Modern Cryptography

Historical Ciphers

Dr Shashank Singh

1 Some Historical Ciphers

Caesar (Shift) Cipher

- It is named after Julius Caesar, who used it to communicate with his generals using this cipher.
- It is one of the simplest and well-known private-key encryption schemes.

$$\mathcal{M} = \{A, B, ..., Z\}^*$$

$$\mathcal{K} = \{0, 1, 2, ..., 25\}$$

$$\text{Gen}() \rightarrow k, \text{where} \quad k \xleftarrow{\$} \mathcal{K}$$

$$\text{Enc}_k(m_1 m_2 ... m_k) = c_1 c_2 ... c_k \text{ where } c_i \equiv (m_i + k) \bmod 26$$

$$\text{Dec}_k(c_1 c_2 ... c_k) = m_1 m_2 ... m_k \text{ where } m_i \equiv (c_i - k) \bmod 26$$

Caesar (Shift) Cipher (ii)

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Suppose the key for a Shift Cipher is $k = 11$, and the plaintext is

$$\mu := \text{WEWILLMEETATMIDNIGHT}.$$

$\text{ENC}_k(\mu) = ?$

Caesar (Shift) Cipher (iii)

$\text{ENC}_k(\mu) = \text{HPHTWWXPPELEXTOYTRSE}$

- The encryption is a cyclic shift of k on each letter in the message, and the decryption is a cyclic shift of $-k$.
- To break the scheme, we just need to try all 26 different values of k and see if the resulting plaintext is "readable" (*Brute Force Attack*).
- Is it possible to modify this scheme to prevent this simple brute-force attack?

The Substitution Cipher

$$\Sigma = \{A, B, ..., Z\}$$

$$\mathcal{M} = \Sigma^*$$

$$\mathcal{K} = \{\tau |\ \tau : \Sigma \rightarrow \Sigma \text{ is a perm.}\}$$

$$\text{Gen}() \rightarrow \pi, \text{where } \pi \xleftarrow{\$} \mathcal{K}$$

$$\text{Enc}_k(\mu_1\mu_2...\mu_k) = \nu_1\nu_2...\nu_k \text{ where } \nu_i = \pi(\mu_i)$$

$$\text{Dec}_k(\nu_1\nu_2...\nu_k) = \mu_1\mu_2...\mu_k \text{ where } \mu_i = \pi^{-1}(\nu_i)$$

- What is the size of key space i.e., $|\mathcal{K}|$?

The Substitution Cipher (ii)

Consider a permutation π, given by the following table:

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
X	N	Y	A	H	P	O	W	Z	Q	W	B	T

n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
S	F	L	R	C	V	M	U	E	K	J	D	I

Remark: We use uppercase letters for ciphertext and lowercase letters for plaintext, in order to improve readability.

The Substitution Cipher (iii)

Exercise: Decrypt the following ciphertext generated using the Substitution Cipher
MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA.

- Is it possible to apply a brute force attack as in the case of the Caesar Cipher?
- $|\mathcal{K}| = 26! \approx 2^{88}$. A brute force attack will not be feasible.
- Can we still attack this scheme?
- What do I mean by attacking/breaking a private key encryption scheme?. I will elaborate on this later.

The Affine Cipher

- The Shift Cipher is a special case of the Substitution Cipher, which includes only 26 of the 26! possible permutations of 26 elements.
- Another special case of the Substitution Cipher is the Affine Cipher.
- In the Affine Cipher, we restrict the encryption functions to functions of the form, for $a, b \in \mathbb{Z}_{26}$

$$\text{Enc}_k(x) = (ax + b) \bmod 26, \text{where} \gcd(a, 26) = 1$$

The Affine Cipher (ii)

$$\Sigma = \{A, B, ..., Z\} = \mathbb{Z}_{26}$$

$$\mathcal{M} = \Sigma^*$$

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} | \gcd(a, 26) = 1\}$$

$$\text{Gen}() \rightarrow \pi := (a, b), \text{where} \quad \pi \xleftarrow{\$} \mathcal{K}$$

$$\text{Enc}_k(x) = ax + b$$

$$\text{Dec}_k(y) = a^{-1}(y - b)$$

Monoalphabetic Cryptosystems

Remark:

- In both the Caesar Cipher and the Substitution Cipher, once a key is chosen, each alphabetic character is mapped to a unique alphabetic character.
- For this reason, these cryptosystems are called monoalphabetic cryptosystems.

- Monoalphabetic Cryptosystem can be easily attacked using frequency analysis of letter and words in a a language.

Vigenère Cipher

- In this cipher $\mathcal{M} = \Sigma^*$, where Σ is English alphabet.
- We will use the correspondence $A \leftrightarrow 0$, $B \leftrightarrow 1$, $C \leftrightarrow 3$, ..., $Z \leftrightarrow 25$ here as well.
- A key k corresponds to an alphabetic string of length m. I.e., the key consists of the length of string m and the string itself. E.g. in the key "cipher", $m = 6$.
- Vigenère Cipher encrypts m alphabetic characters at a time: each plaintext element is equivalent to m alphabetic characters.

