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

Shannon theory and Symmetric Cipher

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

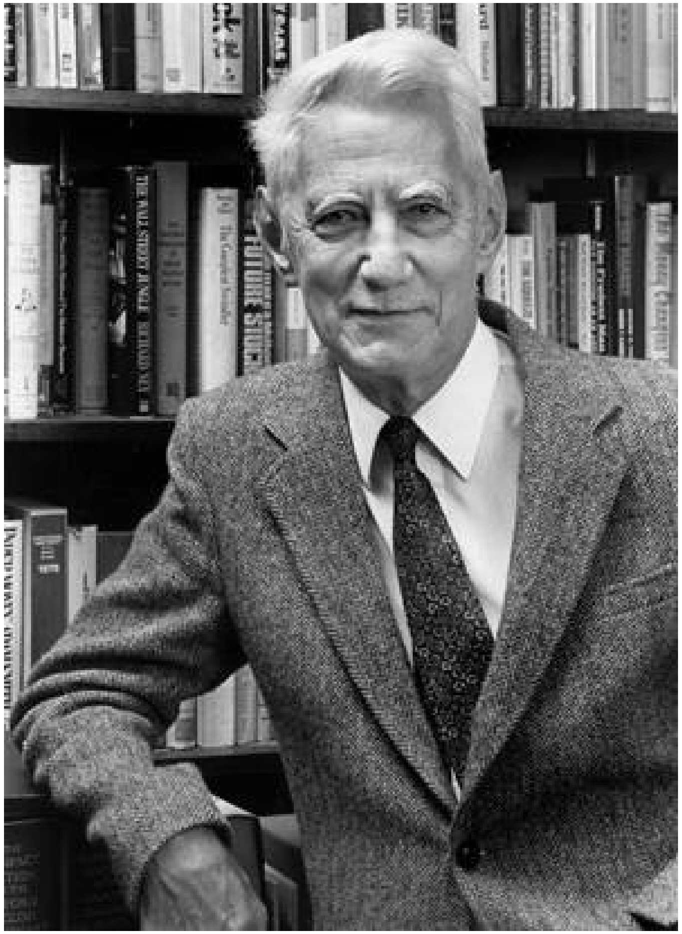
fit@hcmus

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

fit@hcmus

Contents

- Introduction - Claude Shannon
- Perfect security
- Entropy
- Combination of crypto-systems



Claude E. Shannon (1916-2001)

http://www.wisdom.weizmann.ac.il/~naor/COURSE/GiladTsur_YossiOren_ShannonSecrecy.ppt

Probability

- Let X and Y be two random variables.
- Definition:
  - $p(x) = p(X = x)$ is a probability of X receiving value x
  - $p(y) = p(Y = y)$ is a probability of Y receiving value y
  - $p(x \mid y)$ is a probability of X receiving value x if Y receives value y (conditional probability)
- X and Y are independent random variables if only if $p(x, y) =$ $p(x)$ 흐 $p(y)$ for any value x of X and value y of Y

Probability

- Example: consider tossing 2 dices
  - We have result-space Ω = {(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),

    (2,1),(2,2),(2,3),(2,4),(2,5),(2,6),

    (3,1),(3,2),(3,3),(3,4),(3,5),(3,6),

    (4,1),(4,2),(4,3),(4,4),(4,5),(4,6),

    (5,1),(5,2),(5,3),(5,4),(5,5),(5,6),

    (6,1),(6,2),(6,3),(6,4),(6,5),(6,6)}
  - $|\Omega|$ = 36 elements, for $w \in \Omega \mapsto X(w)$
  - Let X (based on Ω) be sum of two dices => $X(w) \in$ {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}

Probability

- Example: consider tossing 2 dices
  - We have result-space Ω = {(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),

    (2,1),(2,2),(2,3),(2,4),(2,5),(2,6),

    (3,1),(3,2),(3,3),(3,4),(3,5),(3,6),

    (4,1),(4,2),(4,3),(4,4),(4,5),(4,6),

    (5,1),(5,2),(5,3),(5,4),(5,5),(5,6),

    (6,1),(6,2),(6,3),(6,4),(6,5),(6,6)}
  - $|\Omega|$ = 36 elements, for $w \in \Omega$
  - Let X (based on Ω) be sum of 2 dices => $X(w) \in$ {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}
- Notation of mapping X: $\Omega \to \mathbb{R}$

  $w \mapsto X(w)$
- Consider $X(w) = 4 \Leftrightarrow$ Event of tossing 2 dices has 4 points
  - We have **Pr**[$X(w) = 4$] = 3/36, due to {{1, 3}, {2, 2}, {3, 1}}, denote **Pr**[$X = 4$]

Probability

- Example: consider tossing 2 dices
  - We have result-space $\Omega = \{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),$

