HUST

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

ONE LOVE. ONE FUTURE.

TRƯỜNG ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

LÝ THUYẾT MẬT MÃ

Cryptography Theory

ET3310

PGS. TS. Đỗ Trọng Tuấn
Trường Điện-Điện tử * Đại học Bách Khoa Hà Nội

ONE LOVE. ONE FUTURE.

*?@#%^&

KHOOR

DOO WKH EHVW

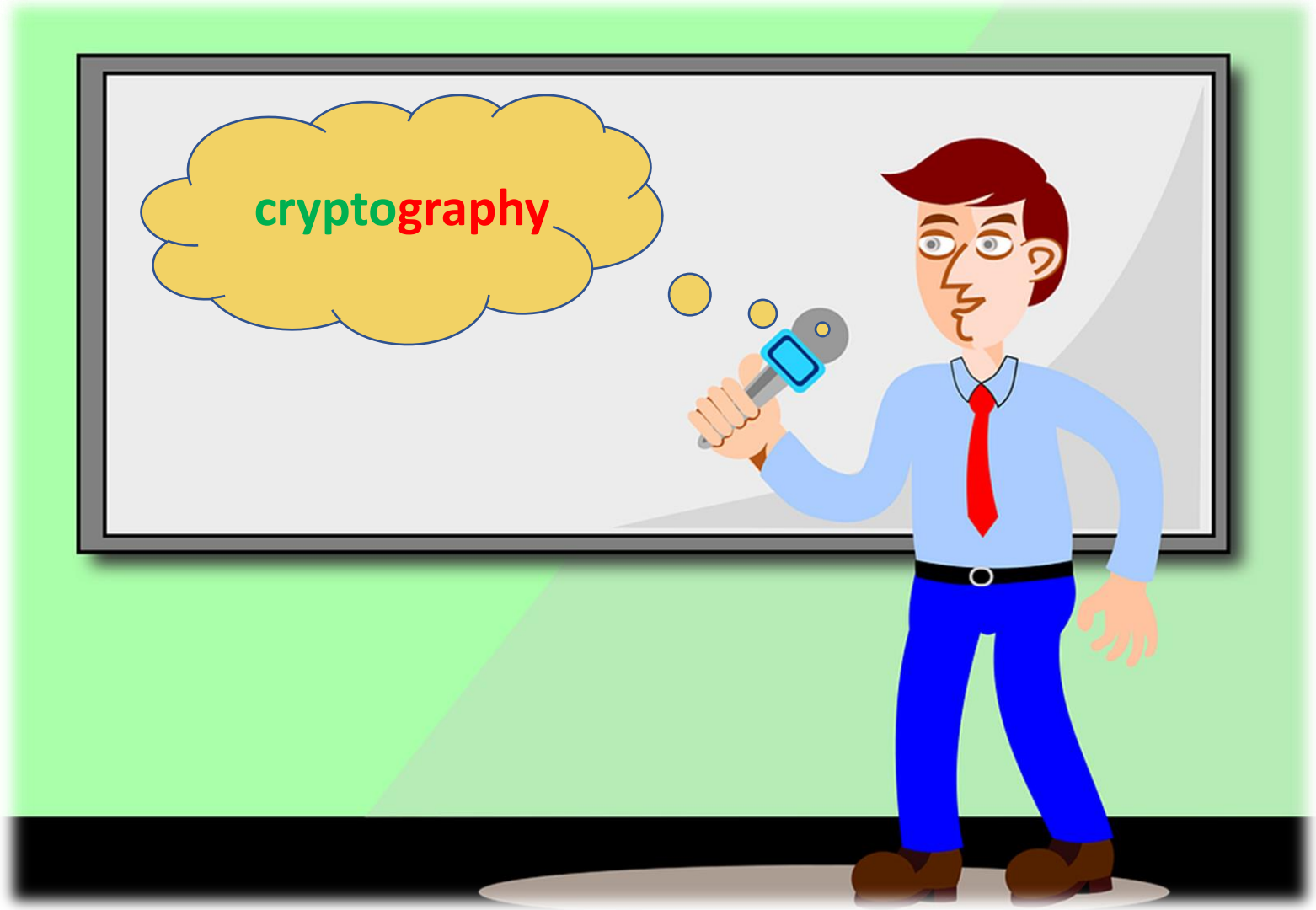
GDV NOHLQH EXFK GHU JURVVHQ OLHEH

*?@#%^&

KHOOR

DOO WKH EHVW

GDV NOHLQH EXFK GHU JURVVHQ OLHEH


cryptography

CRYPTOLOGY - HISTORY + APPLICATIONS

Cryptology (= cryptography + cryptanalysis)
has more than four thousand years long history.