Encryption in Vigenère Cipher

t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	mi	s	n	o	t	s	e	c	u	r	e
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
c	i	p	h	e	r	c	i	p	h	e	r	c	i	p	h	e	r	c	i	p	h	e	r	c	i	p
V	P	X	Z	G	I	A	X	I	V	WP		U	B	T	T	MJ		P	WI		Z	I	T	WZ	T

- Note that first ‘s’ is encrypted to ‘Z’, second ‘s’ is encrypted to ‘W’ and third ‘s’ is encrypted to ‘U’, forth ‘s’ to ‘J’, and the fifth ‘s’ is encrypted to ‘Z’.
- Such cryptosystems are referred as poly-alphabetic cryptosystems.

Formal Description of Vigenère Ciphe

Let m be a positive integer. Define $\mathcal{M} = \mathcal{K} = \mathbb{Z}_{26}^m$. For a key $K = (k_1, k_2, ..., k_m)$, we define

$$\text{Enc}_K(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ..., x_m + k_m)$$

$$\text{Dec}_K(y_1, y_2, ..., y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m),$$

where all operations are performed in $\mathbb{Z}_{26}$.

- Note that $|\mathcal{K}| = 26^m$, so even for relatively small values of m, an exhaustive key search would require a long time.

Permutation Cipher

- It is also known as the Transposition Cipher.

Let m be a positive integer and $\mathcal{M} = \mathbb{Z}_{26}^m$. Let $\mathcal{K}$ consist of all permutations of $\{1, 2, ..., m\}$. For a key (i.e., a permutation) π, we define,

$$\text{Enc}_\pi(x_1, x_2, ..., x_m) = \left(x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(m)}\right)$$

$$\text{Dec}_K(y_1, y_2, ..., y_m) = \left(y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, ..., y_{\pi^{-1}(m)}\right),$$

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

Suppose m = 6 and the key is the following permutation π: x 123456. π(x) 3 5 1 6 4 2

Permutation Cipher (ii)

Let a key π is given by the following table:

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

Exercise: Given the ciphertext

EESLSHSALSESLSHBLEHSYEETHRAEOS,

find out the corresponding message under the key π.

- In general, cryptanalysis is more difficult for polyalphabetic than for monoalphabetic cryptosystems.

2 Stream Ciphers

Stream Ciphers

- In the crypto-systems we have studied so far, successive plaintext elements are encrypted using the same key, k.
- That is, the ciphertext string y is obtained as follows:

$$y = y_1 y_2 ... = \text{Enc}_k(x_1)\text{Enc}_k(x_2)...$$

Cryptosystems of this type are often called block ciphers.

- An alternative approach is to generate a keystream $z = z_1 z_2 ...$, and use it to encrypt a plaintext string $x = x_1 x_2 ...$ according to the rule

$$y = y_1 y_2 ... = \text{Enc}_{z_1}(x_1)\ \text{Enc}_{z_2}(x_2)...$$

Such Cryptosystems are called stream ciphers.

Synchronous stream cipher

- The simplest type of stream cipher is one in which the keystream is constructed from the key, independent of the plaintext string, using some specified algorithm.

Synchronous stream cipher (ii)

A synchronous stream cipher is a tuple $(\mathcal{M}, \mathcal{K}, \mathcal{L}, \text{Gen}, \text{Enc}, \text{Dec})$, together with a function g, called a key stream generator, where

- $\mathcal{M}$ is a finite set of possible plaintexts and $\mathcal{K}$ is key space.
- $\mathcal{L}$ is a finite set called the keystream alphabet.
- g takes a key k as input, and generates an infinite string $z_1 z_2 \ldots$ called the keystream, where $z_i \in \mathcal{L}$ for all $i \geq 1$.
- For each $z \in \mathcal{L}$, there is an encryption rule $e_z \in \text{Enc}$ and a corresponding decryption rule $d_z \in \text{Dec}$ such that

$$d_z(e_z(x)) = x \forall x \in \mathcal{M}$$

Vigenère Cipher as a synchronous stream cipher

Let m be a keyword length. Let $\mathcal{K} = Z_{26}^m$ and $\mathcal{M} = \mathcal{L} = Z_{26}$.