    $(2,1),(2,2),(2,3),(2,4),(2,5),(2,6),$

    $(3,1),(3,2),(3,3),(3,4),(3,5),(3,6),$

    $(4,1),(4,2),(4,3),(4,4),(4,5),(4,6),$

    $(5,1),(5,2),(5,3),(5,4),(5,5),(5,6),$

    $(6,1),(6,2),(6,3),(6,4),(6,5),(6,6)\}$
  - $|\Omega| = 36$ elements, for $w \in \Omega$
  - Let Y (based on Ω) be the result of tossing 2 dices with the same point => $Y(w) \in$ {"2 same points", "2 different points"}

    $w \mapsto Y(w)$
  - Should change "2 same points" to 1, & "2 different points" to 0 => $Y(w)$

Probability

- Example: consider tossing 2 dices
  - We have result-space Ω = {(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),

    (2,1),(2,2),(2,3),(2,4),(2,5),(2,6),

    (3,1),(3,2),(3,3),(3,4),(3,5),(3,6),

    (4,1),(4,2),(4,3),(4,4),(4,5),(4,6),

    (5,1),(5,2),(5,3),(5,4),(5,5),(5,6),

    (6,1),(6,2),(6,3),(6,4),(6,5),(6,6)}
  - $|\Omega|$ = 36 elements, for $w \in \Omega$

    $w \mapsto Y(w)$
  - Let Y (based on Ω) be the result of tossing 2 dices with the same point => $Y(w) \in$ {"2 same points", "2 different points"}
  - Should change "2 same points" to 1, & "2 different points" to 0 => $Y(w) \in$ {0, 1}
- Notation of mapping Y: $\Omega \to \mathbb{R}$

Bayes theorem

- Let X and Y be two random variables

$$p(x, y) = p(x \mid y) \times p(y) = p(y \mid x) \times p(x)$$

- Bayes theorem

Apriori

$$\text{if } p(y) > 0 \Rightarrow p(x \mid y) =$$

Aposteriori

- Corollary: X and Y are two independent ones $\Leftrightarrow$ $p(x \mid y) = p(x)$, $\forall\, x, y$

Bayes theorem

- Reconsider: example of tossing 2 dices
  - We have result-space Ω = {(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),

    …

    (6,1),(6,2),(6,3),(6,4),(6,5),(6,6)}
  - $|\Omega|$ = 36 elements, for $w \in \Omega$
  - X: Sum of points of 2 dices => $X(w) \in$ {2, 3, 4, …, 12}
  - Y: 2 dices with the same point => $Y(w) \in$ {0, 1}
- Compute **Pr**[$Y = 1|X = 4$] (Probability of 4-point with 2 same faces)
  - **Pr**[$X = 4$] = 3/36 => **Pr**[$Y = 1|X = 4$] = 1/3 due to {(1, 3), (2, 2), (3, 1)}
- Compute **Pr**[$X = 4|Y = 1$] (Probability of 4-point with 2 same faces)
  - **Pr**[$Y = 1$] = 6/36 => **Pr**[$X = 4|Y = 1$] = 1/6 due to {(1, 1), (2, 2), …, (6, 6)}
- So **Pr**[$Y = 1|X = 4$] $\times$ **Pr**[$X = 4$] = **Pr**[$X = 4|Y = 1$] $\times$ **Pr**[$Y = 1$]

Context of cryptography

- Some probabilistic notation for crypto-context
  - $p_P(x)$: Probability of appearing plaintext x
  - $p_K(k)$: Probability of choosing key k
  - $p_C(y)$: Probability of ciphertext receiving value y
- Note:
  - Notations p_P, p_K and p_C are the probabilities for each distinct set
  - It can be assumed that the key value k and the plaintext x are independent events
- From the probability distribution of plaintext and key on the set P and K, we can determine the conditional probability distribution of plaintext ???

Context of cryptography

- For each $k \in K$, let $C(k) = \{e_k(x) \mid x \in P\}$ be the set of cipher-text if encrypting plain-text $x \in P$ with key $k \in K$.
- So, we see that probability of cipher-text y is sum of probabilities of choosing k and $x = d_k(y)$.

$$p_C(y) =$$

- For each $y \in C$ and $x \in P$, $p_C(y \mid x)$ is probability of receiving cipher-text y when plain-text is x.

Thực chất là xác suất chọn các khóa k

$$p_C(y \mid x) =$$

- Using Bayes theorem to compute $p_P(x \mid y)$

$$p_P(x \mid y) = \quad =$$

Example

- Let $P = \{a, b\}$ with $p_P(a) = 1/4$, $p_P(b) = 3/4$
- Let $K = \{k_1, k_2, k_3\}$ with $p_K(k_1) = 1/2$, $p_K(k_2) = p_K(k_3) = 1/4$
- Let $C = \{1, 2, 3, 4\}$
- Let E be a set of encryption rules
  - $e_{k1}(a) = 1$, $e_{k1}(b) = 2$
  - $e_{k2}(a) = 2$, $e_{k2}(b) = 3$
  - $e_{k3}(a) = 3$, $e_{k3}(b) = 4$

⇨

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

- Let D be a set of decryption rules
  - $d_{k1}(1) = a$, $d_{k1}(2) = b$
  - $d_{k2}(2) = a$, $d_{k2}(3) = b$
  - $d_{k3}(3) = a$, $d_{k3}(4) = b$

