 2 × 47 = −120

  - Line 6 finds stop-condition $r_6 = 0$
  - Result: $gcd(240, 46) = 2 = -9$ ㅎ 240 + 47 ㅎ 46
- Note: $gcd(a, b) = 1 = as + bt$ (a ㅍ b)
  - If bt mod a ° 1 ㄷ $t = b^{-1}$ mod a
  - If as mod b ° 1 ㄷ $s = a^{-1}$ mod b

https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm