Symmetric cipher model

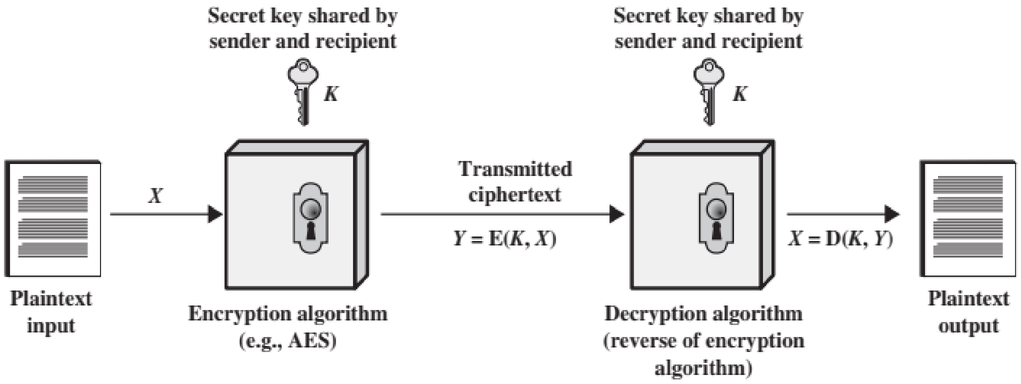

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D(K, Y)$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

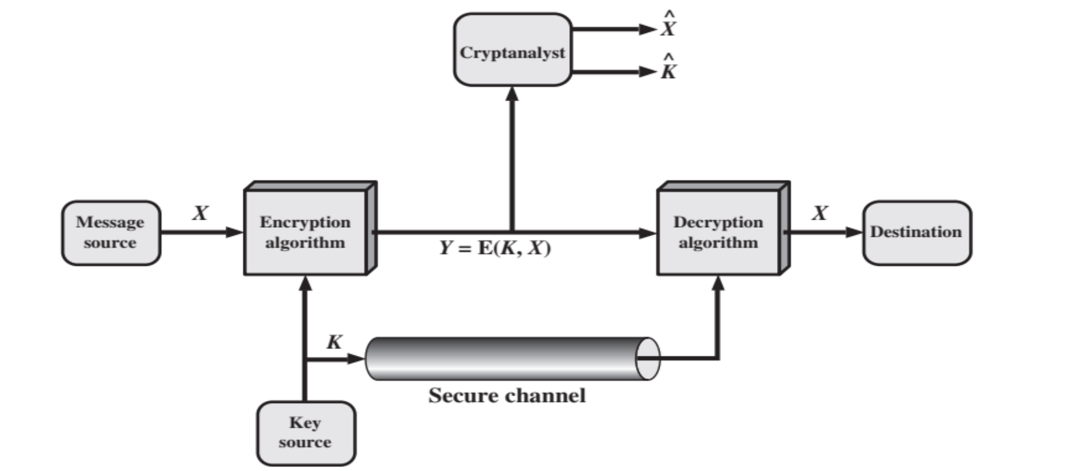
Symmetric cipher model

- **Plaintext: O**riginal intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Requirements for secure use of conventional encryption

- **1.** Strong encryption algorithm. Algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.
- The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
- **2.** Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.
- If someone can discover the key and knows the algorithm, all communication using this key is readable.

Model of Symmetric Cryptosystem



Characteristics of Cryptographic systems

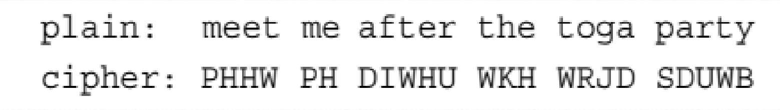
- **1. The type of operations used for transforming plaintext to ciphertext.** substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are 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 use different keys, 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.

Cryptanalysis and Brute-Force Attack

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm and some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible key.