⇨

	1	2	3	4
k_1	a	b		
k_2		a	b	
k_3			a	b

Example

- Compute $p_C(y)$
  - $p_C(y = 1) = ¼ \times ½ = 1/8$
  - $p_C(y = 2) = ½ \times ¾ + ¼ \times ¼ = 7/16$
  - $p_C(y = 3) = ¼ \times ¾ + ¼ \times ¼ = ¼$
  - $p_C(y = 4) = ¼ \times ¾ = 3/16$
- Condition probability of $p_P(x \mid y)$
  - $p_P(x = a \mid y = 1) = \; = \; = 1$
  - $p_P(x = b \mid y = 1) = \; = \; = 0$
  - $p_P(x = a \mid y = 2) = \; = \; =$
  - $p_P(x = b \mid y = 2) = \; = \; =$

1

2

	a $p_P = ¼$	b $p_P = ¾$
k_1 ($p_K = ½$)	1	2
k_2 ($p_K = ¼$)	2	3
k_3 ($p_K = ¼$)	3	4

$$p_P(x = a|y = 3) = \frac{p_P(x=a)\times p_C(y=3|x=a)}{p_C(y=3)} = \frac{\frac{1}{4}\times\frac{1}{4}}{\frac{1}{4}} = ¼$$

$$p_P(x = b|y = 3) = \frac{p_P(x=b)\times p_C(y=3|x=b)}{p_C(y=3)} = \frac{\frac{3}{4}\times\frac{1}{4}}{\frac{1}{4}} = ¾$$

3

$$p_P(x = a|y = 4) = \frac{p_P(x=a)\times p_C(y=4|x=a)}{p_C(y=4)} = \frac{\frac{1}{4}\times 0}{\frac{3}{16}} = 0$$

$$p_P(x = b|y = 4) = \frac{p_P(x=b)\times p_C(y=4|x=b)}{p_C(y=4)} = \frac{\frac{3}{4}\times\frac{1}{4}}{\frac{3}{16}} = 1$$

4

Perfect security

- **Perfectly secure**?
- Significance: The attacker gets nothing from the ciphertext

$$\forall x \in P, k \in K, p_P(x \mid c) = p_P(x), p_K(k \mid c) = p_K(k)$$

- Evaluate Shift-cipher
  - Assume 26 keys in Shift-cipher are randomly chosen with uniform probability (1/26)
  - With set of plaintext having any probability distribution, Shift-cipher achieve perfect security???
  - Let $P = C = K = Z_{26} = \{0, 1, 2, \ldots, 25\}$
  - $e_k(x) = (x + k) \bmod 26$ and $d_k(y) = (y - k) \bmod 26$

Perfect security (on Shift Cipher)

- Probability

$p_C(y) = \quad =$

$=$

- Given y, when changing k from 0 to 25, we receive all 26 values of $\mathbb{Z}_{26}$.

$= \quad = 1$

- So, for all $y \in \mathbb{Z}_{26}$, we have $p_C(y) = 1/26$ (1)
- For (x, y), we have only one key $k \in \mathbb{Z}_{26}$, such that $y = x + k \bmod 26$. Hence, $p_C(y \mid x) = p_K(y - x \bmod 26) = 1/26$ (2)

Perfect security (on Shift Cipher)

- From (1) and (2), apply Bayes theorem we have:

  $$p_P(x \mid y) = \;=\; = p_P(x) \text{ (satisfy standard)}$$

- Shift cipher is perfect security if randomly choosing a new k for each plain-text x.
- From Bayes theorem, we have $p_P(x \mid y) = p_P(x), x \in P, y \in C$
  - This is similar to: $p_C(y \mid x) = p_C(y), x \in P, y \in C$
  - Assume $p_C(y) > 0, y \in C$ (All members of C are used)
  - Crypto-system is secure if $p_C(y \mid x) > 0, x \in P, y \in C \Rightarrow |C| \geq |P|$
  - Due to $p_C(y \mid x) > 0 \Rightarrow k \in K: e_k(x) = y \Rightarrow |K| \geq |C|$
- For the system to be perfect security, key-size used to encrypt must be at least equal to the size of the message to be encrypted: $|K| \geq |P|$

Vernam Cipher

- Is there a perfect secure crypto-system with |K| = |P|?
- Shannon theorem: Let (P, K, C, E, D) be a crypto-system with |K| = |P| = |C|. So, it is perfect secure if and only if:
  - $c \in$ C, $x \in$ P, $k \in$ K: $e_k(x) = c$ (1)
  - $k \in$ K, $p_K(k) = 1/|K|$ (2)
- Proof: Let (P, K, C, E, D) be a crypto-system with |K| = |P| = |C|. Due to its perfect security, we have
  - $x \in$ P, $p_P(x \mid c) = p_P(x)$ and Bayes theorem allows $p_C(c \mid x) = p_C(c)$
  - $!k \in$ K: $e_k(x) = c$ for (x, c), due to |K| = |P| = |C|
  - Fix c, for all x_i, let k_i be key such that $(x_i) = c$
  - From Bayes theorem: $p_P(x_i \mid c) = \;=$
  - Due to $p_P(x_i \mid c) = p_P(x_i)$ $=$ $p_K(k_i) = p_C(c)$.