Some historical observation

- People have always had fascination with keeping information away from others.
- Some people – rulers, diplomats, military people, businessmen – have always had needs to keep some information away from others.

Importance of cryptography nowadays

- Applications: cryptography is the key tool to make modern information transmission secure, and to create secure information society.

MAIN DEVELOPMENTS IN CRYPTOGRAPHY

- Wide use of telegraph - 1844.
- Wide use of radio transmission - 1895.
- Wide use of encryption/decryption machines - 1930.
- Wide use of internet.

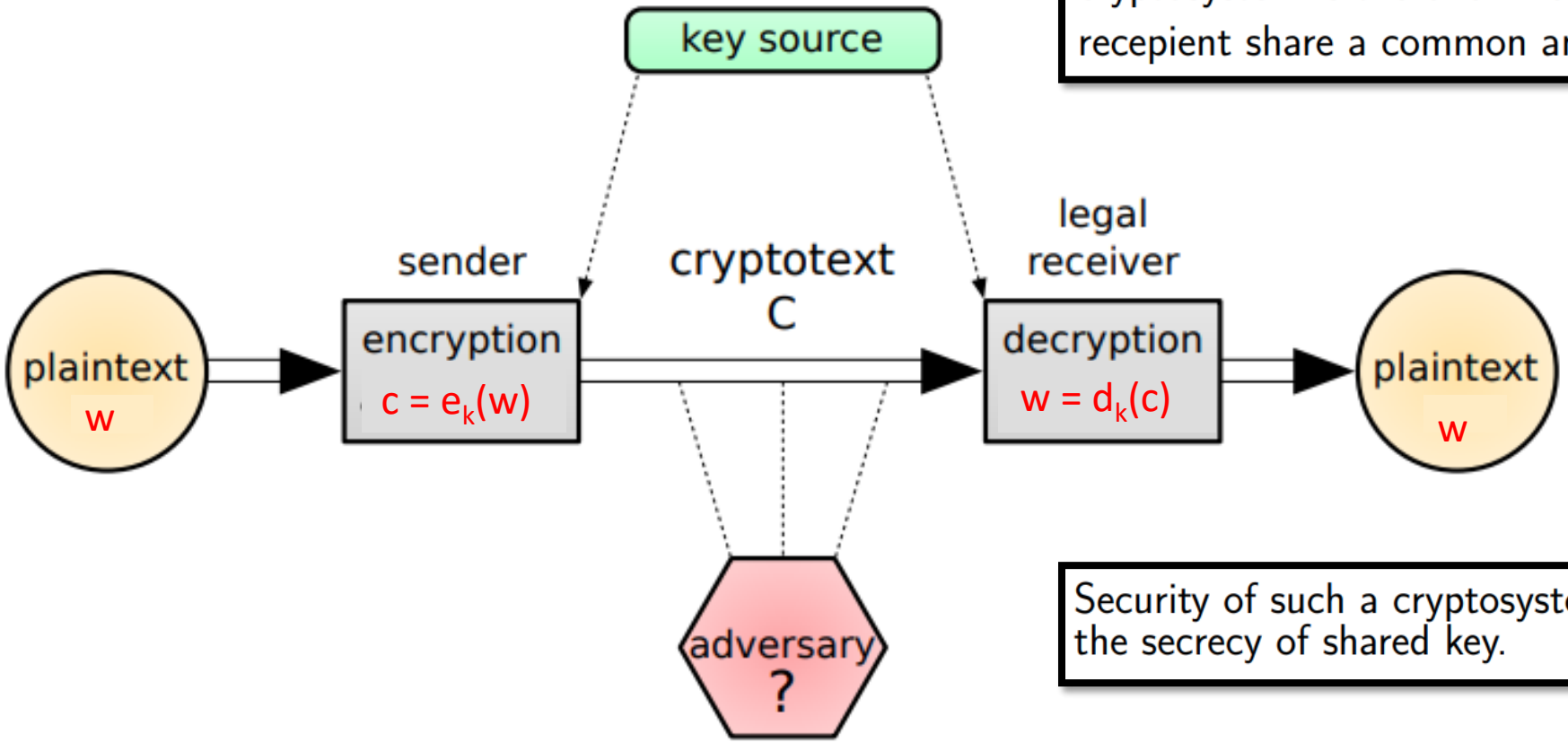
FOUR DEVELOPMENTS THAT CHANGED METHODS and IMPORTANCE of CRYPTOGRAPHY

