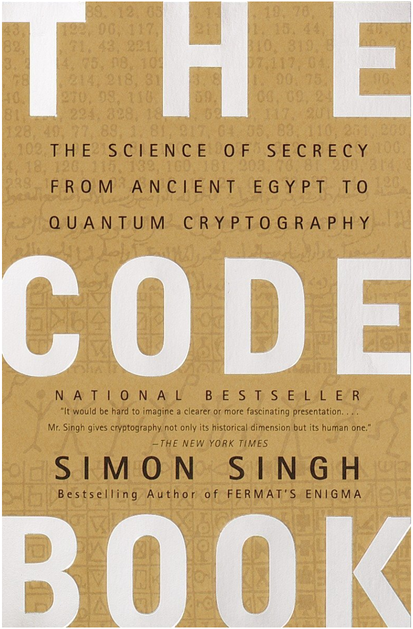


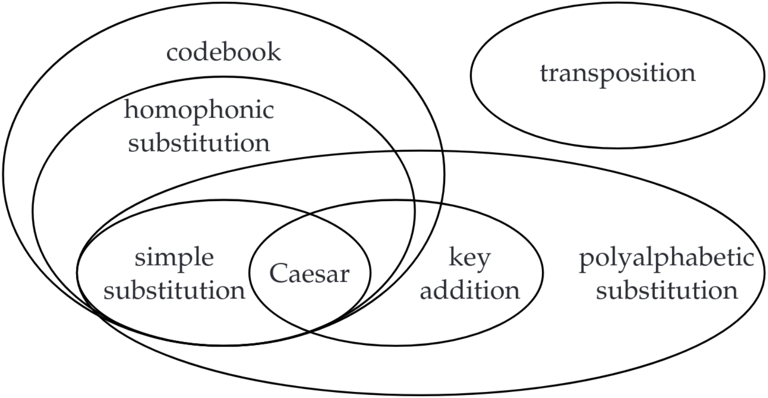
Image Source: Google

CS 553
CRYPTOGRAPHY

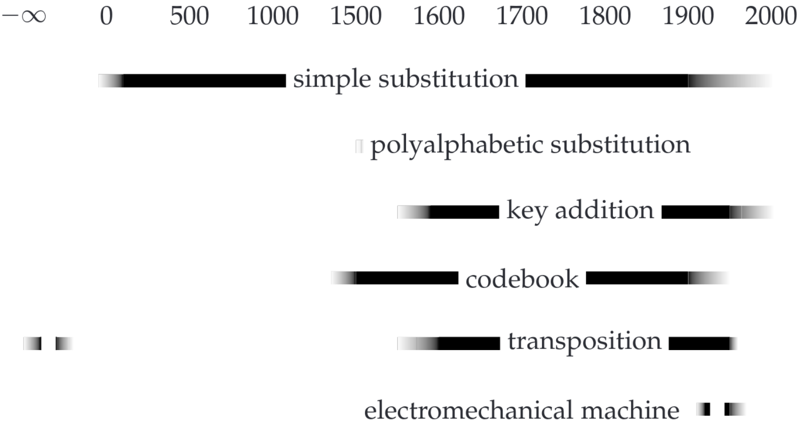
Lecture 2
Historical Ciphers (contd.)

Instructor
Dr. Dhiman Saha

A Taxonomy of Basic Cryptosystems



Timeline of Crypto before Computers



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 $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ 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 $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ 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 $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ 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:

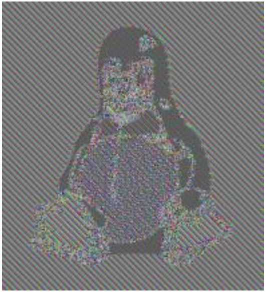
- $\mathcal{P}$ is a finite set of possible *plaintexts*
- $\mathcal{C}$ is a finite set of possible *ciphertexts*
- $\mathcal{K}$ the *keyspace*, is a finite set of possible keys
- For each $K \in \mathcal{K}$, there is an *encryption rule* $e_K \in \mathcal{E}$ and a corresponding *decryption rule* $d_K \in \mathcal{D}$.
- Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ 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:

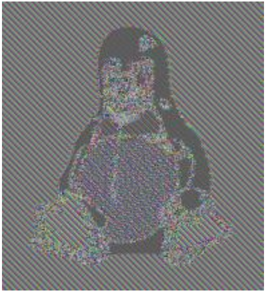
- $\mathcal{P}$ is a finite set of possible *plaintexts*
- $\mathcal{C}$ is a finite set of possible *ciphertexts*
- $\mathcal{K}$ the *keyspace*, is a finite set of possible keys
- For each $K \in \mathcal{K}$, there is an *encryption rule* $e_K \in \mathcal{E}$ and a corresponding *decryption rule* $d_K \in \mathcal{D}$.
- Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ 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?