Vernam Cipher

- Gilbert Vernam (Bell Labs) proposed in 1919
  - A key is a “long enough” random sequence of values. So, $C = P \oplus K$
  - This method is proven to be perfect security
  - Limitation: the key is too long and cannot be reused
  - Advantage: simple
- Description:
  - Let integer $n \geq 1$, and $P = C = K = (\mathbb{Z}_2)^n$. For each $k \in (\mathbb{Z}_2)^n$, we let:
    - $e_k(x) = (x_1 + k_1, \ldots, x_n + k_n)$ mod 2, where $x = (x_1, \ldots, x_n)$ and $k = (k_1, \ldots, k_n)$.
    - $d_k(y) = (y_1 + k_1, \ldots, y_n + k_n)$ mod 2, where $y = (y_1, \ldots, y_n)$
- Note: operator (+ mod 2) is $\oplus$-bit

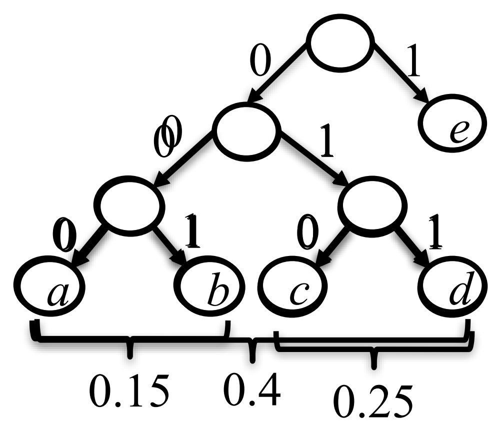
Informatic theory

- Some events are random but more common than others
- Some facts are more important than others
- Entropy is a measure of the uncertainty of a random variable, or the amount of information each event provides
- If X is a random variable receiving values in X, so $H(X)$ = -
- Note: $lim_{x \to 0}(x \times \mathbf{log_2 x}) = 0$
  - $lim_{x \to 0}(x \times \mathbf{log_2 x}) =$
  - With L' Hopital, we have $= \; = \; = 0$

Entropy and Huffman encoding

- Recall the idea of Huffman encoding
- Example: we have $X = \{a, b, c, d, e\}$ with probabilities $p(a) = .05$, $p(b) = .10$, $p(c) = .12$, $p(d) = .13$ and $p(e) = .60$

<table>
<tr><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td></tr>
<tr><td>.05</td><td>.1</td><td>.12</td><td>.13</td><td>.6</td></tr>
<tr><td>0</td><td>1</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">.15</td><td>.12</td><td>.13</td><td>.6</td></tr>
<tr><td colspan="2"></td><td>0</td><td>1</td><td></td></tr>
<tr><td colspan="2">.15</td><td colspan="2">.25</td><td>.6</td></tr>
<tr><td colspan="2">0</td><td colspan="2">1</td><td></td></tr>
<tr><td colspan="4">.4</td><td>.6</td></tr>
<tr><td colspan="4">0</td><td>1</td></tr>
<tr><td colspan="5">1</td></tr>
</table>



Huffman tree

x	$f(x)$
a	000
b	001
c	010
d	011
e	1

Prefix-code

Entropy and Huffman encoding

- Average length to transmit information for an event

$$l(f) = \underbrace{0.05 \times 3}_{`a'} + \underbrace{0.1 \times 3}_{`b'} + \underbrace{0.12 \times 3}_{`c'} + \underbrace{0.13 \times 3}_{`d'} + \underbrace{0.6 \times 1}_{`e'} = 1.8$$

- Entropy:

$$H(X) = \overbrace{0.05 \times \log_2(0.05)}^{0.2161} + \overbrace{0.1 \times \log_2(0.1)}^{0.3322} + \overbrace{0.12 \times \log_2(0.12)}^{0.3671}$$

$$+ \underbrace{0.13 \times \log_2(0.13)}_{0.3842} + \underbrace{0.6 \times \log_2(0.6)}_{0.4422}$$

$$= 1.7402$$

- Result: $H(X) \le l(f) \le H(X) + 1$

Properties of Entropy

- Basic properties
  - $H(X) \geq 0$, equality occurs if and only if the variable X is constant
  - $H(X) \leq \log_2|X|$, equality occurs if and only if $p(X = x) = 1/|X|$
  - $H(X, Y) \leq H(X) + H(Y)$, '=' occurs $\Leftrightarrow$ X & Y are independent distribution
  - $H(X|Y) \leq H(X)$, equality occurs $\Leftrightarrow$ X & Y are independent distribution
  - **Chain Rule:** $H(X, Y) = H(X|Y) + H(Y)$
- Entropy of components of crypto-system
  - $H(C|K) = H(P)$
  - $H(C|P, K) = H(P|C, K) = 0$
  - $H(P, K) = H(P) + H(K)$
  - $H(C) \geq H(P)$
  - $H(C, P, K) = H(C, K) = H(P, K)$
  - $H(K|C) = H(K) + H(P) - H(C)$ và $H(K|C^n) = H(K) + H(P^n) - H(C^n)$

Comments

- There are 26! $\approx 10^{26}$ encryption rule (substitution) for English text (includes normal characters)
- Equivalent to 88-bit security → why is it easy to be attacked in practice?
- Shannon: All approaches of mono-alphabetic cipher of English are easy to break if having 25 characters of cipher-text.