approaches to cryptography

- Shannon's approach based on information theory (Enemy could not have enough information to break a given cryptosystem).
- Current approach based on complexity theory. (Enemy could not have enough computation power to break a given cryptosystem).

The cryptography deals with problem of sending a message (plaintext, ciphertext, cleartext), through an insecure channel, that may be tapped by an adversary (eavesdropper, cryptanalyst), to a legal receiver.

Secret-key (symmetric) cryptosystems scheme:



A secret-key (private-key or symmetric) cryptosystem is the one where the sender and the recepient share a common and secret key.

Security of such a cryptosystem depends solely on the secrecy of shared key.

COMPONENTS of CRYPTOSYSTEMS:

Plaintext-space: P – a set of plaintexts (messages) over an alphabet $\sum$

Cryptotext-space: C – a set of cryptotexts (ciphertexts) over alphabet Δ

Key-space: K – a set of keys

Each key $k \in K$ determines an **encryption algorithm e_k** and an **decryption algorithm d_k** such that, for any plaintext w, $e_k(w)$ is the corresponding cryptotext and

$$w \in d_k(e_k(w)) \quad \text{or} \quad w = d_k(e_k(w)).$$

SECRET-KEY CRYPTOGRAPHY

Symmetric cryptography relies on three algorithms:

Key generating algorithm which generates a secret key in a cryptographically (pseudo)random way.

Encryption algorithm which transforms a plaintext into a cryptotext using a secret key.

Decryption algorithm which transforms a cryptotext into the original plaintext using the same secret key.

Secret key cryptosystems provide secure transmission of messages along insecure channel provided **the secret keys are transmitted over an extra secure channel.**

SECURITY of CRYPTOSYSTEMS

There are three fundamentally different ways a cryptosystem/cipher can be seen as secure.

Unconditional security: is in the case it can be proven that the cryptosystem cannot be broken no matter how much power has the enemy (eavesdropper).

Computational security is in the case it can be proven that no eavesdropper can break the cryptosystem in polynomial (reasonable) time..

Practical security is in the case no one was able to break the cryptosystem so far after many years and many attempts.

WHO ARE CODEBREAKERS - DEVELOPMENTS

The vision of codebreakers has changed through the history, depending on the tools used for encryption and cryptoanalysis.

- **Old times view:** Cryptology is a **black art** and crypanalysts communicate with **dark spirits** and even are **followers of the devil**.
- **Pre-computers era view:** Codebreakers or cryptanalysts are linguistic alchemists - a mystical tribe attempting to discover meaningful texts in the apparently meaningless sequences of symbols.
- **Current view** Codebreakers and cryptanalysts are artists that can superbly use modern mathematics, informatics and computing supertechnology for decrypting encrypted messages.

CLASSICAL SECRET-KEY CIPHERS

Substitution ciphers: are ciphers where units of plaintext are replaced by parts of cryptotext according a fixed rule.

Simple substitution ciphers operates on single letters.

Monoalphabethic (simple) substitution ciphers: are defined by a single fixed permutation π with encoding

$$e_\pi(a_1 a_2 \dots a_n) = \pi(a_1)\pi(a_2)\dots\pi(a_n)$$

Polyalphabetic (simple) substitutions systems may use different permutations at different positions of the plaintext.

Polygraphic (digraphic) substitution ciphers operate on larger, for instance on the length two) substrings of the plaintext.

Transposition ciphers do not replace but only rearrange order of symbols in the plaintext - sometimes in a complicated way.

CAESAR (100 - 42 B.C.) CRYPTOSYSTEM - SHIFT CIPHER I

SHIFT CIPHER is a simple monoalphabetic cipher that can be used to encrypt words in any alphabet.

