Fundamental techniques of cryptography –

Substitution and Transposition
Monoalphabetic & Polyalphabetic
Caesar Cipher

B Tech CSE- IV Sem

TCS 491

Introduction to Cryptography

Jan- Jun 2022

Classical Encryption Techniques

- Cryptographic systems are generically classified along three independent dimensions:
- 1. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations be reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.
- 2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two-key, or public-key encryption.
- 3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Substitution Ciphers

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Monoalphabetic & Polyalphabetic Ciphers

- This is a substitution technique that uses a single alphabet to replace symbols of plaintext for symbols of ciphertext as dictated by the key. The key often represents the number of symbols to shift the plaintext from a circular alphabet. These techniques are relatively easy to break due to the fact that symbol frequencies remain invariant.
- Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’. Example: **Caesar Cipher**
- Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The two examples are **playfair and Vigenere Cipher**.

Caesar Cipher(Monoalphabetic Cipher)

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

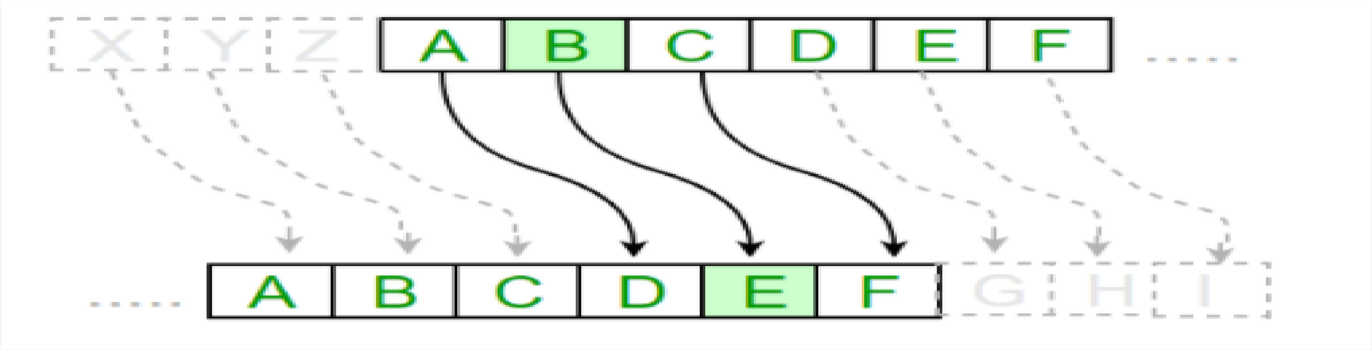
Encryption and Decryption in Caesar Cipher

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)



Algorithm for Caesar Cipher:

- **Input:**

1.A String of lower case letters, called Text.

2.An Integer between 0-25 denoting the required shift.

- **Procedure:**
- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
- Return the new string generated.

Examples:

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI

Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:

- 1. The encryption and decryption algorithms are known.
- 2. There are only 25 keys to try.
- 3. The language of the plaintext is known and easily recognizable.

Difference between Monoalphabetic Cipher and Polyalphabetic Cipher

- **1. Monoalphabetic Cipher :**

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

- **2. Polyalphabetic Cipher :**

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

S.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
1	Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
3	Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto ‘m’ alphabetic characters of a cipher text.
4	A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream.	A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of the plain text character in the plain text stream.
5	It includes additive, multiplicative, affine and monoalphabetic substitution cipher.	It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.
6	It is a simple substitution cipher.	It is multiple substitutions cipher.
7	Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.	Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different cryptoalphabets.
8	Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.

Thank You

&

Best Wishes