**Classical Encryption Techniques**

**Substitution Ciphers:**

* It replaces one symbol with another.
* If the symbols in the plain text are alphabetic characters, we can replace one character with another. Eg: we can replace letter “A” with “B”.
* If the symbols are digits (0-9), we can replace one digit with another. Eg: we can replace “3” with “5”.
* Substitution ciphers are categorized as 2 types. Mono-alphabetic ciphers, Poly-alphabetic ciphers.

1. **Mono-alphabetic ciphers:**

* In mono-alphabetic cipher, a character in the plain text is always changed to the same character in the cipher text regardless of its position.
* If the algorithm says, a letter “A” in the plain text is changed to “D”. Every occurrence of “A” is changed to “D”.
* Eg: plain text: “hello” - cipher text: “KHOOR”. The cipher is mono-alphabetic because both l’s are encrypted as O’s.
* Eg: plain text: “hello” - cipher text: “ABNZF”. The cipher is not mono-alphabetic because each ‘l’ is encrypted by a different character.

1. **Additive cipher:**

* The simplest mono-alphabetic cipher is the “Additive cipher”.
* It is also called as “Shift cipher” or “Caesar cipher”.
* Assume that the plain text consists of lower case letters and the cipher text consists of upper case letters.
* To apply mathematical operations on plain text and cipher text, we assign numerical values to each letter.

Plain text -> a b c d e …. w x y z

Cipher text -> A B C D E …. W X Y Z

Value -> 00 01 02 03 04 …. 22 23 24 25

* The secret key between sender (Alice) and receiver (Bob) is an integer.
* The encryption algorithm adds the key to the plain text character and the decryption algorithm subtracts the key from the cipher text character.
* In encryption, C = (P + k) mod 26 and in decryption, P = (C - k) mod 26. Where C means “Cipher text”, P means “Plain text”, k means “Key”.

1. **Multiplicative cipher:**

* This cipher is also similar to the “Additive cipher”.
* In this cipher, we use “multiplication” as the mathematical operation.
* In encryption, C = (P X k) mod 26 and in decryption, P = (C X k-1) mod 26. Where C means “Cipher text”, P means “Plain text”, k means “Key” and k-1 means the multiplicative inverse of key.
* To find out the multiplicative inverse, use “Extended Euclidean algorithm”.
* The Extended Euclidean algorithm finds the multiplicative inverse of ”b” in Zn, where “n” and “b” are given and gcd (n,b) =1.
* Algorithm:

r1 <- n; r2  <- b;

t1 <- 0; t2 <- 1;

while ( r2 > 0)

{

q <- r1 / r2;

r <- r1 – q X r2;

r1 <- r2; r2 < - r;

t <- t1 – q X t2;

t1 <- t2; t2 <- t;

}

if ( r1 = 1) then b-1 <- t1;

1. **Affine cipher:**

* It is the combination of both “Additive cipher” and “Multiplicative cipher”.
* In this cipher, we use a pair of keys. One key is used for “Multiplicative cipher” and one ley for “Additive cipher”.
* In encryption, C = (P X k1 + k2) mod 26 and in decryption, P = ((C – k2) X k1-1) mod 26. Where k1-1 is the multiplicative inverse of k1.

1. **Poly-alphabetic ciphers:**

* In this cipher, each occurrence of a character may have different substitute.
* The relationship between a character in the plain text to a character in the cipher text is “one-to-many”.

**Playfair cipher:**

* This cipher is used by the British army during World War-I.
* The secret key is made up of 25 alphabet letters arranged in a 5X5 matrix.
* In this cipher, the key can be constructed using a 5X5 matrix of letters using a “keyword”.
* There should be only a single occurrence of letter must be there in the “keyword”
* The matrix is constructed by filling the letters of the “keyword” from left-to-right and from top-to-bottom.
* And then fill the remaining matrix with remaining letters in alphabetical order.
* The letter “I” & “J” are assumed as a single letter.
* Eg: Keyword=MONARCHY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

Key=

* Before encryption, the letters of plain text is divided into pairs.
* If the letters in a pair is same, then add one bogus letter. (or) if the no.of letters in the plain text are “odd”, then add one bogus letter at the end.
* Eg: h e l l o - > h e | l l | o - > h e | l x | l o
* During encryption, consider each pair of letters at a time.
* If the letters in a pair are in the same row in the key matrix, then each letter is replaced by the letter to the immediate right. So that we can get the cipher text. Eg: “ar” is encrypted as “RM”.
* If the letters in a pair are in the same column in the key matrix, then each letter is replaced by the beneath (bottom) letter. So that we can get the cipher text. Eg: “mu” is encrypted as “CM”.
* If the letters in a pair are at random positions in the key matrix, then each letter is replaced by the letter of intersection points (row intersection point followed by column intersection point). So that we can get the cipher text. Eg: “hs” is encrypted as “BP”.

**Transposition Ciphers**

* This cipher doesn’t substitute one symbol with another. Instead of it, it changes the location (or) position of the symbols.
* A symbol in the 1st position of plain text may appear in the 5th position of cipher text.
* This cipher, reorders the symbols while transmission.
* These ciphers are categorized into 3 types:

1. Keyless transposition cipher.
2. Keyed transposition cipher.
3. Combined approaches.
4. **Keyless transposition cipher:**

* In this cipher there will be no key for conversion.
* There are 2 methods to reorder the symbols during transmission.

**Method-I:**

* In the first method, the text is written into a table (column by column) and then transmitted in row by row manner.
* This method is called “Rail fence cipher”. In this cipher, the plain text is arranged in column by column (zigzag pattern). The cipher text is created by reading the table row by row.
* Where as in decryption, the cipher text is divided into 2 halves. The first half forms the first row and the second half the second row. To get the plain text, read the table column by column.
* In this method, the no.of rows are fixed (i.e) “2”.

**Method-II:**

* In this method, both the sender and receiver must agree on the no.of columns.
* In this method, the text is written into a table (row by row) and then transmitted in column by column manner.

1. **Keyless transposition cipher:**

* In this cipher, first we will divide the plain text into groups of predetermined size, called “Blocks”.
* And then use a key to reorder the letters in each block separately.
* The key value must be used as the block size.
* If any block contains less no.of letters than the block size, then add bogus letters at the end of that block.

1. **Combined approaches:**

* In this approach both the encryption & decryption is done in 3 steps.
* First, the plain text is written into a table, row by row based on the no.of columns. (Key value is assumed as the no.of columns).
* Second, the permutation is done by reordering the columns using a key.
* Third, the new table is read column by column to get the cipher text.
* The 1st & 3rd steps are related to “Keyless transposition cipher” and 2nd step is related to “Keyed transposition cipher”.