Introduction to Cryptography

CUI TINGTING

School of Cypberspace, Hangzhou Dianzi University

September 11, 2023

Contents

1 Course Basic Information

2 History of Cryptography

3 Some Classic Ciphers

1 Course Basic Information

2 History of Cryptography

3 Some Classic Ciphers

What, Who, When, Where

- Course: Introduction to Cryptography
- Teacher: Cui Tingting (A. P., cuitingting@hdu.edu.cn)
- Time: Monday (3-5) and Tuesday (3-4)
- Address: Building No. 6, Room 117

What will you learn

- Cryptographic primitives, schemes and protocols used in the real world
  - definition of security goals
  - design rationale: how are the goals achieved
- Questions we aim at answering
  - how cryptographic schemes are constructed and why
  - what does it mean for a scheme to be secure
- Basics of underlying mathematics:
  - modular arithmetic and elementary number theory
  - finite groups and fields

What this course does not cover

This is intro to crypto, not more, not less
More specialized topics are treated in other courses, e.g.,

- Securely implementing crypto in Cryptographic engineering
- Embedded systems security in Hardware security
- Firewalls, network sniffing and traffic analysis in Network security
- UNIX security, malware detection in OS security

Grading

The final grade consists of:

- 15% homework (per section)
- 15% in-class exercises (5 times)
- 70% final exam

Lectures and tutorial schedule

Contents	#Courses	Security services
Intro+history	3	
stream cipher	4	Condentiality
block cipher	12	Condentiality
Hash function	4	Integrity
MAC	4	Integrity & Authentication
public cipher	18	Condentiality
digital signature	6	Integ. & Auth. &Non-repudiation
key establishment	5	
Total	56	

Resources

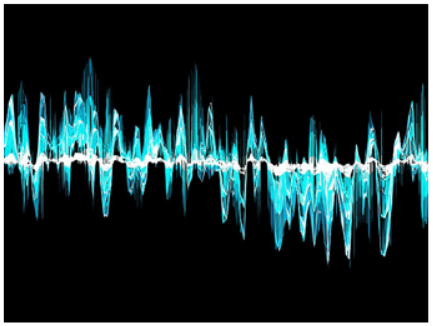
- **Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners**
- Schneier B, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Son, Inc. 2015.
- William Stallings, Cryptography and Network Security: Principles and Practice (7th Edition), Pearson Education Ltd, 2016.
- .....

