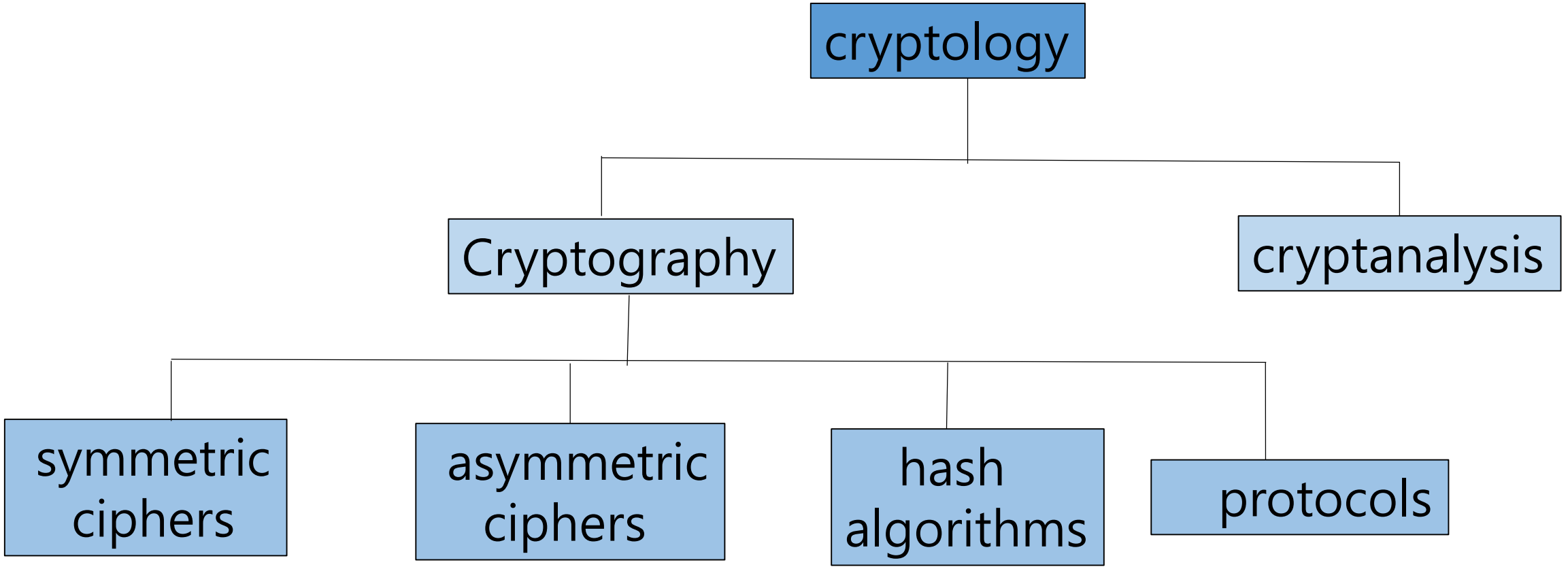
Intro to Crypto

2019. 3. 11

Contents

Cryptology


cryptology
Cryptography
cryptanalysis
symmetric ciphers
asymmetric ciphers
hash algorithms
protocols