In order to encrypt words in English alphabet we use:

Key-space: $K = \{1, 2, \ldots, 25\}$

For any key $k \in K$, the encryption algorithm e_k for SHIFT CIPHER $SC(k)$ substitutes any letter by the letter occurring k positions ahead (cyclically) in the alphabet.

The decryption algorithm d_k for $SC(k)$ substitutes any letter by the one occurring k positions backward (cyclically) in the alphabet.

SHIFT CIPHER $SC(k)$ - $SC(3)$ is called CAESAR SHIFT

Example

$e_2(\text{EXAMPLE}) = \text{GZCORNG},$
$e_3(\text{EXAMPLE}) = \text{HADPSOH},$
$e_1(\text{HAL}) = \text{IBM},$
$e_3(\text{COLD}) = \text{FROG}$

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Example Find the plaintext to the following cryptotext obtained by the encryption with SHIFT CIPHER with $\mathbf{k} = ?$.

Decrypt the cryptotext:

VHFUHW GH GHXA, VHFUHW GH GLHX,
VHFUHW GH WURLV, VHFUHW GH WRXV.

SHIFT CIPHER $SC(k)$ - $SC(3)$ is called CAESAR SHIFT

Example

$e_2(\text{EXAMPLE}) = \text{GZCORNG},$
$e_3(\text{EXAMPLE}) = \text{HADPSOH},$
$e_1(\text{HAL}) = \text{IBM},$
$e_3(\text{COLD}) = \text{FROG}$

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Example Find the plaintext to the following cryptotext obtained by the encryption with SHIFT CIPHER with $\mathbf{k} = ?$.

Decrypt the cryptotext:

VHFUHW GH GHXA, VHFUHW GH GLHX,
VHFUHW GH WURLV, VHFUHW GH WRXV.

Numerical version of $SC(k)$ is defined, for English, on the set $\{0, 1, 2, \ldots, 25\}$ by the encryption algorithm:

$$e_k(i) = (i + k)(mod\ 26)$$

EXAMPLE

Decrypt:

VHFUHW GH GHXA
VHFUHW GH GLHX,
VHFUHW GH WURLV
VHFUHW GH WRXV.

Solution:

Secret de deux
secret de Dieu,
secret de trois
secret de tous.

KERCKHOFF's PRINCIPLE

The basic philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883 by **Jean Guillaume Hubert Victor Francois Alexandre Auguste Kerckhoffs von Nieuwenhof** (1835 - 1903).

The security of a cryptosystem must not depend on keeping secret the encryption algorithm. The security should depend only on *keeping secret the key.*

KERKHOFFS' REQUIREMENTS - 1883

- Cryptotext should be unbreakable in practice.
- Cryptosystem should be convenient for the correspondence.
- The key should be easily remembered and changeable.
- The cryptotext should be transmissible by telegraph.
- The cryptosystem apparatus should be easily portable.
- The encryption machine should be relatively easy to use.

BASIC REQUIREMENTS for GOOD CRYPTOSYSTEMS

1. Given e_k and a plaintext w, it should be easy to compute $c = e_k(w)$.
2. Given d_k and a cryptotext c, it should be easy to compute $w = d_k(c)$.
3. A cryptotext $e_k(w)$ should not be much longer than the plaintext w.
4. It should be unfeasible to determine w from $e_k(w)$ without knowing d_k.
5. The so called avalanche effect should hold: A small change in the plaintext, or in the key, should lead to a big change in the cryptotext (i.e. a change of one bit of the plaintext should result in a change of all bits of the cryptotext, each with the probability close to 0.5).
6. The cryptosystem should not be closed under composition, i.e. not for every two keys k_1, k_2 there is a key k such that

$$e_k(w) = e_{k_1}(e_{k_2}(w)).$$

7. The set of keys should be very large.

(Sir Francis R. Bacon (1561 - 1626))

CRYPTANALYSIS

The aim of cryptanalysis is to get as much information about the plaintext or the key as possible.

Main types of cryptanalytic attacks

1. **Cryptotexts-only attack.** The cryptanalysts get cryptotexts $c_1 = e_k(w_1), \ldots, c_n = e_k(w_n)$ and try to infer the key k,or as many of the plaintexts $w_1, \ldots, w_n$ as possible.