Language's unicity distance

- Spurious keys: if using shift-cipher, we have cipher-texts "WNAJW"
  - There may be 5 and 22 to decrypt "RIVER" and "ARENA"
  - One of them is wrong
- Introduction of random variables
  - Let $P \in \mathcal{P} = \{a, b, \ldots, z\}$ ($|\mathcal{P}| = 26$): set of characters
  - Let $P^2 \in \mathcal{P}^2 = \{aa, \ldots, zz\}$ ($|\mathcal{P}^2| = 26^2$): set of digraphs
  - …
  - Let $P^n \in \mathcal{P}^n = \{a\ldots a, \ldots, z\ldots z\}$ ($|\mathcal{P}^2| = 26^n$): set of *n*-graphs

Language's unicity distance

- Some notations
  - $p(\mathrm{i})$ is probability of appearing of character 'i'
  - $p_{\mathrm{i}}(j)$ is probability of appearing of character 'j' when 'i' appears
  - $p(i, j)$ is probability of appearing of 2 characters 'i' and 'j'
- Example: compute entropy of P ㅍ P ={a, b, …, z} (|P | = 26)
  - $H(P)$ = - ㄹㅁ 4.14 bits/character (real data)
- Example: compute entropy of P^2 ㅍ P ^{2}= {aa, …, zz} (|P ^{2}| = 26^2)
  - $H(P^2)$ = - ㄹㅁ 7.7 bits
- Formular to compute entropy (for each character) of another language 'L': H_{L} =
- Let R_{L} = 1 - (Rate of "spurious elements" of a language 'L')

Language's unicity distance

- Due to $H_L = , H(P^n)$ ㄹㅁ n ㅎ $H_L = n$ ㅎ $(1 - R_L)$ ㅎ $\log_2|P|$
- Due to $|P| = |C|$, $H(C^n)$ ㅓㅣ n ㅎ $H(C)$ ㅓㅣ n ㅎ $\log_2|C| = n$ ㅎ $\log_2|P|$
  - Where P and C are sets of plain-texts and cipher-texts
  - K is a set of keys
- We have $H(K|C^n) = H(K) + H(P^n) - H(C^n)$

ㄹㅁ $H(K) + n$ ㅎ $(1 - R_L)$ ㅎ $\log_2|P| - n$ ㅎ $\log_2|P|$

$= H(K) - n$ ㅎ R_L ㅎ $\log_2|P|$ ㅓㅣ $\log_2|K| - n$ ㅎ R_L ㅎ $\log_2|P|$

- Crypto-system is broken when:

$H(K|C^n) = 0$ ㅡㅣ $\log_2|K| - n$ ㅎ R_L ㅎ $\log_2|P| = 0$ ㅡㅣ $n =$

  - Means: entropy of random variable K when C^n is zero ㅡ there is only one key to decrypt.

Language's unicity distance

- Unicity of crypto-system is n_0 such that a number of spurious-key are zero
- English case: (|P| = 26, R_L = 0.75, |K| = 26! due to using substitution cipher)

$$n_0 = = \; 25 \text{ (Language distance)}$$

- Mean that: need a cipher-text with at least length of 25 characters to ensure that there exists only one key