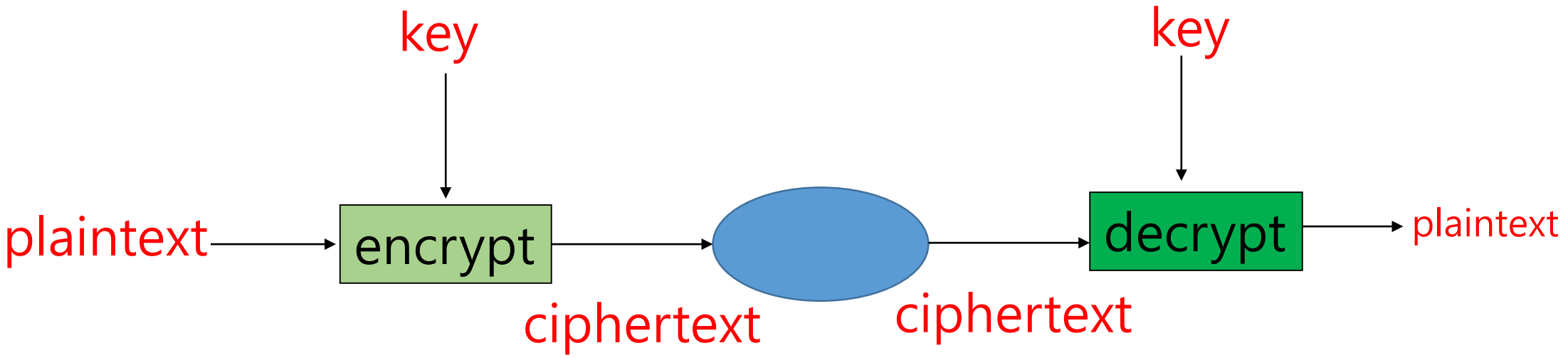
Cryptography system

- Basic assumptions
  - The system is completely known to the attacker
  - That is, crypto algorithms are not secret
  - Only the key is secret
- This is known as **Kerckhoffs' Principle**
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to cope with weaknesses beforehand