Substitution Techniques

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- **Caesar Cipher**
  - The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.



```
plain:   meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

- General Caesar algorithm:

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

- Decryption algorithm:

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$

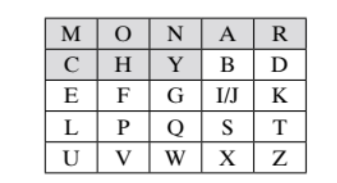
Characteristics used for Brute force Cryptanalysis

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

Monoalphabetic Ciphers

- A **permutation** of a finite set of elements *S* is an ordered sequence of all the elements of *S*, with each element appearing exactly once.
- if *S* = {a, b, c}, there are six permutations of *S*:
  abc, acb, bac, bca, cab, cba

Playfair Cipher

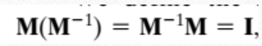
- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- Keyword “MONARCHY”
- 

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

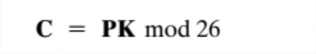
Playfair Cipher

- Plaintext is encrypted two letters at a time, according to the following rules:
- **1.** Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
- **2.** Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
- **3.** Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Hill Cipher

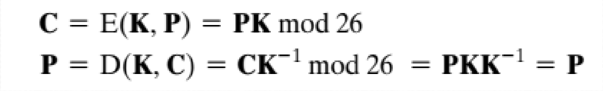


$$\mathbf{M}(\mathbf{M}^{-1}) = \mathbf{M}^{-1}\mathbf{M} = \mathbf{I},$$



$$\mathbf{C} = \mathbf{PK} \bmod 26$$

- Hill system can be expressed as :



$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

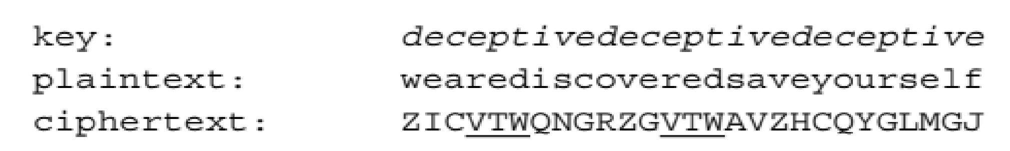
Polyalphabetic cipher

- Features
  - A set of related monoalphabetic substitution rules is used.
  - A key determines which particular rule is chosen for a given transformation.
- ***Vigenère Cipher***
- Assume a sequence of plaintext letters *P* = *p*0, *p*1, *p*2, c, *pn* - 1 and a key consisting of the sequence of letters *K* = *k*0, *k*1, *k*2, c, *km* - 1, where typically *m* 6 *n*. The sequence of ciphertext letters *C* = *C*0, *C*1, *C*2, c, *Cn* - 1 is calculated as follows:

$$
\begin{aligned}
C = C_0, C_1, C_2, \ldots, C_{n-1} &= \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, \ldots, k_{m-1}), (p_0, p_1, p_2, \ldots, p_{n-1})] \\
&= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26, \\
&\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26, \ldots
\end{aligned}
$$

Vigenère Cipher

- Example



```
key:                deceptivedeceptivedeceptive
plaintext:          wearediscoveredsaveyourself
ciphertext:         ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

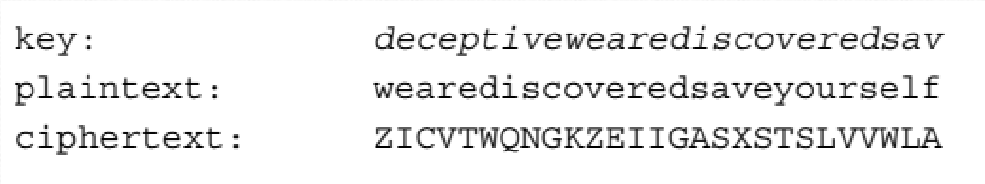
- Encryption

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

- Decryption

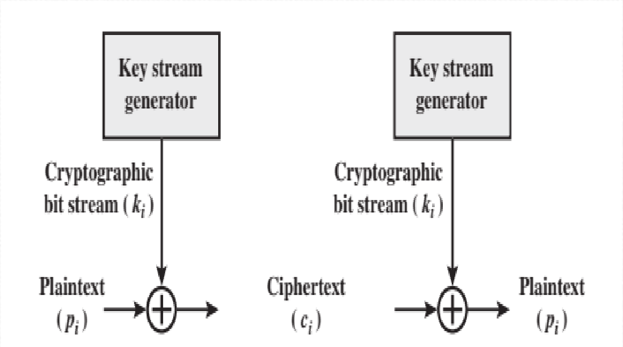
$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