1 Course Basic Information

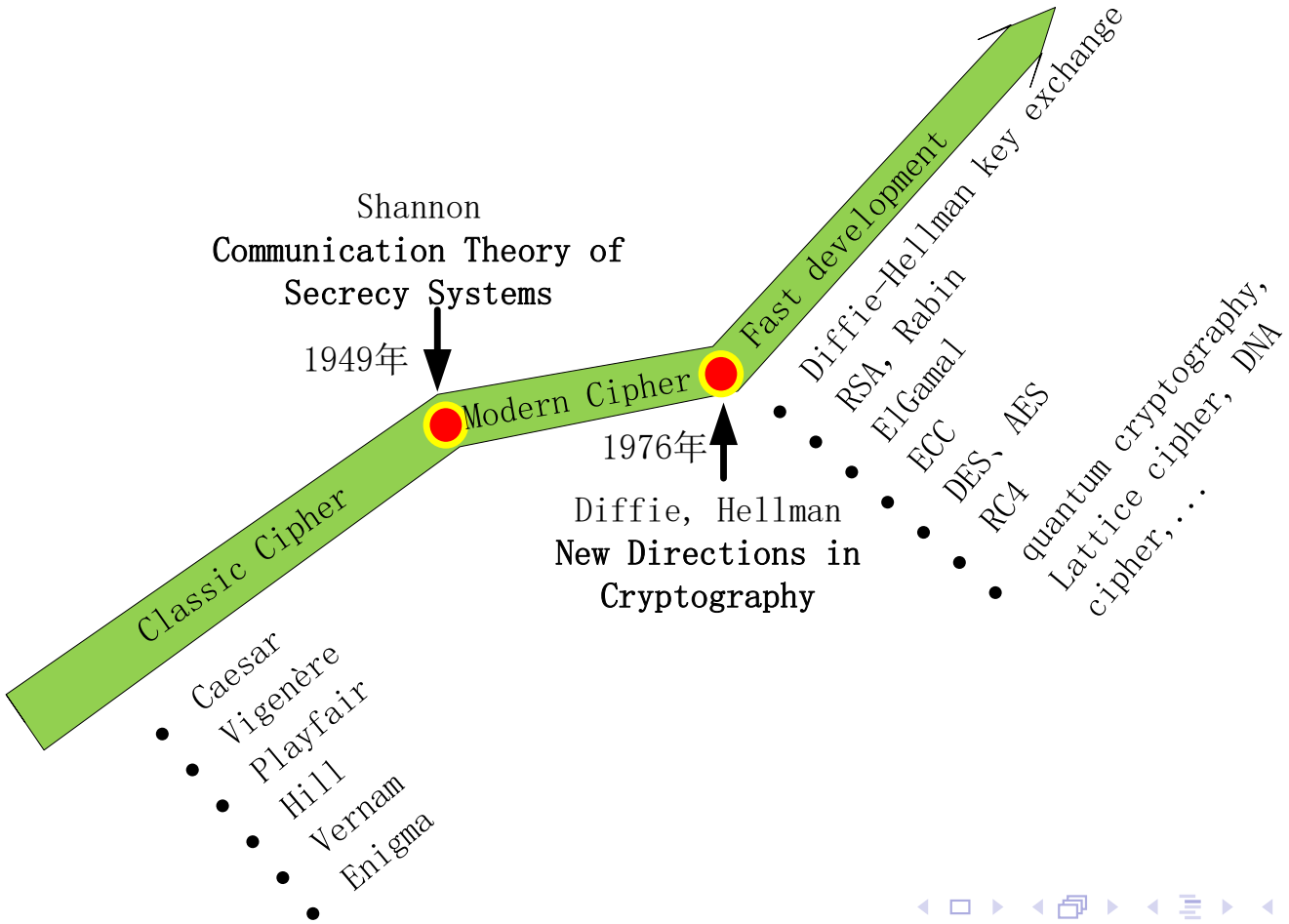
2 History of Cryptography

3 Some Classic Ciphers

What is Cryptography



History of Cryptography



1 Course Basic Information

2 History of Cryptography

3 Some Classic Ciphers

Caesar Cipher

- Ancient cipher, allegedly used by Julius Caesar
- Replaces each plaintext letter by another one (Needs mapping from letters $\rightarrow$ numbers)

Replacement rule

Take letter that follows after k positions in the alphabet.

$$c = (p + k) mod\ 26$$

Caesar Cipher

- Ancient cipher, allegedly used by Julius Caesar
- Replaces each plaintext letter by another one (Needs mapping from letters $\rightarrow$ numbers)

Replacement rule

Take letter that follows after k positions in the alphabet.

$$c = (p + k) mod\ 26$$

Example 1

$k = 7$, Plaintext= ATTACK
Ciphertext = haahr

Caesar Cipher

Example 2

Ciphertext: BRXDUHFOHYHUVWXGHQW

Substitution Cipher

- Historical cipher
- Great tool for understanding brute-force vs. analytical attacks
- Encrypts letters rather than bits (like all ciphers until WW II)

Idea of Substitution Cipher

Replace each plaintext letter by a fixed other letter.

Plaintext		Ciphertext
A	→	k
B	→	d
C	→	w
	....	

for instance, ABBA would be encrypted as kddk.