Kerckhoffs' Principle

- A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Symmetric Cryptography



Simple Substitution Cipher

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

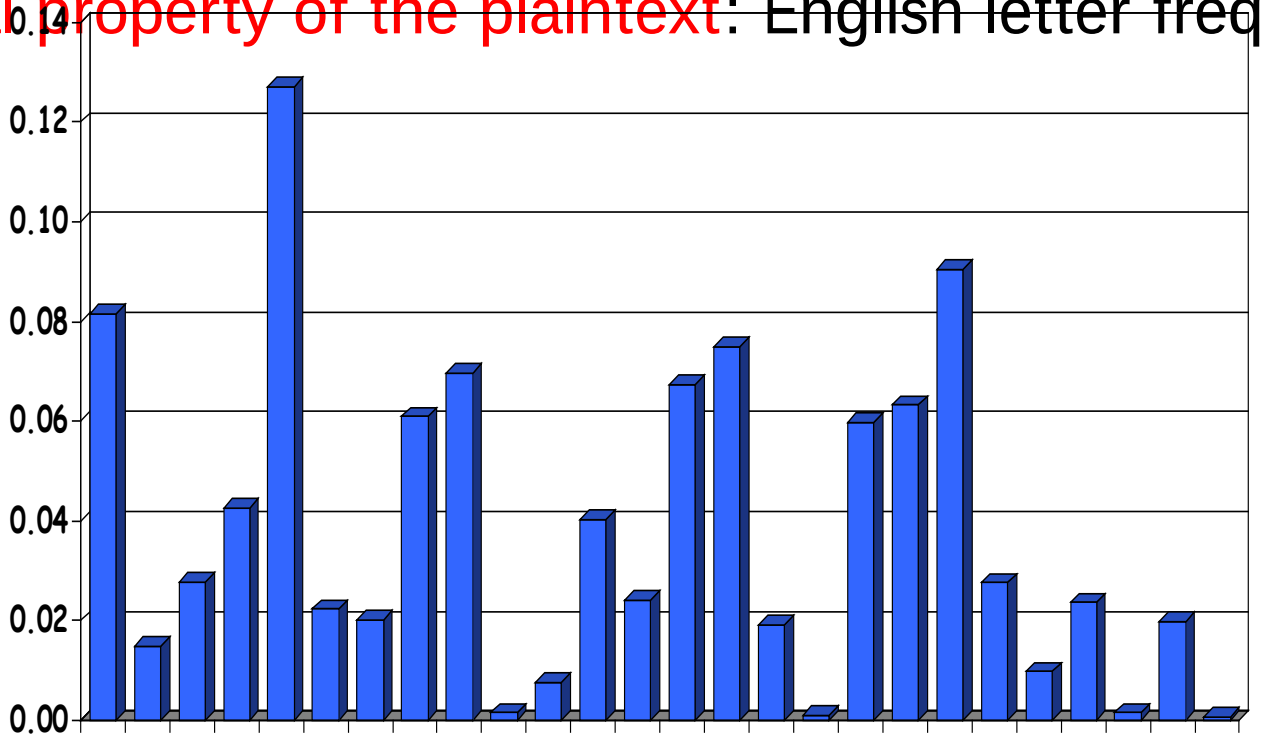
- Ciphertext: IRXUVFRUHDQGVHYHQBHDUVDJR

Cryptanalysis I

- Exhausted key search or Brute-Force Attack
  - Try them all keys
- How may keys?
  - Key space = $26 \cdot 25 \cdot \cdots \cdot 3 \cdot 2 \cdot 1 = 26! \approx 2^{88}$
- According to the key space size, the substitution cipher is secure.

Cryptanalysis II

- Letter frequency analysis
  - Cannot try all 2^{88} simple substitution keys
  - Can we be more clever?
  - Statistical property of the plaintext: English letter frequency



Example

- Statistical property of the encrypted plaintext
- Ciphertext:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVWLEQNTOZQG
GQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXP
FHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQ
VAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJI
WFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLV
WPTOFFA

- Ciphertext frequency counts:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6	8

History of Frequency Analysis

- Discovered by Arabs
  - The first record of the frequency analysis can be found in the book of Al-Kindi in the 9C. (**Abū Yūsuf Yaqūb ibn Isḥāq al-Kindī**, **أبو يوسف يعقوب إبن إسحاق الكندي**) (c. 801–873 CE), (Alkindus)
- Introduced to Europe at the Renaissance

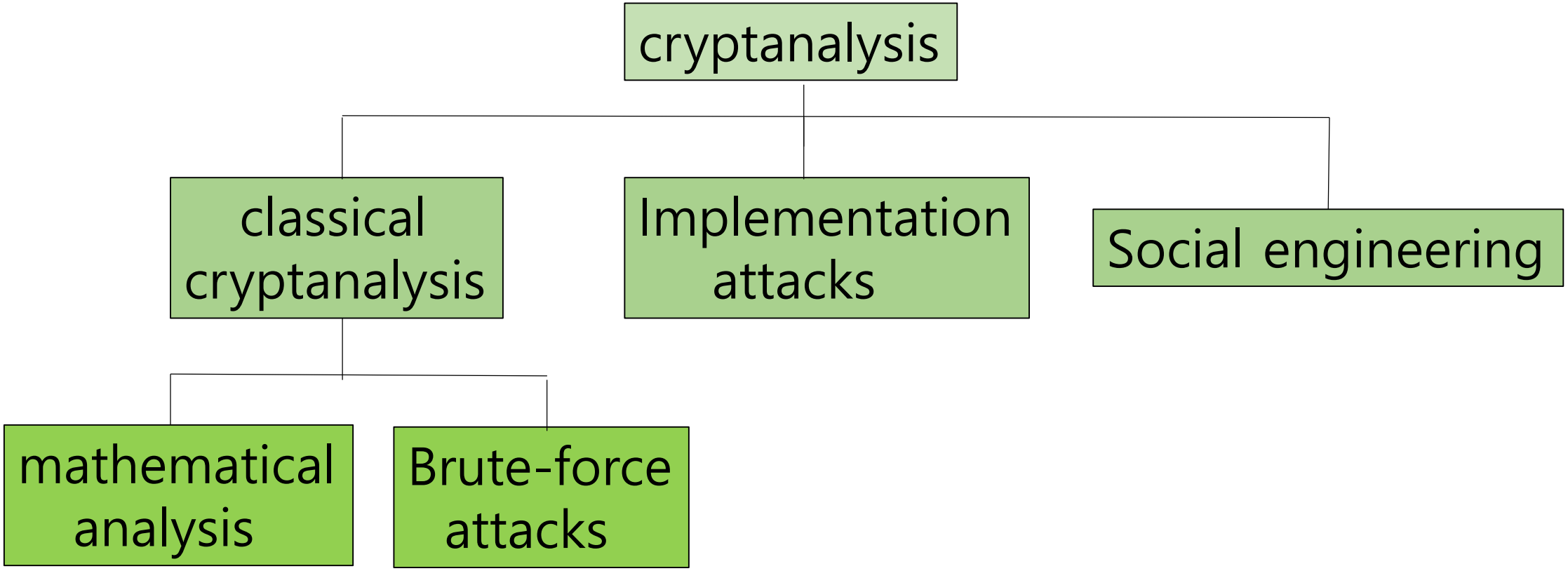
What is the “secure” crytposystem?

