Symmetric Key Algorithms.

- Shift Cipher
- Substitution Cipher
- Affine Cipher
- Hill Cipher
- Vigenere Cipher
- DES - Data Encryption Standard
- AES – Advanced Encryption Standard …

Shift Cipher (Caesar Cipher)

- Message – x; cipher text - y
- Key – k, where 0<=k<=25
- **Encryption**: $y = E_k(x) = (x+k)\%26$
- **Decryption:** $x = D_k(y) = (y-k)\%26$
- **Example.** Encrypt: wewillmeetatmidnight using shift cipher with key 11.
  - Ans: HPHTWWXPPELEXTOYTRSE
- **Note1.** Julius Caesar used k=3, so it is also called Caser cipher.
- **Note2.** (–r)%m= m-r when r<=m. (If s=-r, then (s+r)%m=0, so s+r=m, since m%m=0. i.e., s=m-r.
- In general, a%n=a-(floor(a/n)*n). Eg. -11%7=3, -7%9=2

Cryptanalysis of Caesar Cipher

- Brute force attack on key (i.e, exhaustive key search). Try for k=1, k=2, … k=25. Find the value of k for which you get meaningful form.
- **Example.** Perform cryptanalysis on the following cipher text: JBCRCLQRWCRVNBJENBWRWN
- **Ans:** Try for k=1→ iabqbkp…

  for k=2→ hzapaj…

  for k=3…for k=9→astitchintimesavesnine

Substitution Cipher

- Plain text – x, Cipher text – y.
- Key k = permutation of 0,1,2,…25.
- Encryption.
- Decryption.
- Example. Let key k=(3,10,21,…,25,13)

  abcdefghijklmnopqrstuvwxyz

  DKVQFIBJWPESCXHTMYAUOLRGZN (Key)

  Plaintext: ifwewishtoreplaceletters

  Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
- Cryptanalysis. Brute force attack- no of possible keys = 26! – takes time. Use frequency analysis

Affine Cipher

- Key k=(a,b), where a,b are integers %26 and gcd(a,26)=1
- Encryption: $y = E_k(x)=(ax+b)\%26$
- Decryption: $x=D_k(y)=a^{-1}(y-b)\%26$
- Example. Let k=(7,3). Then

