

CS 553

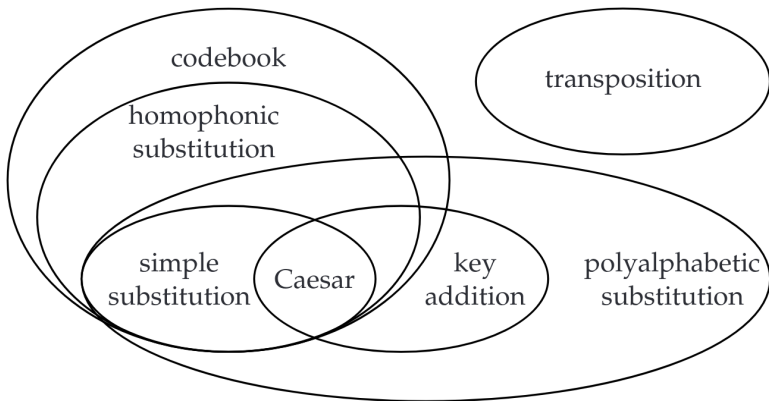
CRYPTOGRAPHY

Lecture 2

Historical Ciphers (contd.)

Instructor
Dr. Dhiman Saha

A Taxonomy of Basic Cryptosystems



Timeline of Crypto before Computers

$-\infty$ 0 500 1000 1500 1600 1700 1800 1900 2000

simple substitution

polyalphabetic substitution

key addition

codebook

transposition

electromechanical machine

Cryptographic Time Periods

antiquity	1500 BC – 100 AD
Arab civilization	800 – 1400
European Middle Ages	1000 – 1500
Renaissance	1450 – 1600
Baroque, salon cryptography	1600 – 1850
mechanical devices	1580 – 1950
electromechanical devices	1920 – 1950
computers	1943 – present
public key systems	1976 – present

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

- ▶ \mathcal{P} is a finite set of possible plaintexts
- ▶ \mathcal{C} is a finite set of possible ciphertexts
- ▶ \mathcal{K} the keyspace, is a finite set of possible keys
- ▶ For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$.
- ▶ Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

- ▶ \mathcal{P} is a finite set of possible plaintexts
- ▶ \mathcal{C} is a finite set of possible ciphertexts
- ▶ \mathcal{K} the keyspace, is a finite set of possible keys
- ▶ For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$.
- ▶ Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

- ▶ \mathcal{P} is a finite set of possible plaintexts
- ▶ \mathcal{C} is a finite set of possible ciphertexts
- ▶ \mathcal{K} the keyspace, is a finite set of possible keys
- ▶ For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$.
- ▶ Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

- ▶ \mathcal{P} is a finite set of possible plaintexts
- ▶ \mathcal{C} is a finite set of possible ciphertexts
- ▶ \mathcal{K} the keyspace, is a finite set of possible keys
- ▶ For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$.
- ▶ Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

- ▶ \mathcal{P} is a finite set of possible plaintexts
- ▶ \mathcal{C} is a finite set of possible ciphertexts
- ▶ \mathcal{K} the keyspace, is a finite set of possible keys
- ▶ For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$.
- ▶ Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where the following conditions are satisfied:

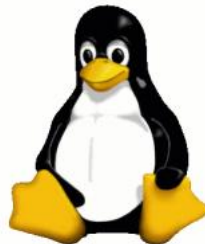
- ▶ \mathcal{P} is a finite set of possible plaintexts
- ▶ \mathcal{C} is a finite set of possible ciphertexts
- ▶ \mathcal{K} the keyspace, is a finite set of possible keys
- ▶ For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$.
- ▶ Each $e_K : \mathcal{P} \rightarrow \mathcal{C}$ and $d_K : \mathcal{C} \rightarrow \mathcal{P}$ such that $d_K(e_K(x)) = x$ for every plaintext element $x \in \mathcal{P}$.

- ▶ Each encryption function should be injective. Why?
- ▶ What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- ▶ It is possible that $|\mathcal{C}| > |\mathcal{P}|$?
- ▶ d_K is definitely deterministic but what about e_K :
Deterministic/Probabilistic?
- ▶ Notion of efficiency & security?



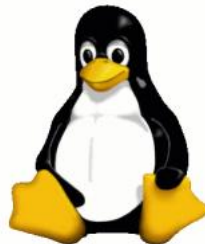
e.g. Deterministic Encryption

- ▶ Each encryption function should be injective. Why?
- ▶ What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- ▶ It is possible that $|\mathcal{C}| > |\mathcal{P}|$?
- ▶ d_K is definitely deterministic but what about e_K :
Deterministic/Probabilistic?
- ▶ Notion of efficiency & security?



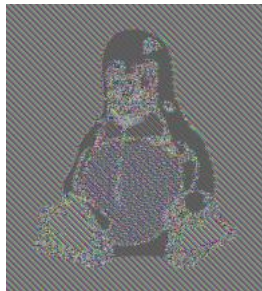
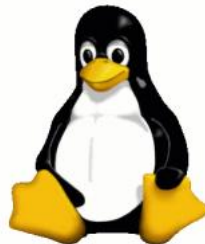
e.g. Deterministic Encryption

- ▶ Each encryption function should be injective. Why?
- ▶ What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- ▶ It is possible that $|\mathcal{C}| > |\mathcal{P}|$?
- ▶ d_K is definitely deterministic but what about e_K :
Deterministic/Probabilistic?
- ▶ Notion of efficiency & security?



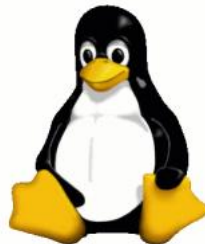
e.g. Deterministic Encryption

- ▶ Each encryption function should be injective. Why?
- ▶ What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- ▶ It is possible that $|\mathcal{C}| > |\mathcal{P}|$?
- ▶ d_K is definitely deterministic but what about e_K :
Deterministic/Probabilistic?
- ▶ Notion of efficiency & security?



e.g. Deterministic Encryption

- ▶ Each encryption function should be injective. Why?
- ▶ What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- ▶ It is possible that $|\mathcal{C}| > |\mathcal{P}|$?
- ▶ d_K is definitely deterministic but what about e_K :
Deterministic/Probabilistic?
- ▶ Notion of efficiency & security?



e.g. Deterministic Encryption

- ▶ Notion of Semantic Security and Randomized Encryption
- ▶ Captures the intuition that ciphertexts *shouldn't leak any information about plaintexts* as long as the key is secret.
- ▶ The indistinguishability game



- ▶ To be studied in detail in lecture on block ciphers

Math Recap

Algebraic Structures: Groups, Rings

Definition 2.1.1. An **Abelian group** $\langle G, + \rangle$ consists of a set G and an operation defined on its elements, here denoted by '+':

$$+ : G \times G \rightarrow G : (a, b) \mapsto a + b. \quad (2.1)$$

In order to qualify as an **Abelian group**, the operation has to fulfill the following conditions:

$$\text{closed: } \forall a, b \in G : a + b \in G \quad (2.2)$$

$$\text{associative: } \forall a, b, c \in G : (a + b) + c = a + (b + c) \quad (2.3)$$

$$\text{commutative: } \forall a, b \in G : a + b = b + a \quad (2.4)$$

$$\text{neutral element: } \exists \mathbf{0} \in G, \forall a \in G : a + \mathbf{0} = a \quad (2.5)$$

$$\text{inverse elements: } \forall a \in G, \exists b \in G : a + b = \mathbf{0} \quad (2.6)$$

Example

The set of integers with the operation 'addition': $\langle \mathbb{Z}, + \rangle$

► What about \mathbb{Z}_m ?

Definition 2.1.2. A ring $\langle R, +, \cdot \rangle$ consists of a set R with two operations defined on its elements, here denoted by $+$ and \cdot . In order to qualify as a ring, the operations have to fulfill the following conditions:

1. The structure $\langle R, + \rangle$ is an Abelian group.
2. The operation \cdot is closed, and associative over R . There is a neutral element for \cdot in R .
3. The two operations $+$ and \cdot are related by the law of distributivity:

$$\forall a, b, c \in R: (a + b) \cdot c = (a \cdot c) + (b \cdot c). \quad (2.7)$$

The neutral element for \cdot is usually denoted by 1 . A ring $\langle R, +, \cdot \rangle$ is called a *commutative ring* if the operation \cdot is commutative.

Example

The set of integers with the operation *addition* and *multiplication*: $\langle \mathbb{Z}, +, \cdot \rangle$

► What about \mathbb{Z}_m ?

Informally

\mathbb{Z}_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ in which we can **add**, **subtract**, **multiply**, and **sometimes divide**.

- ▶ **Sometimes** divide. Why?
- ▶ Recall, ring, by definition is not required to have multiplicative inverse for all elements,
- ▶ It exists only for some, say $a \in \mathbb{Z}_m$
- ▶ Then

$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \pmod{m}$$

- ▶ If inverse exists for a , then we can divide by a since $b/a \equiv b \cdot a^{-1} \pmod{m}$

How do you know inverse exists for an element?

Informally

\mathbb{Z}_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ in which we can add, subtract, multiply, and **sometimes** divide.

- ▶ **Sometimes** divide. Why?
- ▶ Recall, ring, by definition is not required to have multiplicative inverse for all elements,
- ▶ It exists only for some, say $a \in \mathbb{Z}_m$
- ▶ Then

$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \pmod{m}$$

- ▶ If inverse exists for a , then we can divide by a since $b/a \equiv b \cdot a^{-1} \pmod{m}$

How do you know inverse exists for an element?

Informally

\mathbb{Z}_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ in which we can add, subtract, multiply, and **sometimes** divide.

- ▶ **Sometimes** divide. Why?
- ▶ Recall, ring, by definition is not required to have multiplicative inverse for all elements,
- ▶ It exists only for some, say $a \in \mathbb{Z}_m$
- ▶ Then

$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \pmod{m}$$

- ▶ If inverse exists for a , then we can divide by a since $b/a \equiv b \cdot a^{-1} \pmod{m}$

How do you know inverse exists for an element?

Informally

\mathbb{Z}_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ in which we can add, subtract, multiply, and **sometimes** divide.

- ▶ **Sometimes** divide. Why?
- ▶ Recall, ring, by definition is not required to have multiplicative inverse for all elements,
- ▶ It exists only for some, say $a \in \mathbb{Z}_m$
- ▶ Then

$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \pmod{m}$$

- ▶ If inverse exists for a , then we can divide by a since $b/a \equiv b \cdot a^{-1} \pmod{m}$

How do you know inverse exists for an element?

Informally

\mathbb{Z}_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ in which we can add, subtract, multiply, and **sometimes** divide.

- ▶ **Sometimes** divide. Why?
- ▶ Recall, ring, by definition is not required to have multiplicative inverse for all elements,
- ▶ It exists only for some, say $a \in \mathbb{Z}_m$
- ▶ Then

$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \pmod{m}$$

- ▶ If inverse exists for a , then we can divide by a since
 $b/a \equiv b \cdot a^{-1} \pmod{m}$

How do you know inverse exists for an element?

Informally

\mathbb{Z}_m is the set of integers $\{0, 1, 2, \dots, m-1\}$ in which we can add, subtract, multiply, and **sometimes** divide.

- ▶ **Sometimes** divide. Why?
- ▶ Recall, ring, by definition is **not required** to have **multiplicative inverse for all elements**,
- ▶ It exists only for some, say $a \in \mathbb{Z}_m$
- ▶ Then

$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \pmod{m}$$

- ▶ If inverse exists for a , then we can divide by a since $b/a \equiv b \cdot a^{-1} \pmod{m}$

How do you know inverse exists for an element?

- ▶ Elements relatively prime to m are invertible
- ▶ How to find?
- ▶ Hint: Greatest Common Divisor - gcd

$$\text{Verify} \rightarrow \gcd(a, m) = 1$$

Theorem

An element $a \in \mathbb{Z}_m$ is invertible if and only if $\gcd(a, m) = 1$

- ▶ Check if 15, 14 are invertible in \mathbb{Z}_{26} .
- ▶ If $a \in \mathbb{Z}_m$ is invertible, how find a^{-1}
- ▶ Euclidean GCD Algorithm

Affine Cipher

Further Generalization of Shift Cipher

► Recall Shift Cipher

Encryption

$$e(x) = (x + k) \bmod 26$$

Decryption

$$d(x) = (x - k) \bmod 26$$

Definition (Affine Cipher)

Let $x, y, a, b \in \mathbb{Z}_{26}$

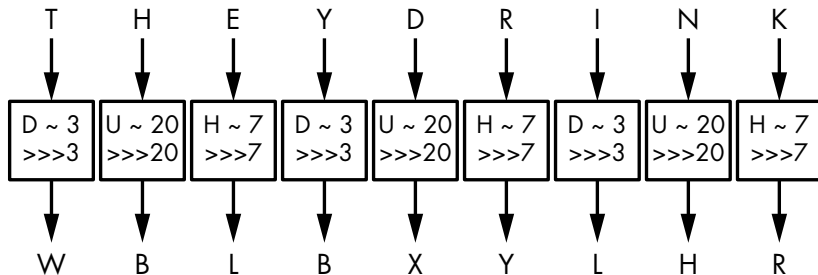
Encryption: $e_K(x) = y \equiv a \cdot x + b \bmod 26$

Decryption: $d_K(y) = x \equiv a^{-1} \cdot (y - b) \bmod 26$

with the key: $K=(a,b)$ which has the restriction: $\gcd(a, 26) = 1$

► “Affine” ?

- ▶ By Giovan Battista Bellaso in 16th Century
- ▶ Used in American Civil War and World-War I
- ▶ Polyalphabetic Substitution



Key = 'DUH'

Example 2.4 Suppose $m = 6$ and the keyword is *CIPHER*. This corresponds to the numerical equivalent $K = (2, 8, 15, 7, 4, 17)$. Suppose the plaintext is the string

thiscryptosystemisnotsecure.

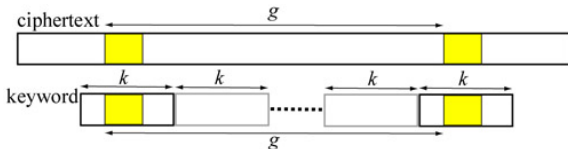
We convert the plaintext elements to residues modulo 26, write them in groups of six, and then “add” the keyword modulo 26, as follows:

$$\begin{array}{cccccccccccc}
 19 & 7 & 8 & 18 & 2 & 17 & 24 & 15 & 19 & 14 & 18 & 24 \\
 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 \\
 \hline
 21 & 15 & 23 & 25 & 6 & 8 & 0 & 23 & 8 & 21 & 22 & 15 \\
 \\
 18 & 19 & 4 & 12 & 8 & 18 & 13 & 14 & 19 & 18 & 4 & 2 \\
 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 \\
 \hline
 20 & 1 & 19 & 19 & 12 & 9 & 15 & 22 & 8 & 25 & 8 & 19 \\
 \\
 & & & & & & 20 & 17 & 4 & & & \\
 & & & & & & 2 & 8 & 15 & & & \\
 \hline
 & & & & & & 22 & 25 & 19 & & &
 \end{array}$$

- Ciphertext \rightarrow VPXZGIAXIVWPUBTTMJPWIZITWZT
- What is the size of the key-space?

Intuition

If a repeated substring in a plaintext is encrypted by the same substring in the keyword, then the ciphertext contains a repeated substring and the distance of the two occurrences is a multiple of the keyword length.



THEY DRINK THE TEA \rightarrow WBLBXYLHRWBLWYH

- Note: Since the keyword of length k is repeated to fill the length of the ciphertext, the distance g is a multiple of the keyword length k .
- For example, if the distance is $g = 18$, since the factors of g are 2, 3, 6, 9 and 18, one of them may be the length of the unknown keyword.

- ▶ Friedrich W. Kasiski, a German military officer, published his book *Die Geheimschriften und die Dechiffirkunst* (Cryptography and the Art of Decryption) in 1863

The Kasiski test works as follows. We search the ciphertext for pairs of identical segments of length at least three, and record the distance between the starting positions of the two segments. If we obtain several such distances, say $\delta_1, \delta_2, \dots$, then we would conjecture that m divides all of the δ_i 's, and hence m divides the greatest common divisor of the δ_i 's.


- ▶ Still difficult to break for short messages
- ▶ Good for short-lived messages

Trivia

The 19th-century cryptographer Auguste Kerckhoffs estimated that most encrypted wartime messages required confidentiality for only three to four hours

- Polyalphabetic; by Lester S. Hill. in 1929
- $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
- Let, $(x_1, x_2, \dots, x_m) \in \mathcal{P}$, $K = (k_{i,j}) \in \mathcal{K}$ then
 $y = e_K(x) = (y_1, y_2, \dots, y_m)$

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m) \begin{bmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{bmatrix}$$

- Note: every y_i is a linear combination of all x_j 
- In matrix notation:
 Encryption $y = xK$ and Decryption $x = yK^{-1}$
- Invertibility of K

Permutation/Transposition Cipher

Definition

Let m be a positive integer. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ and let \mathcal{K} consist of all permutations of $1, \dots, m$. For a key π , we define

$$e_{\pi}(x_1, x_2, \dots, x_m) = x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)}$$

and

$$d_{\pi}(y_1, y_2, \dots, y_m) = x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \dots, x_{\pi^{-1}(m)}$$

where π^{-1} is the inverse permutation of π .

Example

Let $m = 6$ and a possible key is the permutation π :

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

► This is a special case of Hill Cipher. How? 