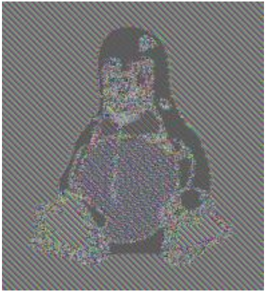
e.g. Deterministic Encryption

- 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?



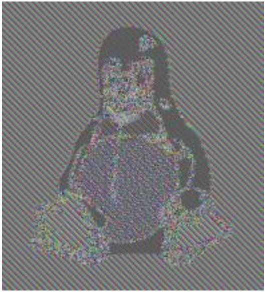
e.g. Deterministic Encryption

- 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

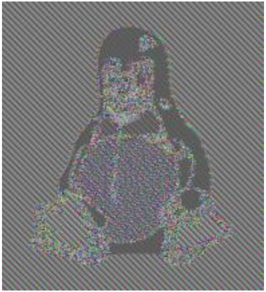
- Each encryption function should be *injective*. Why?
- What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- It is possible that $|\mathcal{C}| > |\mathcal{P}|$?
- d_K is definitely deterministic but what about e_K : Deterministic/Probabilistic?
- Notion of efficiency &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



e.g. Deterministic Encryption

Points to Ponder

- Each encryption function should be *injective*. Why?
- What is the nature of every encryption function if $\mathcal{P} = \mathcal{C}$?
- It is possible that $\left|\mathcal{C}\right| > \left|\mathcal{P}\right|$?
- 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 $< G, + >$ *consists of a set* G *and an operation defined on its elements, here denoted by '+':*

$$+ : G \times G \to G : (a, b) \mapsto a + b. \tag{2.1}$$

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

$$\begin{aligned}
\textit{closed:}\quad & \forall\ a, b \in G : a + b \in G && (2.2)\\
\textit{associative:}\quad & \forall\ a, b, c \in G : (a + b) + c = a + (b + c) && (2.3)\\
\textit{commutative:}\quad & \forall\ a, b \in G : a + b = b + a && (2.4)\\
\textit{neutral element:}\quad & \exists \mathbf{0} \in G, \forall\ a \in G : a + \mathbf{0} = a && (2.5)\\
\textit{inverse elements:}\quad & \forall\ a \in G, \exists\ b \in G : a + b = \mathbf{0} && (2.6)
\end{aligned}$$

Example

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

Definition 2.1.2. *A ring* $< R, +, \cdot >$ *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* $< R, + >$ *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:*

$$\forall\, a, b, c \in R: \; (a + b) \cdot c = (a \cdot c) + (b \cdot c). \tag{2.7}$$

The neutral element for '$\cdot$' is usually denoted by $\mathbf{1}$. A ring $< R, +, \cdot >$ is called a *commutative ring* if the operation '$\cdot$' is commutative.

Example

The set of integers with the operation 'addition' and 'multiplication': $< \mathbb{Z}, +, \cdot >$

- What about $\mathbb{Z}_m$?

Informally

$\mathbb{Z}_m$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$ 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

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

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

How do you know inverse exists for an element?

Informally

$\mathbb{Z}_m$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$ 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

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

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

How do you know inverse exists for an element?

Informally

$\mathbb{Z}_m$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$ 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
$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \mod m$$
- If inverse exists for a, then we can divide by a since $b/a \equiv b \cdot a^{-1} \mod m$

How do you know inverse exists for an element?

Informally

$\mathbb{Z}_m$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$ 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

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

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

How do you know inverse exists for an element?

Informally

$\mathbb{Z}_m$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$ 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
$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \mod m$$
- If inverse exists for a, then we can divide by a since $b/a \equiv b \cdot a^{-1} \mod m$

How do you know inverse exists for an element?

Informally

$\mathbb{Z}_m$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$ 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
$$\exists a^{-1} \in \mathbb{Z}_m : a \cdot a^{-1} \equiv 1 \mod m$$
- If inverse exists for a, then we can divide by a since $b/a \equiv b \cdot a^{-1} \mod m$

How do you know inverse exists for an element?

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

$$Verify \;\rightarrow\; gcd(a, m) = 1$$

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

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

Decryption

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

Definition (Affine Cipher)

Let $x, y, a, b \in \mathbb{Z}_{26}$
Encryption: $e_K(x) = y \equiv a \cdot x + b \mod 26$
Decryption: $d_K(y) = x \equiv a^{-1} \cdot (y - b) \mod 26$
with the key: K=(a,b) which has the restriction: $gcd(a, 26) = 1$

- "Affine" ?