2. **Known-plaintexts attack** (given are some pairs [plaintext, cryptotext]) The cryptanalysts know some pairs $w_i, e_k(w_i), 1 \leq i \leq n$, and try to infer k, or at least w_{n+1} for a new cryptotext $e_k(w_{n+1})$.

Main types of cryptanalytic attacks

3. **Chosen-plaintexts attack** (given are cryptotext for some chosen plaintexts). The cryptanalysts choose plaintexts $w_1, \ldots, w_n$ to get cryptotexts $e_k(w_1), \ldots, e_k(w_n)$, and try to infer k or at least w_{n+1} for a new cryptotext $c_{n+1} = e_k(w_{n+1})$. (For example, if they get temporary access to the encryption machinery.)

4. **Chosen-cryptotext attack (given are plaintexts for some chosen cryptotexts)** The cryptanalysts know some pairs

$$[c_i, d_k(c_i)], \quad 1 \leq i \leq n,$$

where the cryptotexts c_i have been chosen by the cryptanalysts. The aim is to determine the key. (For example, if cryptanalysts get a temporary access to decryption machinery.)

CRYPTANALYSIS

WHAT CAN BAD EVE DO?

Let us assume that a clever Alice sends an encrypted message to Bob.

What can a bad enemy, called usually Eve (eavesdropper), do?

GOALS of CRYPTOGRAPHY

Confidentiality: Eve should not be able to decrypt the message Alice sends to Bob.

Data integrity: Bob wants to be sure that Alice's message has not been altered by Eve.

Authentication: Bob wants to be sure that only Alice could have sent the message he has received.

Non-repudiation: Alice should not be able to claim that she did not send messages that she has sent.

Anonymity: Alice does not want Bob to find out who sent the message

M A T H S

Groups Z_n and Z_n^*

GROUPS

ORDER oF GROUPS

PROPERTIES of the GROUP Z_n^*

FINITE FIELDS

RINGS and FIELDS

NUMBER THEORY

MODULO OPERATIONS

EXTENDED EUCLID ALGORITHM

GROUPS

A **group** G is a set of elements and an operation, call it *, with the following properties:

- G is closed under *; that is if $a, b \in G$, so is $a * b$.
- The operation * is associative $(a * (b * c) = (a * b) * c$, for any $a, b, c \in G$.
- G has an identity element e such that $e * a = a * e = a$ for any $a \in G$.
- Every element $a \in G$ has an inverse $a^{-1} \in G$, so that $a * a^{-1} = a^{-1} * a = e$.

A group G is called **Abelian group** if the operation $*$ is commutative ($a * b = b * a$ for any $a, b \in G$). **Example** Which of the following sets is an (Abelian) group:

- The set of real numbers with $*$ being: (a) addition; (b) multiplication.
- The set of matrices of degree n and an operations (a) addition; (b) multiplication.
- What happens if we consider only matrices with determinants not equal zero?

GROUPS

Two integers a, b are congruent modulo n if

$$a \mod n = b \mod n.$$

Notation: $a \equiv b(\mod n)$
Let $+_n, \times_n$ denote addition and multiplication modulo n

Groups Z_n and Z_n^*

$$a +_n b = (a + b) \mod n$$

$$a \times_n b = (ab) \mod n$$

$\mathbf{Z_n} = \{0, 1, \ldots, n-1\}$ is a group under the operation $+_n$.

$\mathbf{Z_n^\star} = \{x | 1 \leq x \leq n, \gcd(x, n) = 1\}$ is a group under the operation $\times_n$

$\mathbf{Z_n^\star}$ is a field under the operations $+_n, \times_n$ if n is a prime
Theorem For any n, the multiplicative inverse of any $m \in \mathbf{Z_n^\star}$ can be computed in polynomial time.
Comment: Computation can be done by the extended Euclid algorithm.
Theorem In the group $(\mathbf{Z_n^\star}, \times_n)$ the exponentiation can be performed in polynomial time.

GROUPS

ORDER oF GROUPS

- If a is an element of a finite group G, then its **order** is the smallest integers k such that $a^k = 1$.
- Order of each element of a group G is a divisor of the number of elements of G.
- This implies that every element $a \in \mathbf{Z}_p^*$, where p is a prime, has order $p - 1$ and it holds

$$a^{p-1} \equiv 1 \pmod{p}$$

Definition (1) For any group $(G, \circ)$ and any $x \in G$

$$\text{order of } x = \min\{k > 0 | x^k = 1\}$$

(2) The group $(G, \circ)$ is called cyclic if it contains an element g, called generator, such that the order of $(g) = |G|$.