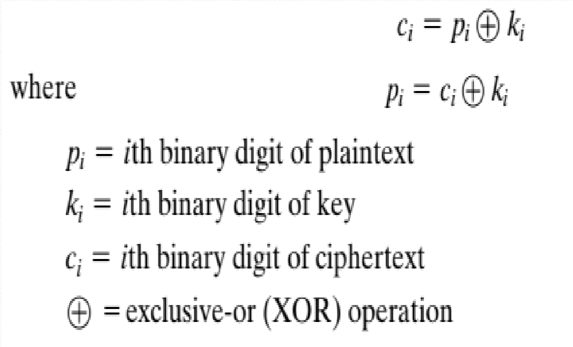
Vigenère Cipher

- The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself. Vigenère proposed an **autokey system**, in which a keyword is concatenated with the plaintext itself to provide a running key.
- 

```
key:           deceptivewearediscoveredsav
plaintext:     wearediscoveredsaveyourself
ciphertext:    ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Vernam Cipher





$$c_i = p_i \oplus k_i$$

where

$$p_i = c_i \oplus k_i$$

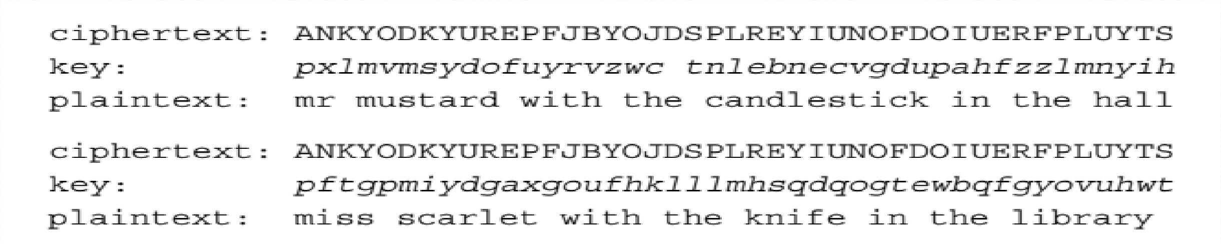
p_i = ith binary digit of plaintext

k_i = ith binary digit of key

c_i = ith binary digit of ciphertext

$\oplus$ = exclusive-or (XOR) operation

One-Time Pad

- Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.
- Each new message requires a new key of the same length as the new message. Such a scheme, known as a **one-time pad**, is unbreakable.
- 

```
ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext:  mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:        pftgpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext:  miss scarlet with the knife in the library
```

One-Time Pad

- If the actual key were produced in a truly random fashion, then the cryptanalyst cannot say that one of these two keys is more likely than the other.

Monoaphabetic Vs Polyalphabetic cipher

- Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.
- The relationship between a character in the plain text and the characters in the cipher text is one-to-one.

- Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The relationship between a character in the plain text and the characters in the cipher text is one-to-many.

Monoaphabetic Vs Polyalphabetic cipher

- Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.
- 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.

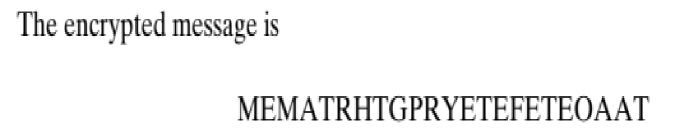
- Each alphabetic character of plain text can be mapped onto ‘m’ alphabetic characters of a cipher text.
- A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of the plain text character in the plain text stream

Monoaphabetic Vs Polyalphabetic cipher

- It is a simple substitution cipher.
- 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.
- Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.

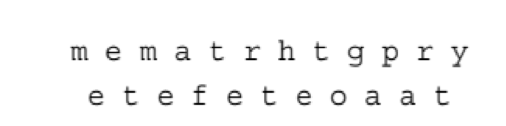
- It is multiple substitutions cipher.
- Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different cryptoalphabets.
- Polyalphabetic ciphers are much stronger.

Transposition techniques

- **Rail fence** technique
- “meet me after the toga party”
- 

  The encrypted message is

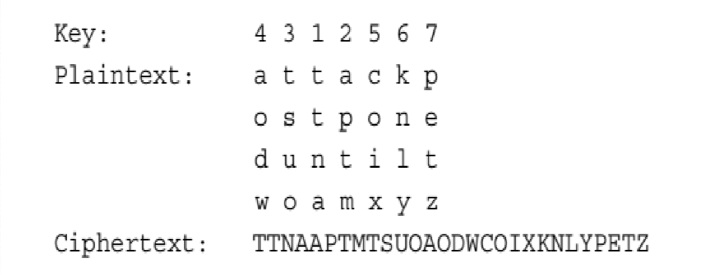
  MEMATRHTGPRYETEFETEOAAT



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

Transposition techniques

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm



```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```