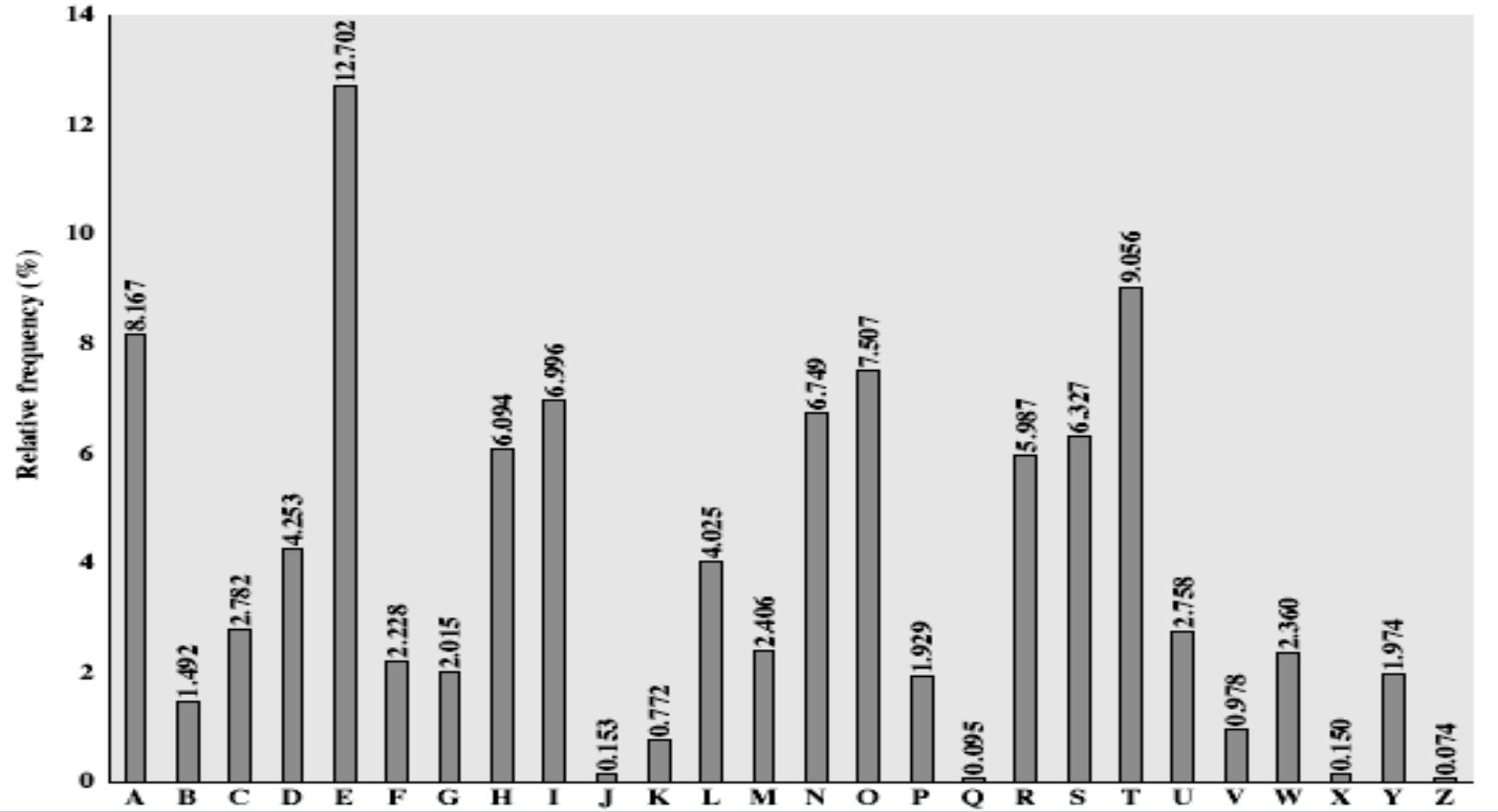
  $y = E_k(x)=(7x+3)\%26$ and

  $x=D_k(y)=7^{-1}(y-3)\%26$, where $7^{-1}=15$.

  Eg., hot→AXG

Cryptanalysis of mono-alphabetic substitution algorithms

- Generate tables of single, double & triple letter frequencies for various languages
- Eg. Single letter frequency for English is :
- Frequently used letters are: E,T,R,N,I,O,A,S
- Rarely used letters are: Z,J,K,Q,X.


Relative frequency (%)
0
2
4
6
8
10
12
14
8.167
1.492
2.782
4.253
12.702
2.228
2.015
6.094
6.996
0.153
0.772
4.025
2.406
6.749
7.507
1.929
0.095
5.987
6.327
9.056
2.758
0.978
2.360
0.150
1.974
0.074
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

Frequency cryptanalysis. Example.

- given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- count relative letter frequencies – P has the highest frequency and then Z has next higher frequency...
- guess P & Z are e and t
- guess ZW is ‘th’ and hence ZWP is ‘the’
- proceeding with trial and error finally get:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Poly-alphabetic Substitution algorithms- Playfair cipher

- Instead of encrypting character by character, playfair encrypts pair by pair.
- Algorithm:
- Generate a 5X5 matrix of letters based on a keyword

  fill in letters of keyword (remove duplicates)

  fill rest of matrix with other letters

  eg. using the keyword MONARCHY

Playfair…

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…

- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X’
  2. if both letters fall in the same row, replace each with letter to right (i.e., row successor) (wrapping back to start from end)
  3. if both letters fall in the same column, replace each with the letter below it (i.e., column successor) (again wrapping to top from bottom)
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Playfair…

- Decrypting works exactly in reverse
- Example. Encrypt balloon and verify the process by decrypting it.

Hill Cipher

- Key K= m x m matrix invertible over integer mod 26
- Encrypts m letters at a time.
- Encryption. $y = E_k(x) = xK$ (here x is of length m)
- Decryption. $x = D_k(y) = yK^{-1}$

Example.

- Key K= 11 8 So K^{-1} = 7 18
  3 7 23 11
- Plain text: july
- ju → (9 20) → (9 20) K = (3 4) →DE
- Cipher text: DELW
- Example 2. Let k= 10 5 12
  3 14 21
  8 9 11

Vigenere Cipher

- key is multiple letters long
- use each alphabet in turn
- repeat from start after d letters in message
- decryption works in reverse

Example of Vigenère Cipher

- write the plaintext
- write the keyword repeated above it
- use each key letter as a caesar cipher key (Refer Vigenere table)
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Autokey Cipher

- ideally want a key as long as the message
- keyword is prefixed to message as key
- knowing keyword can recover the first few letters
- use these in turn on the rest of the message
- but still have frequency characteristics to attack
- eg. given key *deceptive*

  key: deceptivewearediscoveredsav
  plaintext: wearediscoveredsaveyourself
  ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA

One-Time Pad

- if a truly random key as long as the message is used, the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- can only use the key **once** though
- problems in generation & safe distribution of key