Comments

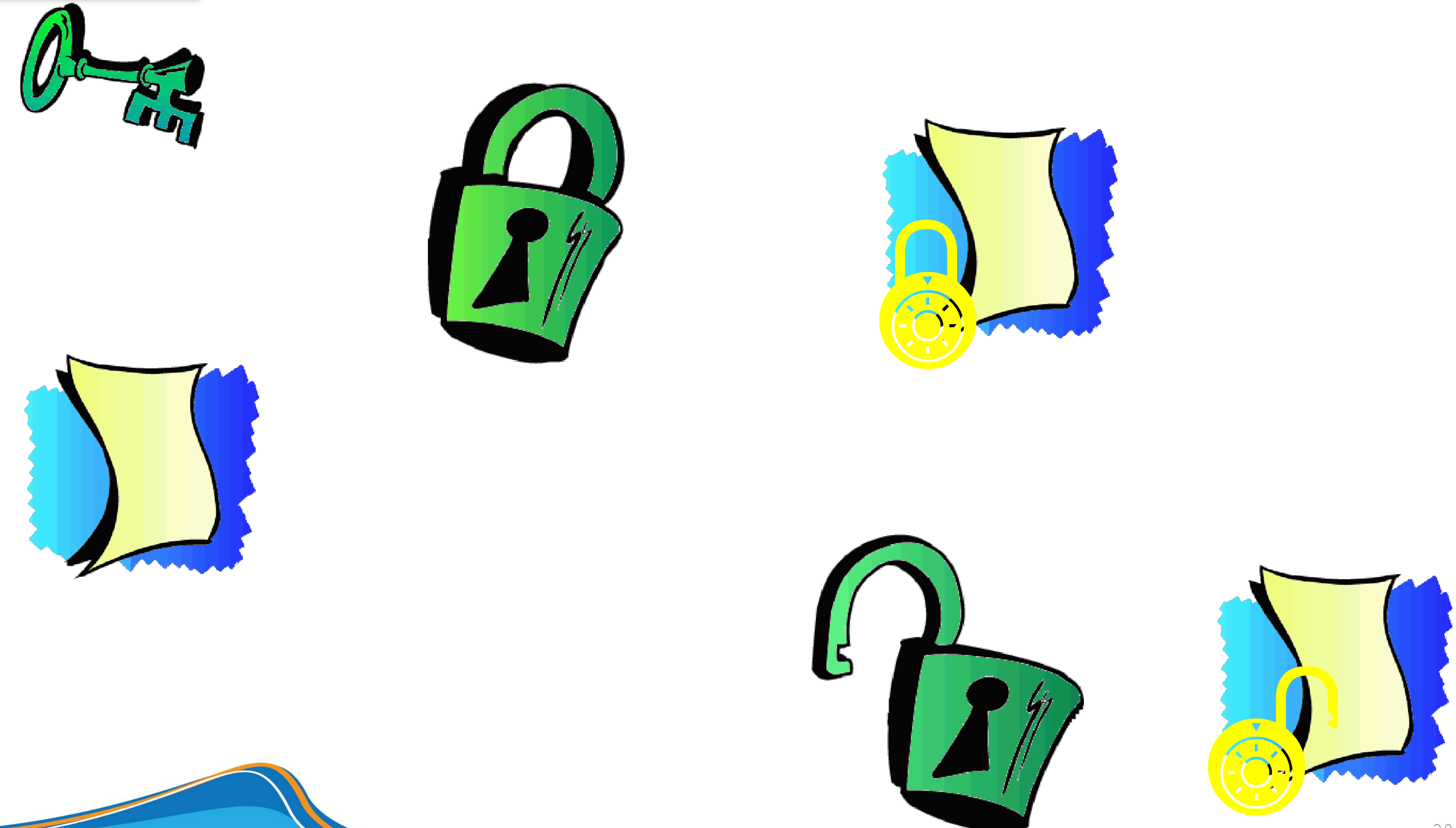
- **Data Compression**
  - Good compression – good encryption
  - Good encryption – bad compression
- **Combination of encryption approaches**
  - "Weighted sum" of crypto-systems
    - Create new crypto-systems from existing crypto-systems
    - Choose 2 crypto-systems with the same message space, use system A with probability p, use system B with probability $1 - p$.
  - Product cipher: sequentially apply successive encryption algorithms

fit@hcmus

Introduction

- Symmetric cryptosystem
  - Conventional cryptosystem
  - An encryption system in which the encryption and decryption processes both use the same key – *secret key*.
  - The security of information depends on the security of the key.
- Traditional methods use:
  - Substitution: replace 1 word/character with another word/character
  - Transposition: characters are changed their positions
- Substitution/Transposition can be done with:
  - Mono-alphabetic
  - Poly-alphabetic

Symmetric cipher



Shift cipher

- **Shift Cipher:**
  - One of the oldest methods used for encryption
  - The message is encrypted by rotating each character by k places in the alphabet
  - The case with $k = 3$ is called the Caesar encryption method.
- Let P = C = K = Z_n. For each $k \in$ K we have:
  - $e_k(x) = x + k \bmod n$ and $d_k(y) = y - k \bmod n$, for $x, y \in Z_n$
  - E = $\{e_k, k \in$ K$\}$ and D = $\{d_k, k \in$ K$\}$
- Properties:
  - Simple
  - Encryption and decryption processing is done quickly
  - Key-space $K = \{0, 1, 2, \ldots, n - 1\} = Z_n$
  - Easily broken by trying every possible key

Shift cipher

- Example: to encrypte a message represented by the letters A to Z (26 letters), we use Z_{26}.
  - Encrypted messages are not secure and can be easily decrypted by trying one after another, 26 *keys*.
  - On average, an encrypted message can be decrypted in about 26/2 = 13 tries.
- Ciphertexts: JBCRCLQRWCRVNBJENBWRWN
- Try $k = 0, 1, 2, \ldots 25$

k = 0	**jbcrclqrwcrvnbjenbwrwn**	k = 5	**ewxmxglmrxmqiweziwrmri**
k = 1	**iabqbkpqvbqumaidmavqvm**	k = 6	**dvwlwfklqwlphvdyhvqlqh**
k = 2	**hzapajopuaptlzhclzupul**	k = 7	**cuvkvejkpvkogucxgupkpg**
k = 3	**gyzozinotzoskygbkytotk**	k = 8	**btujudijoujnftbwftojof**
k = 4	**fxynyhmnsynrjxfajxsnsj**	k = 9	**astitchintimesavesnine**