The key-stream generation is defined as follows:

$$z_i = \begin{cases} k_i & \text{if } 1 \leq i \leq m \\ z_{i-m} & \text{if } i > m+1 \end{cases}$$

where $k = (k_1, ..., k_m)$ and this generates the keystream

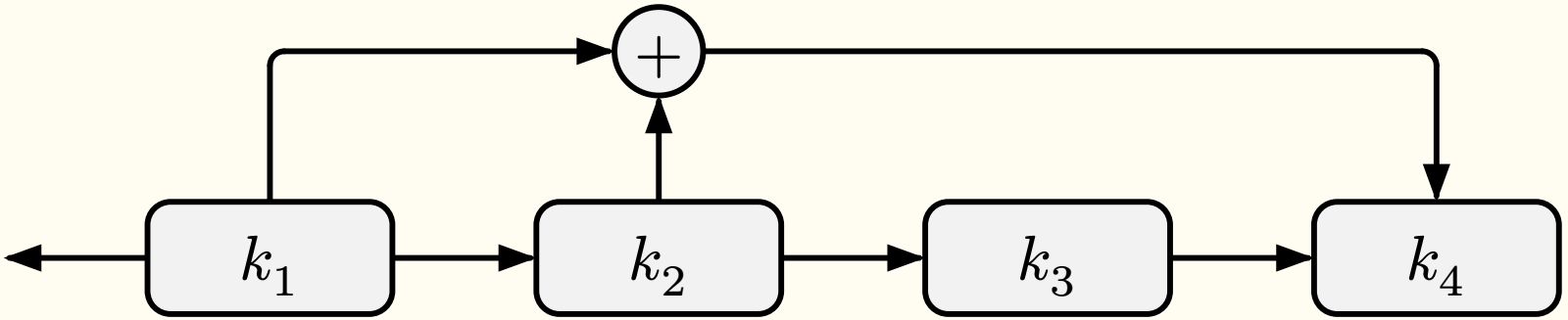
$$k_1, k_2, ..., k_m, k_1, k_2, ..., k_m, k_1, k_2, ..., k_m, ...$$

Definition: A stream cipher is a periodic stream cipher with period d if $z_{i+d} = z_i$ for all integers $i \geq 1$.

Stream Ciphers..

- Stream ciphers are often described in terms of binary alphabets, i.e., $\mathcal{M} = \mathcal{L} = \mathbb{Z}_2 = \{0, 1\}$.
- An efficient method of keystream generation is a **linear feedback shift register**, or **LFSR**.
- Let $k = (k_1, k_2, ...k_m, c_0, ..., c_{m-1})$, the LFSR works as follows:
  - $z_i = k_i$ for $i = 1, ..., k$
  - $z_{i+m} = \sum_{j=0}^{m-1} c_i z_{i+j} \bmod 2$, $c_i \in \mathbb{Z}_2$
- This method of keystream generation can be efficiently implemented in the hardware.

Stream Ciphers.. (ii)



- The vector $(k_1, ..., k_m)$ would be used to initialize the shift register.
- k_1 would be tapped as the next keystream bit.
- $k_2, ..., k_m$ would each be shifted one stage to the left.
- The new value of k_m would be computed to be $\sum_{j=0}^{m-1} c_j k_{j+1}$.

3 Cryptanalysis of historical ciphers in the light of modern cryptography

Principles of Modern Cryptography

- Systematic development of cryptographic protocols and its rigorous security analysis and proofs of security.
- And this requires **formal definitions**, **precise assumptions** and **proper proofs** for security.
- We follow the general assumption that the adversary knows the design of the cryptosystem being used (**Kerckhoffs' Principle**).

Security Goals of Schemes

What do we mean by an encryption scheme to be secure?

Security Goals of Schemes..

What do we mean by an encryption scheme to be secure?

- Regardless of the information an attacker already has about the plaintext, it should not learn any additional information about it after seeing the ciphertext.
- In more simpler words **"the information an attacker can guess about plaintext even without seeing its corresponding ciphertext is same as the information it can find out even after seeing the ciphertext."**
- How should we mathematically model it?

Attack Model

The attack model specifies the information available to the adversary when (s)he mounts an attack.

- **Ciphertext-only Attack**: The adversary possesses a string of ciphertexts.
- **Known Plaintext Attack**: Ciphertext-only attack + some plaintext-ciphertext pair(s) with same key.
- **Chosen Plaintext Attack**: Ciphertext-only attack + some plaintext, chosen by adversary, and its corresponding ciphertext generated with same key.

Attack Model (ii)

- **Chosen Ciphertext Attack**: Ciphertext-only attack + some ciphertext, chosen by adversary, and its corresponding decryption by the same key.

Modern Cryptography: Precise Assumptions and Proof of Security

- Assumptions are required for mathematical proofs of the security of a cryptographic scheme.
- The assumptions should be precisely stated, and their validity needs to be examined thoroughly.
- We trust a cryptographic scheme based on better-studied/ recognised assumptions.
- Precisely stated assumptions are often crucial in re-assessing the security of a scheme once some weaknesses are found.
- Proofs of security give an iron-clad guarantee relative to the definition and assumptions that no attacker will succeed.