Attacks against the Substitution Cipher

ATTACK: Exhaustive Key Search (Brute-Force Attack)

- Simply try every possible subsititution table until an intelligent plaintext appears (note that each substitution table is a key).

Attacks against the Substitution Cipher

ATTACK: Exhaustive Key Search (Brute-Force Attack)

- Simply try every possible subsititution table until an intelligent plaintext appears (note that each substitution table is a key).
- How many substitution tables (= keys) are there?

Attacks against the Substitution Cipher

ATTACK: Exhaustive Key Search (Brute-Force Attack)

- Simply try every possible subsititution table until an intelligent plaintext appears (note that each substitution table is a key).
- How many substitution tables (= keys) are there?

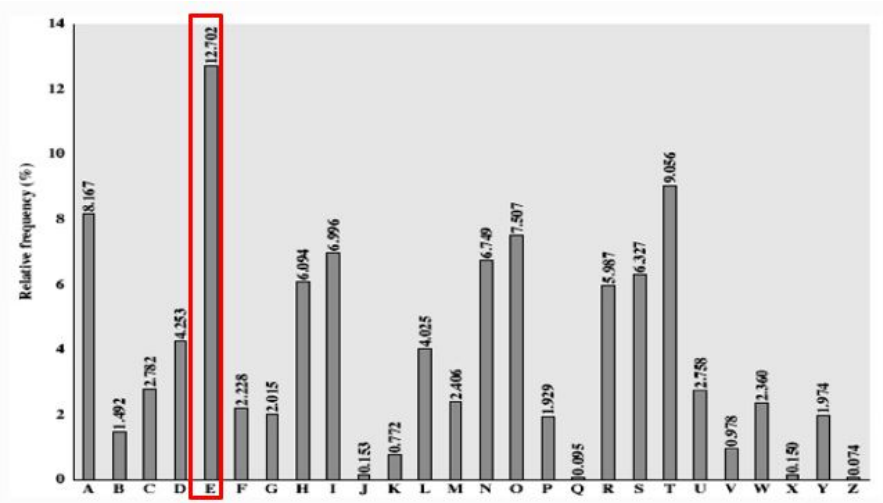
$$26 \times 25 \times \ldots \times 2 \times 1 = 26! \approx 2^{88}.$$

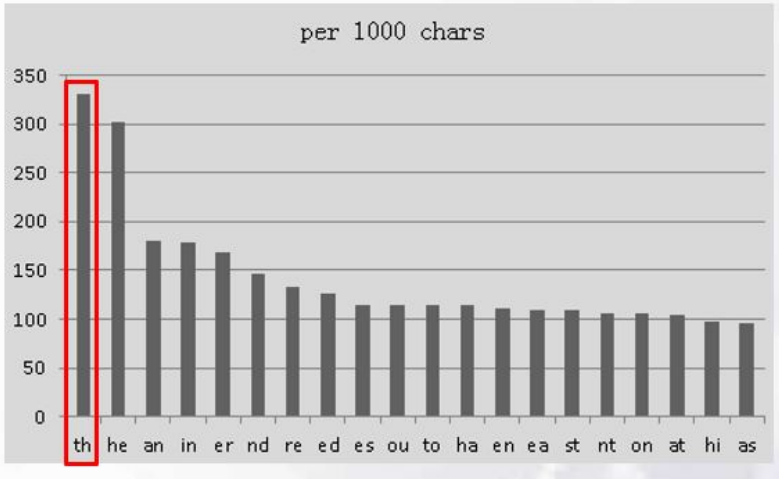
Search through 2^{88} keys is completely infeasible with today's computers!

Can we now conclude that the substitution cipher is secure since a bruteforece attack is not feasible?