Substitution cipher

- **Substitution Cipher**:
  - Well-known and widely used encryption method for hundreds of years
  - Encrypt the message by permuting the elements of the alphabet or, more generally, permuting the elements in the source set P.
- Let P = C = Z_n, K are the sets of permutations of n elements 0, 1, …, $n - 1$. So, for each $\pi \in$ K, a permutation of n elements 0, 1, …, $n - 1$. For each key $\pi \in$ K, define:
  - $e_\pi(x) = \pi(x)$ and $d_\pi(y) = \pi^{-1}(y)$, for $x, y \in Z_n$
  - E = $\{e_\pi, \pi \in$ K$\}$ and D = $\{d_\pi, \pi \in$ K$\}$ *Really secure???*
- Properties:
  - Simple, encryption and decryption are done quickly
  - Key-space K has *n! keys*
  - Overcoming the limitation of the Shift-Cipher method: It is impossible to attack by exhausting the key values $k \in K$

Substitution cipher

AO VCO JO IBU RIBU

AO VCO JO IB

?A H?A ?A

MA HOA VA UNG DUNG

Attacks based on the occurrence of characters in the language

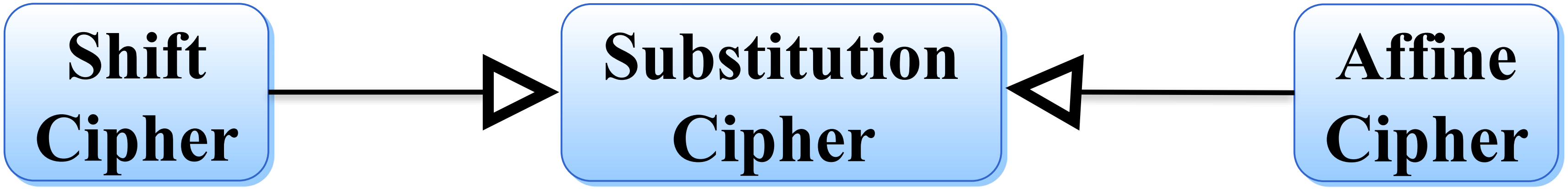
Substitution cipher

```
L FDPH L VDZ L FRQTXHUHG
L FDPH L VDZ L FRQTXHUHG
i ?a?e i ?a? i ?????e?e?
i came i saw i conquered
```

- Frequency analysis
  - Character: E > T > R > N > I > O > A > S
  - Digraph: TH > HE > IN > ER > RE > ON > AN > EN
  - Trigraph: THE > AND > TIO > ATI > FOR > THA > TER > RES

Affine cipher

- Let P = C = Z_n, K = $\{(a, b) \in Z_n \times Z_n : gcd(a, n) = 1\}$. For each key $k = (a, b) \in$ K, define:
  - $e_k(x) = (ax + b) \bmod n$ and $d_k(y) = a^{-1}(y - b) \bmod n$, for $x, y \in Z_n$
  - E = $\{e_k, k \in$ K$\}$ and D = $\{d_k, k \in$ K$\}$
- For correct decrypt then e_k must be a bijection $\Leftrightarrow gcd(a, n) = 1$



Affine cipher

- Let ㄹㅎ(n) be a number of elements in Z_n and coprime with n
- If $n =$ where p_i are distinct prime numbers and e_i ㅍ Z^+, 1 게 i 게 m then ㄹㅎ$(n) =$
- We have
  - n ways of choosing b
  - ㄹㅎ(n) ways of choosing a
  - n ㅎ ㄹㅎ(n) ways of choosing key $k = (a, b)$

fit@hcmus

Euclide algorithm

- Consider 2 prime numbers a and b ($a > b$) we have:
  - $a = q_0 b + r_0$ $(0 < r_0 < b)$
  - $b = q_1 r_0 + r_1$ $(0 < r_1 < r_0)$
  - $r_0 = q_2 r_1 + r_2$ $(0 < r_2 < r_1)$
  - $r_1 = q_3 r_2 + r_3$ $(0 < r_3 < r_2)$
  - …
  - $r_{m-2} = q_{m-1} r_{m-1} + r_m$ $(0 < r_m < r_{m-1})$
  - $r_{m-1} = q_m r_m$ $(0 = r_{m+1} < r_m)$
- Easily see:
  - $gcd(a, b) = gcd(b, r_0) = gcd(r_0, r_1) = \ldots = gcd(r_{m-1}, r_m) = r_m$.
  - Example: $gcd(1071, 462) = gcd(462, 147) = gcd(147, 21) = 21$