- Cryptosystem is **secure** if the best known attack is to try all keys.
  - i.e., Exhaustive key search
- Cryptosystem is **insecure** if ***any*** shortcut attack is known.
- But sometimes insecure cipher might be harder to break than a secure cipher!

More to “secure” crytposystem

- Computationally security
  - A cryptosystem is computationally secure if the best known algorithm for breaking it requires the exhaustive search.
- Unconditional security
  - A cryptosystem is unconditionally or information-theoretically secure if it cannot be broken even with infinite computational resources.

Cryptanalysis



Implementation Attacks

- Side-channel Analysis can obtain the key by measuring the electrical power consumption of a processor which operates on the key. The power trace can then be used to recover the key by applying signal processing techniques.
- Electromagnetic radiation can give information about the key.
- The implementation attacks are related to the physical access of attackers.

Social Engineering Attacks

- Any human related activities such as bribing, blackmailing, tricking, or espionage
- Current fishing is a typical attack.

Cryptanalysis

- From perspective of information available to attackers
  - Ciphertext only
  - Known plaintext
  - Chosen plaintext
    - “Lunchtime attack”
    - Protocols might encrypt chosen data
  - Adaptively chosen plaintext
  - Related key
  - Forward search (public key crypto)

Safe key space

- How many keys are enough?

Key length	Estimated time
56-64 bits	A few hours or days
112-128 bits	Several decades in the absence of quantum computers
256 bits	Several decades even with quantum computers that run the current known quantum computing algorithms

Exhaustive Key Search times

Key size (bits)	Key space	Execution time (when 1 decypt/us)	Execution time (when 10^6 decypt/us)
32	$2^{32}=4.3X10^9$	2^{31}us=35.8 min	2.15 ms
56	$2^{56}=7.2X10^{16}$	2^{55} us=1142 yrs	10.01 hrs
128	$2^{128}=4.3X10^{38}$	2^{127} us=$5.4X10^{24}$ yr	$5.4X10^{18}$ yrs
168	$2^{168}=4.3X10^{50}$	2^{167} us=$5.9X10^{36}$ yr	$5.9X10^{30}$ yr

Powers of Two Conversion & Useful Units

- $2^n = 10^m$
  $m \sim (n/10) * 3$
  $n \sim (m/3) * 10$
- Fast conversion trick:
  - $2^{10} \sim 10^3$, $2^{20} \sim 10^6$, $2^{30} \sim 10^9$
  - $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, 128, 256, 512
- Seconds per day $\sim 2^{16}$, seconds per year $\sim 2^{25}$
- Schneier's Applied Cryptography, p18
  - Probability to get hit by lightning per day (10^{-10} , 2^{-33})
  - Number of atoms on earth (10^{51} , 2^{170})
  - Number of atoms in the universe (10^{77} , 2^{265})
  - Time until next ice age (14,000, 2^{14} years)
  - Duration until sun goes nova (10^9 , 2^{30} years)
  - Age of the Universe (10^{10} , 2^{33} years)

Confusion and Diffusion

- Claude Shannon: the founder of Information Theory
- He proposed two fundamental concepts:
  - **Confusion** — obscure relationship between key and ciphertext (or plaintext and ciphertext)
  - **Diffusion** — the influence of one plaintext symbol is spread over many ciphertext symbols to hide statistical properties of the plaintext

Cryptography areas