Attack: Letter Frequency Analysis

- Letters have very different frequencies in the English language
- Frequency of plaintext letters is preserved in the ciphertext.
- For instanc, ‘e ‘ is the most common letter in English;
- For instanc, ‘th ‘ is the most common two-letter in English;

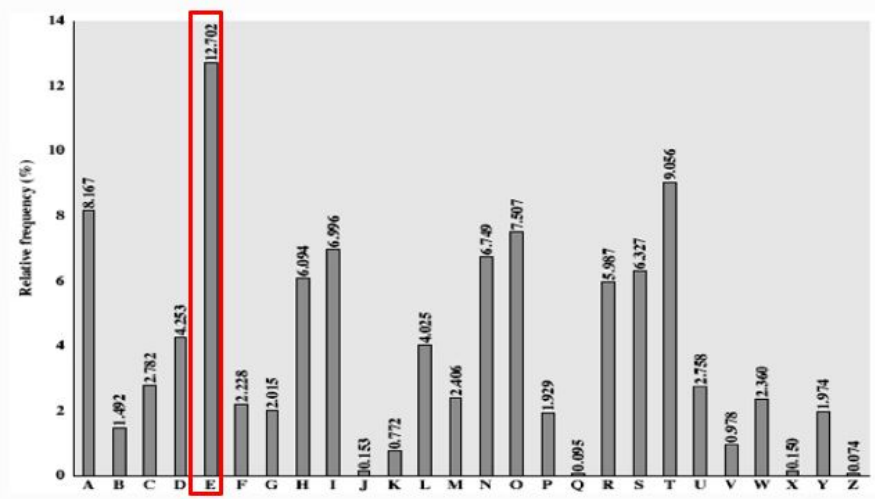


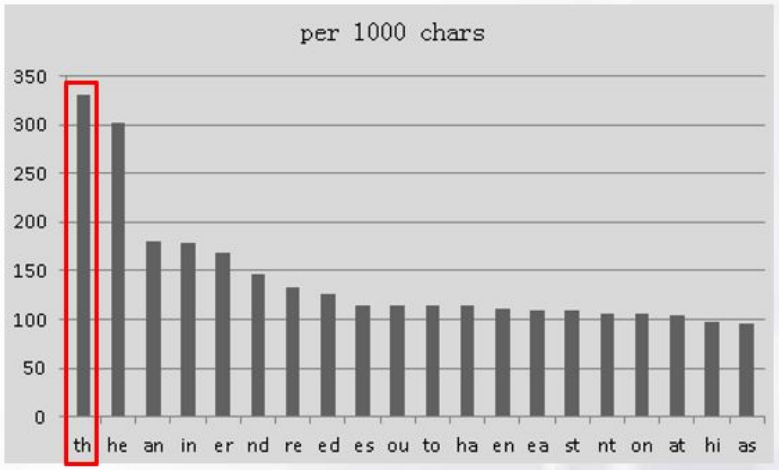


Breaking the Substitution Cipher with Letter Frequency Attack

Example 3

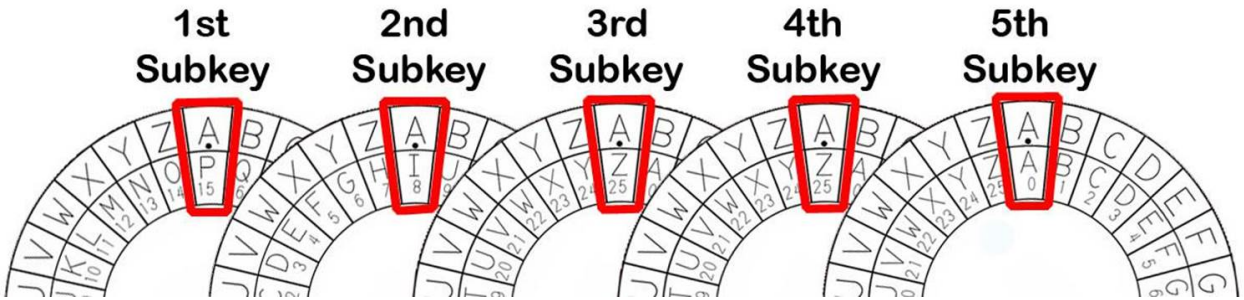
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq vhlq