Theorem If the multiplicative group $(Z_n^\star, \times_n)$ is cyclic, then it is isomorphic to the additive group $(Z_{\Phi(n)}, +_{\Phi(n)})$. (However, no effective way is known, given n, to create such an isomorphism!)

Theorem The mutliplicative group $(Z_n^\star, \times_n)$ is cyclic iff n is either $1, 2, 4, p^k$ or $2p^k$ for some $k \in N^+$ and an odd prime $p > 2$.

Theorem Let p be a prime. Given the prime factorization of $p-1$ a generator for group $(Z_p^\star, \times_p)$ can be found in polynomial time by a randomized algorithm.

Proof (1) Pick randomly $x \in Z_p^\star$ and checks whether its order is $p-1$. If yes, it is a generator. The probability to find a generator in a single trial is

$$\frac{\Phi(p-1)}{p-1} = \Omega\left(\frac{1}{p}\right).$$

How to check whether the order of x is $p-1$? Let $p_1, \ldots, p_t$ be different prime factors of $p-1$. If order of $x < p-1$, then the order of x has to be proper divisor of $p-1$, that is for some p_i,

$$\text{order of} x \left| \frac{p-1}{p_i} \right.$$

RINGS and FIELDS

A **ring** R is a set with two operations $+$ (addition) and $\cdot$ (multiplication) , with the following properties:

- R is closed under $+$ and $\cdot$.
- R is an Abelian group under $+$ (with the unity element for addition called **zero**).
- The associative law for multiplication holds.
- R has an identity element 1 for multiplication
- The distributive laws hold $(a \cdot (b + c) = a \cdot b + a \cdot c$ a $(b + c) \cdot a = b \cdot a + c \cdot a)$ a for all $a, b, c \in R$.

A ring is called **commutative ring** if multiplication is commutative

RINGS and FIELDS

A **field** F is a set with two operations $+$ (addition) and $\cdot$ (multiplication) , with the following properties:

- F is a commutative ring.
- Non-zero elements of F form an Abelian group with respect to multiplication.

A non-zero element g is a **primitive element** of a field F if all non-zero elements of F are powers of g.

FINITE FIELDS

Theorem If p is a prime, then the integers mod p, $GF(p)$, constitute a field. Every finite field F contains a subfield that is $GF(p)$, up to relaabeling, for some prime p and $p \cdot \alpha = 0$ for every $\alpha \in F$.

If a field F contains the prime field $GF(p)$, then p is called the **characteristic** of F.

Theorem (1) Every finite field F has p^m elements for some prime p and some m.
(2) For any prime p and any integer m there is a unique (up to isomorphism) field of p^m elements $GF(p^m)$.
(3) If $f(x)$ is an irreducible polynomial of degree m in $F_p[x]$, then the set of polynomials in $F_p[x]$ with additions and multiplications modulo $f(x)$ is a field with p^m elements.

FINITE FIELDS

There are two important ways GF(4), the Galois field of four elements, is realized.

1. It is easy to verify that such a field is the set

$$\mathrm{GF}(4) = \{0, 1, \omega, \omega^2\}$$

with operations $+$ and $\cdot$ satisfying laws

- $0 + x = x$ for all x;
- $x + x = 0$ for all x;
- $1 \cdot x = x$ for all x;
- $\omega + 1 = \omega^2$

2. Let $\mathbf{Z}_2[x]$ be the set of polynomials whose coefficients are integers mod 2. GF(4) is also $\mathbf{Z}_2[x] \pmod{x^2 + x + 1}$ therefore the set of polynomials

