Cairo University
Faculty of Engineering
Computer Engineering Dept.

Sheet 2

Chapter2

1) What is the difference between an unconditionally secure cipher and a computationally secure cipher?

2) Briefly define the **Caesar** cipher.

3) This is a cipher text "GCUA VQ DTGCM" generated using the Caesar cipher where the key is C. Extract the plain text.

4) Briefly define the **monoalphabetic** cipher.

5) A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword CIPHER, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

plain: 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

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

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

C I P H E R

A B D F G J

K L M N O Q

S T U V W X

Y Z

This yields the sequence:

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

Such a system is used in the following example:

Plaintext:
“it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in Moscow”

Ciphertext:
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ

Determine the keyword.

6) Briefly define the **Playfair** cipher.

7) When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:
KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBNT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ
The key used was *royal new zealand navy*.
Decrypt the message. Translate TT into tt.

8) Using the **Vigenère** cipher, encrypt the word “explanation” using the key *leg*.

9) Using the **Autokey** cipher, encrypt the word “explanation” using the key *leg*.

10) Using the **Rail Fence** cipher, decrypt the message “TEKOOHRACIRMNREATANFTETYTGHH” using key/depth=4.

11) Using the **Row Transposition** cipher, encrypt the message “thirdyearcomputer” using key=43215.

Chapter3

12) Explain the avalanche effect.

13) What is the purpose of the S-boxes in DES?

Chapter6

14) What is triple encryption?

15) What is a meet-in-the-middle attack? When can it happen?

16) Describe how triple-DES works.