Vigenère Cipher

- Consist of N different Carsar ciphers

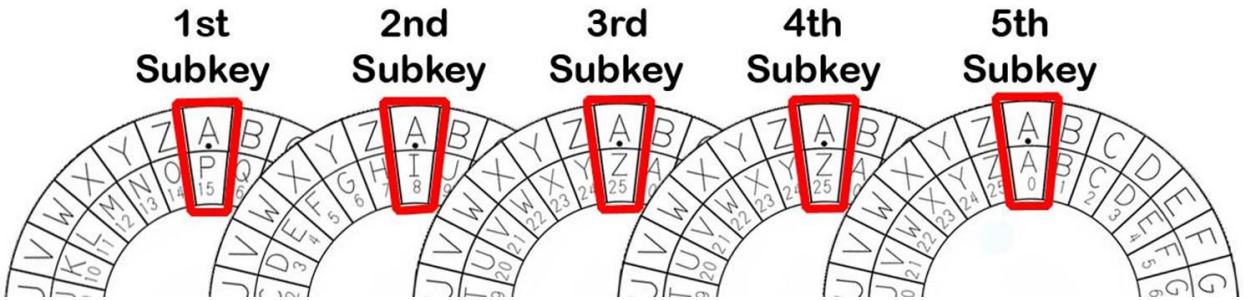


Example 4

Plaintext: AAAAAAAP
Ciphertext: PIZZAPIP

Vigenère Cipher

- Consist of N different Carsar ciphers



Example 4

Plaintext: AAAAAAAP
Ciphertext: PIZZAPIP

Example 5

Plaintext is **I have a lot of money**, key is **math**, What is the ciphertext?

ATTACK Vigenère Cipher

The frequency in ciphertext is broken, so is Vigenère secure?

ATTACK Vigenère Cipher

The frequency in ciphertext is broken, so is Vigenère secure? **Of course not.**

Attack Process

- Use a special plaintext (all letters are same) to find out the length of key;
- Use frequency attack to break every Carsar cipher to recover the key.

Enigma Machine

- Use in the early- to mid-20th century to protect commercial, diplomatic, and military communication.
- It was employed extensively by Nazi Germany during World War II, in all branches of the German military.

Process

1. Input letter on keyboard;
2. keyboard→ plugboard (Stecker)→ Rotors → Reflector→ inverse Rotors →plugboard→ Lampboard (lightboard)
3. output letter from Lampboard.

Enigma Machine

How to use:
https://www.bilibili.com/video/av31393190/?spm_id_from=trigger_reload