$$0, 1, x, x + 1$$

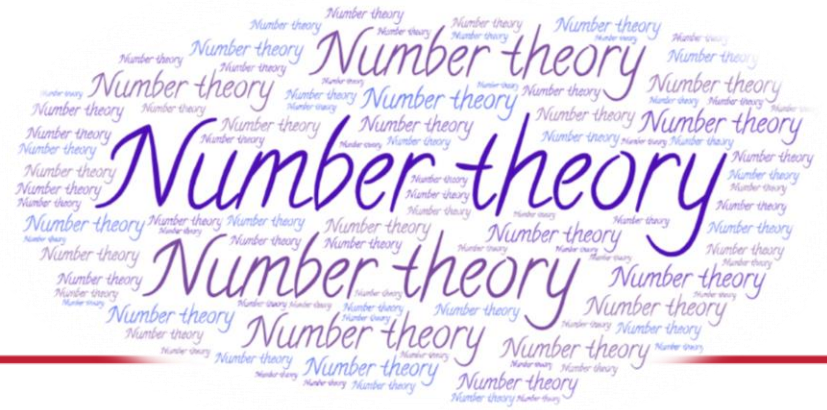
where addition and multiplication are $\pmod{x^2 + x + 1}$.

3. Let p be a prime and $\mathbf{Z}_p[x]$ be the set of polynomials with coefficients mod p. If $p(x)$ is a irreducible polynomial mod p of degree n, then $\mathbf{Z}_p[x] \pmod{p(x)}$ is a $\mathrm{GF}(p^n)$ with p^n elements.

NUMBER THEORY

The number theory concepts, methods and results introduced in the following play an important role in modern considerations concerning cryptography, cryptographic protocols and randomness.

The key concept is that of primality. The key methods are based on randomized algorithms.



NUMBER THEORY

CEILING and FLOOR FUNCTIONS

Flour $\lfloor x \rfloor$ – the largest integer $\leq x$

Ceiling $\lceil x \rceil$ – the smallest integer $\geq x$

Example

$$\lfloor 3.14 \rfloor = 3 = \lfloor 3.75 \rfloor \quad \lfloor -3.14 \rfloor = -4 = \lfloor -3.75 \rfloor$$
$$\lceil 3.14 \rceil = 4 = \lceil 3.75 \rceil \quad \lceil -3.14 \rceil = -3 = \lceil -3.75 \rceil$$

$$\lceil x \rceil - \lfloor x \rfloor = ?$$

NUMBER THEORY

MODULO OPERATIONS

The remainder of n when divided by m is defined by

$$n \mod m = \begin{cases} n - m\left\lfloor \frac{n}{m} \right\rfloor & m \neq 0 \\ 0 & m = 0 \end{cases}$$

Example $7 \mod 5 = 2 \qquad 122 \mod 11 = 1$

Identities

$$(a + b) \mod n = ((a \mod n) + (b \mod n)) \mod n$$
$$(a \cdot b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n$$
$$a^b \mod n = ((a \mod n)^b) \mod n.$$

NUMBER THEORY

MODULO OPERATIONS

Identities

$$(a+b) \mod n = ((a \mod n) + (b \mod n)) \mod n$$
$$(a \cdot b) \mod n = ((a \mod n) \cdot (b \mod n)) \mod n$$
$$a^b \mod n = ((a \mod n)^b) \mod n.$$

Example

$$3^{123456789} \mod 26 = ?$$

EUCLID ALGORITHM for GCD

This is algorithm to compute greatest common divisor (gcd) of two integers, in short

to compute $gcd(m, n), 0 \leq m < n$

$$\begin{aligned} \gcd(0, n) &= n \\ \gcd(m, n) &= \gcd(n \mod m, m) \text{ for } m > 0 \end{aligned}$$

Example $gcd(296, 555) = gcd(259, 296) = gcd(37, 259) = gcd(0, 37) = 37$

because

$$555 = 1 \times 296 + 259$$

$$296 = 1 \times 259 + 37$$

$$259 = 7 \times 37 + 0$$

NUMBER THEORY

EXTENDED EUCLID ALGORITHM

Theorem For all $0 < m < n$ there exist integers x and y such that

$$\gcd(m, n) = xm + yn.$$

Moreover, x and y can be computed in polynomial time.