Permutation Cipher Algorithms
Rail Fence cipher

- write message letters out diagonally over a number of rows
- then read off cipher row by row
- eg. write message out as:

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

- giving ciphertext

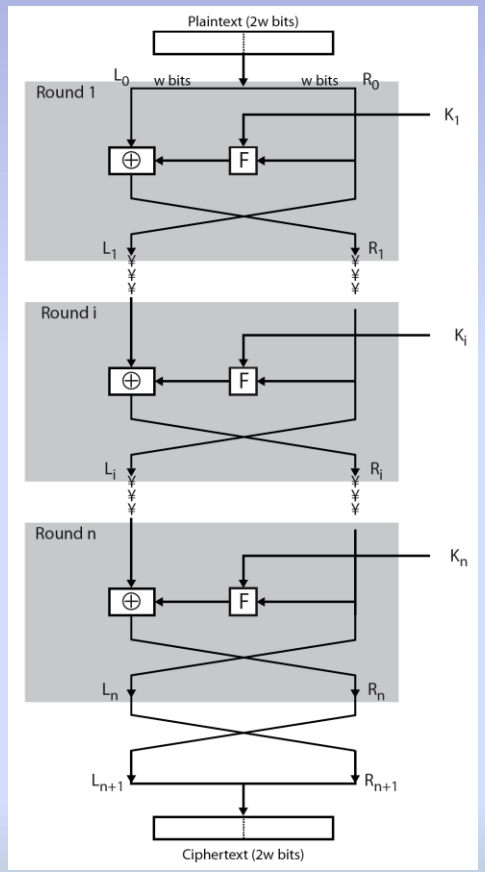
```
MEMATRHTGPRYETEFETEOAAT
```

Row Transposition Ciphers

- write letters of message in rows over a specified number of columns
- then reorder the columns according to some key before reading off the rows

Key: 3 4 2 1 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

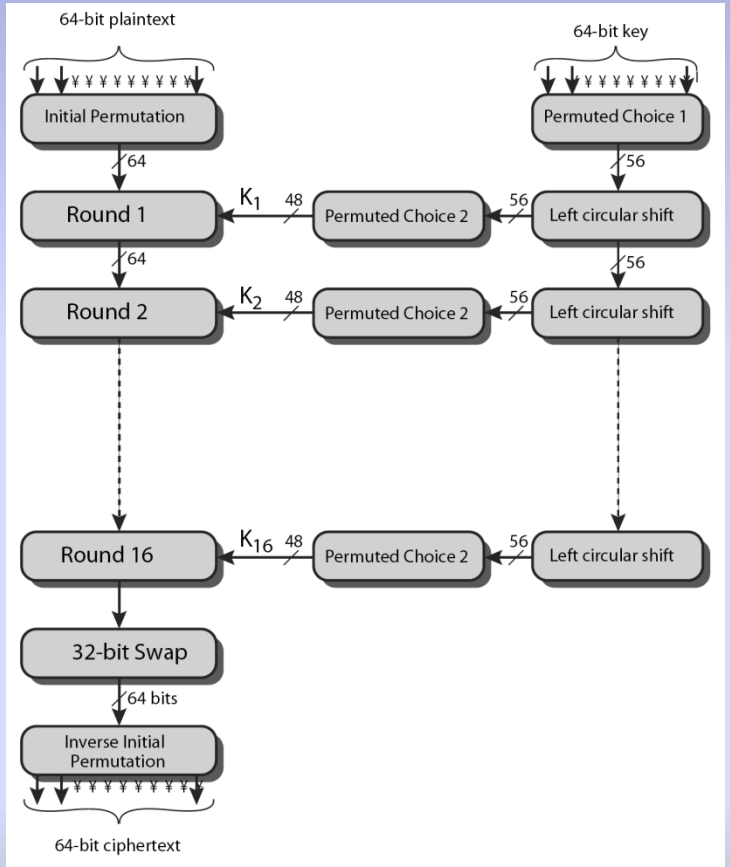
Feistel Cipher Structure



Feistel Cipher Design Elements

- block size
- key size
- number of rounds
- subkey generation algorithm
- round function
- fast software en/decryption
- ease of analysis

DES Encryption Overview



Drawback of Secret Key Crypt

- **Key Distribution** – Safe and authenticated distribution of keys – very difficult – condition worsens when keys are changed frequently
- **Key Management**: N nodes in a n/w => N-1 keys with each node.
- **Difficult** to provide Digital Signature schemes that provide **non-repudiation** services.
- **Solution:** Public Key Cryptography (PKC)