Symmetric Key Cryptography

Classical Substitution Cipher

Here, letters of plaintext are replaced by other letters or by numbers or symbols, or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Ceasar Cipher

It is the earliest known substitution cipher. The approach was first used in military affairs. Here, each letter is replaced by 3rd letter on. An example can be:

Plain text: meet me after the toga party
Cipher text: PHHW PH DIWHU WKH WRJD SDUWB

So, Caesar cipher can be represented as

$c = E(k, p) = (p + k) \bmod (26)$
$p = D(k, c) = (c - k) \bmod (26)$

Mono Alphabetic Substitution

In Mono-alphabetic Substitution, each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter. For example,

Plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

The general system of symbol for symbol substitution is called a mono alphabetic substitution. ‘attack’ would be transformed into the cipher text ‘QZZQEA’.

Poly Alphabetic Substitution

A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes. For example, ‘a’ can be enciphered as ‘d’ in the starting of the text, but as ‘n’ at the middle.

Transposition Cipher

In classical **transposition** or **permutation** ciphers, the message is hidden by rearranging the letter order without altering the actual letters used.

Rail Fence Cipher

Message letters are written out diagonally over a number of rows and then the cipher is read off row by row. For example,

Plain text: meet me after the toga party

m e m a t r h t g p r y
e t e f e t e o a a t

Cipher text: MEMATRHTGPRYETEFETEOAAT

Row Transposition Cipher

It is a more complex transposition approach where letters of message are written out in rows over a specified number of columns and then the columns are reordered according to some key before reading off the rows.

Key: 41532
Plain text: the simplest possible transpositions

1	2	3	4	5
t	h	e	s	i
m	p	l	e	s
t	p	o	s	s
i	b	l	e	t
r	a	n	s	p
o	s	i	t	i
o	n	s	x	x

4	1	5	3	2
s	t	i	e	h
e	m	s	l	p
s	t	s	o	p
e	i	t	l	b
s	r	p	n	a
t	o	i	i	s
x	o	x	s	n

Cipher Text: s t i e h e m s l p s t s o p e i t l b s r p n a t o i i s x o x s n

Columnar Transposition Cipher

In Columnar transposition cipher, each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Plain text: meet me after the party
Keyword: HACK Order of alphabets in HACK: 3124

H	**A**	**C**	**K**
3	**1**	**2**	**4**
m	e	e	t
m	e	a	f
t	e	r	t
h	e	p	a
r	t	y	x

Cipher text: e e e e t e a r p y m m t h r t f t a x

Product Cipher

Ciphers using only substitutions or transpositions are not secure because of language characteristics. Hence, using several ciphers can be considered in succession to make harder.

- two substitutions make a more complex substitution
- two transpositions make more complex transposition
- but a substitution followed by a transposition makes a new much harder cipher

Steganography

Stenography is an alternative to encryption that hides existence of message. The technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected; for example, hiding in LSB in graphic image or sound file.

Data Encryption Standard (DES)

DES was Adopted by NIST in 1977. It is based on a cipher (Lucifer) developed earlier by IBM for Lloyd's of London for cash transfer. DES uses the Feistel cipher structure with 16 rounds of processing. DES uses a 56-bit encryption key. The key size was apparently dictated by the memory and processing constraints imposed by a single-chip implementation of the algorithm for DES. The key itself is specified with 8 bytes, but one bit of each byte is used as a parity check.

DES encryption was broken in 1999 by Electronics Frontiers Foundation (EFF, www.eff.org). This resulted in NIST issuing a new directive that year that required organizations to use Triple DES, that is, three consecutive applications of DES. Later, NIST initiated the development of new standards for data encryption. The result is Advanced Encryption Standard (AES).

Triple DES continues to enjoy wide usage in commercial applications even today. What is specific to DES is the implementation of the F function in the algorithm and how the round keys are derived from the main encryption key