Example: If $m = 0$, then $x = 0, y = 1$.
If $m > 0$, take $r = n \mod m$ and compute recursively x', y' such that

$$x'm + y'r = \gcd(r, m).$$

Since $r = n - \left\lfloor \frac{n}{m} \right\rfloor m$ we have:

$$\gcd(m, n) = x'm + y'\left(n - \left\lfloor \frac{n}{m} \right\rfloor m\right) = \left(x' - y'\left\lfloor \frac{n}{m} \right\rfloor\right) m + y'n$$


ENCRYPTION
NETWORK
PROGRAMMING
STANDARDS
INTERNET
PROJECT MANAGEMENT
INTERFACE
DEFINITION
BOARD
ANALYSIS
SOURCING
CONNECTION
GUI
CSS
SUPPORT
CLASSES
RANDOM
ROUTER
QUALITY
INSTRUCTIONS
HARDDISK
SWITCH
HOST
CONDITION
MARKUP
COMPUTER
OPERATING
LINK


Cryptography
with Python

Conversion Table

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

M A T H S

12, 0, 19, 7, 18

modulo 26

$$E(x) \equiv ax + b \pmod{26}$$

$$E(x) \equiv 3x + 1 \pmod{26}$$

11, 1, 6, 22, 3

L B G W D

Conversion table

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

LBGWD

$E(x) \equiv 3x+1 \pmod{26}$

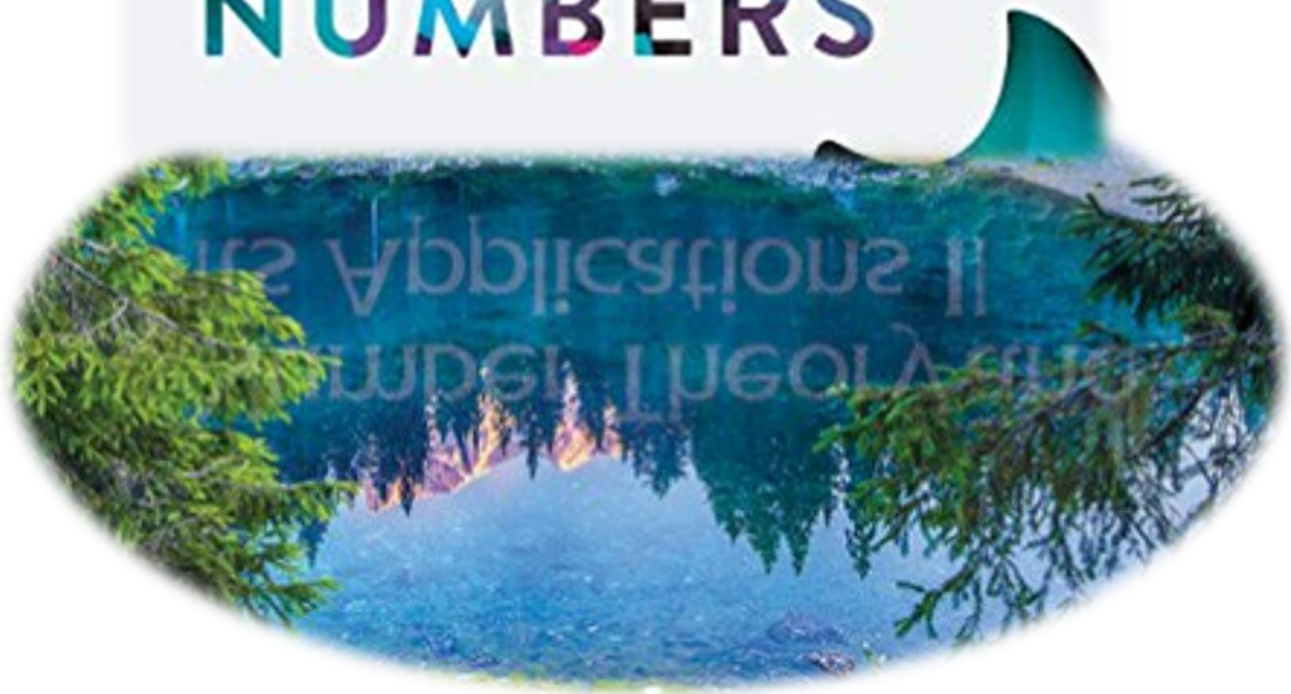
$D(y) \equiv 9(y-1) \pmod{26}$

11, 1, 6, 22, 3

12, 0, 19, 7, 18

MATHS

THE UNIVERSE SPEAKS IN NUMBERS



Butterfly
by Unknown Author
Museu do Amanhã

HUST

hust.edu.vn fb.com/dhbkhn

THANK YOU !