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

Vigenere cipher

- Choose a positive integer m. Let P = C = K = $(Z_n)^m$.
  - K = $\{(k_1, k_2, \ldots, k_m) \in (Z_n)^m\}$
  - For each key $k = (k_1, k_2, \ldots, k_m) \in$ K and $x, y \in (Z_n)^m$, define:
    - $e_k(x_1, x_2, \ldots, x_m) = ((x_1 + k_1) \bmod n, (x_2 + k_2) \bmod n, \ldots, (x_m + k_m) \bmod n)$
    - $d_k(y_1, y_2, \ldots, y_m) = ((y_1 - k_1) \bmod n, (y_2 - k_2) \bmod n, \ldots, (y_m - k_m) \bmod n)$
- Subtitution cipher: for each key k, plain-text $x \in P$ is mapped to only one $y \in C$.
- Vigenere cipher uses key with length m.
  - Named after Blaise de Vigenere (Century 16)
  - The Vigenere cipher can be viewed as consisting of m displacement ciphers that are applied alternately on a periodic basis.
  - Key-space K of Vigenere cipher is n^m
  - For example: $n = 26$, $m = 5$ then key-space has $\sim 1.1 \times 10^7$ keys

Vigenere cipher

- Example: $m = 6$ and keyword CIPHER
- Then, key $k = (2, 8, 15, 7, 4, 17)$
- Let plaintexts: **thiscryptosystemisnotsecure**

t	h	i	s	c	r
19	7	8	18	2	17
2	8	15	7	4	17
21	15	23	25	6	8

y	p	t	o	s	y
24	15	19	14	18	24
2	8	15	7	4	17
0	23	8	21	22	15

s	t	e	m	i	s
18	19	4	12	8	18
2	8	15	7	4	17
20	1	19	19	12	9

n	o	t	s	e	c
13	14	19	18	4	2
2	8	15	7	4	17
15	22	8	25	8	19

u	r	e
20	17	4
2	8	15
22	25	19

Hill cipher

- Hill cipher (1929), author: Lester S. Hill
- Main idea: use m linear-combinations of m characters in plaintext to produce m characters in ciphertext
- Example:

$$(y_1, y_2) = (x_1, x_2)\ \text{ㅎ}\ \ \text{ㄷ}$$

$$(x_1, x_2) = (y_1, y_2)\ \text{ㅎ}\ \ \text{ㄷ}$$

Hill cipher

- Choose a positive integer m. Define
  - P = C = $(Z_n)^m$
  - K is a set of inverse matrixes $m \times m$, for each key $k \in$ K, Let:
    - $e_k(x) = xk = (x_1, x_2, \ldots, x_m) \times$ where $x = (x_1, x_2, \ldots, x_m) \in$ P
    - $d_k(y) = yk^{-1}$ where $y \in$ C.
  - All arithmetic operations are performed on Z_n

Inverse matrix

- Let inverse matrix K, define K^{-1}
- Steps:
  - Convert from matrix $(K \mid I_n)$ to $(I_n \mid K^{-1})$
  - Elementary transformations:
    - Multiply 1 line by 1 a number ㄴ등 0
    - Replace 1 line by using that line adding/subtracting ㄱㅅ times to/from other lines

Permutation cipher

- The idea of the presented methods: replace each character in the source message with another character to form the encrypted message.
- The main idea of the Permutation Cipher method is to keep the characters in the source message the same, but only change the position of the characters.
- Choose a positive integer m. Let
  - P = C = $(Z_n)^m$
  - K is a set of permutations of m elements $\{1, 2, \dots, m\}$. For each key □ □ K, define:
    - $e_{□}(x_1, x_2, \dots, x_m) = (x_{□(1)}, x_{□(2)}, \dots, x_{□(m)})$
    - $d_{□}(y_1, y_2, \dots, y_m) = (, , \dots,)$, where $□^{-1}$ is an inverse permutation of □

Permutation cipher

- The permutation encryption method is a special case of Hill cipher.
- Example: choose $m = 3$, so $\pi = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline\end{array}$ & $\pi^{-1} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline\end{array}$
  - Let plain-text = EAT = (4, 0, 19)
    - Compute $(y_1, y_2, y_3) = (x_1, x_2, x_3) \times \pi = (4, 0, 19) \times = (19, 4, 0)$ = TEA
    - So, cipher-text = TEA
  - To decrypt to plain-text, we need an inverse matrix $\pi^{-1} =$
    - Compute $(x_1, x_2, x_3) = (y_1, y_2, y_3) \times \pi^{-1} = (19, 4, 0) \times = (4, 0, 19)$ = EAT

Permutation cipher

- Example: choose $m = 6$
  - So $\pi =$

1	2	3	4	5	6
3	5	1	6	4	2

& $\pi^{-1} =$

1	2	3	4	5	6
3	6	1	5	2	4

  - Assume plain-texts = shesellsseashellsbytheseashore

s	h	e	s	e	l
e	e	s	l	s	h

l	s	s	e	a	s
s	a	l	s	e	s

h	e	l	l	s	b
l	s	h	b	l	e

y	t	h	e	s	e
h	s	y	e	e	t

a	s	h	o	r	e
h	r	a	e	o	s

  - So, cipher-texts = eeslshsalseslshblehsyeethraeos