How to break:
https://www.bilibili.com/video/av21919076/?p=2

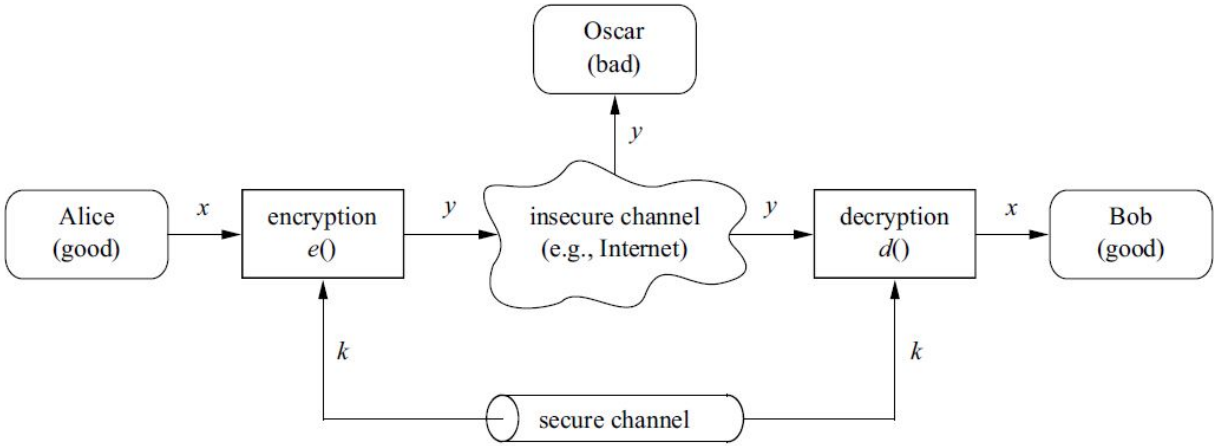
Cryptography is everywhere nowdays






Cryptography is about communication in the presence of adversaries.

Secure communication model



- **Plaintext**: send by Alice;
- **Ciphertext**: recieve by Bob;
- **Encyption algorithm**: ecrypt plaintext to ciphertext;
- **Decryption algorithm**: decrypt ciphertext to plaintext;
- **Key**: used in Encyption and Decryption.

Why do we need Cryptanalysis

- There is no mathematical proof of security for any practial cipher!
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

Why do we need Cryptanalysis

- There is no mathematical proof of security for any practial cipher!
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

Kerckhoff's Principle

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key.

Why do we need Cryptanalysis

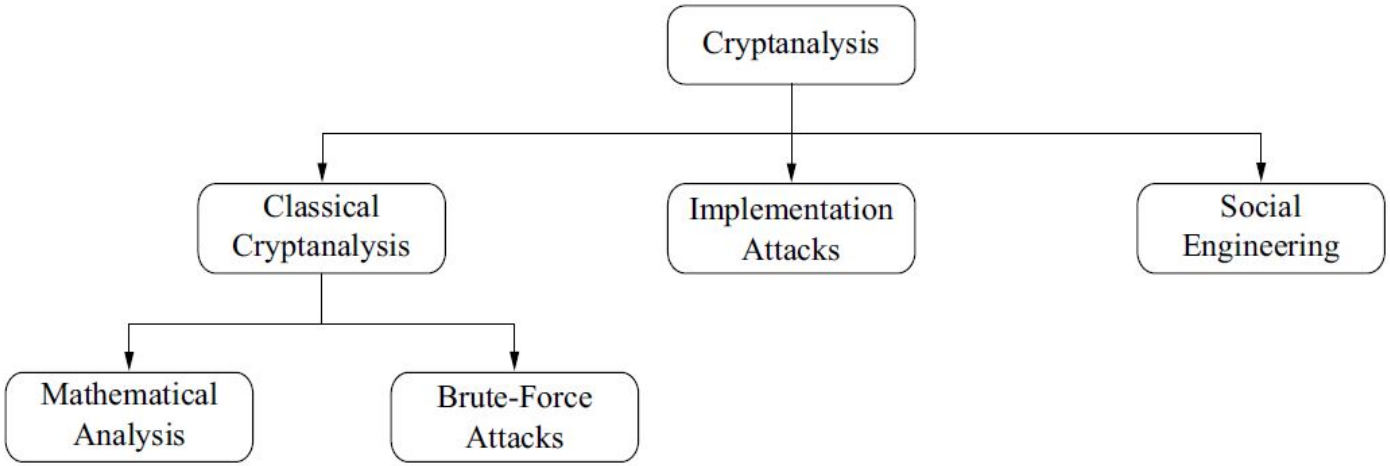
- There is no mathematical proof of security for any practial cipher!
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

Kerckhoff's Principle

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key.

- Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers!
- A cipher is **NOT** "more secure" if its details are kept secret.

Cryptanalysis: Attacking Cryptosystems



- Mathematical Analysis: Differential attack, Linear attack, Algebra attack...
- Implementation Attack: Try to extract key through reverese engineering or power measurement
- Social Engineering: E.g., trick a user into giving up her password

Thanks & Questions