Mid Term Paper

Subject: Adv. Network Security

Name: Noreen

ID: 14839

Submitted to Dr. Sheeraz Ahmed

Program: MSCS

Q. Apply the following 3 codes:

(a) Monoalphabetic Cipher **(b)** Playfair Cipher **(c)** Vigenere Cipher

(a) Monoalphabetic Cipher:

Definition:

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

Monoalphabetic Cipher substitutes one letter of the alphabet with any random letter from the alphabet.

Possible Combination: **26! =24x10^{26}** Possibilities

Plain Text:

Components for these systems are now commercially available, and it seems very likely that quantum cryptography will be an important technology long before quantum computers of useful size are constructed.

Method:

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

Plain text:

Components for these systems are now commercially available, and it seems very likely that

TGEHGFVFLK WGJ LYVKV KQKLVE RJV FGO TGEEVJTZRDDQ RNRZDRSDV RFU ZL KVVEK NVJQ DZCVDQ LYRL

quantum cryptography will be an important technology long before quantum computers of

IMRFLME TJQHLGXJRHYQ OZDD SV RF ZEHGJLRL LVTYFGDGXQ DGFX SVWGJV IMRFLME TGEHMLVJK GW

useful size are constructed.

MKVWMDV KZAV RJV TGFKLJMTLVU.

Cipher text:

TGEHGFVFLK WGJ LYVKV KQKLVE RJV FGO TGEEVJTZRDDQ RNRZDRSDV RFU ZL KVVEK NVJQ DZCVDQ LYRL

IMRFLME TJQHLGXJRHYQ OZDD SV RF ZEHGJLRL LVTYFGDGXQ DGFX SVWGJV IMRFLME TGEHMLVJK GW

MKVWMDV KZAV RJV TGFKLJMTLVU.

(b) Playfair Cipher:

- The **Playfair cipher** was the first practical digraph substitution cipher.
- The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher.

Encryption Technique

For the encryption process let us consider the following example:

Key: monarchy
Plaintext: instruments

The Playfair Cipher Encryption Algorithm:

The Algorithm consistes of 2 steps:

1. **Generate the key Square(5×5):**
   - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext.
   - Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets).
   - If the plaintext contains J, then it is replaced by I.
   - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

For example:

The key is "**monarchy**"
Thus the initial entires are
'm', 'o', 'n', 'a', 'r', 'c', 'h', 'y'
followed by remaining characters of
a-z(except 'j') in that order.

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

2. **Algorithm to encrypt the plain text:**
   The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Rules for Encryption:

- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).

  For example:
  Diagraph: "me"
  Encrypted Text: cl

  Encryption:
  m -> c
  e -> l

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

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

For example:

Diagraph: "st"
Encrypted Text: tl
Encryption:
s -> t
t -> l

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

- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

  For example:

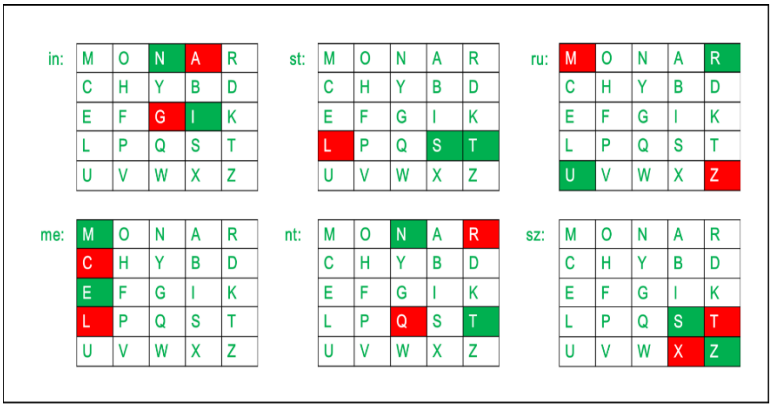
Diagraph: "nt"
Encrypted Text: rq
Encryption:
n -> r
t -> q

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

For example:

Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:
i -> g
n -> a
s -> t
t -> l
r -> m
u -> z
m -> c
e -> l
n -> r

t -> q
s -> t
z -> x



Answer:

Keyword: MONARCHY

Plain text:

Components for these systems are now commercially available, and it seems very likely that quantum cryptography will be an important technology long before quantum computers of useful size are constructed.

Making Pairs:

Co mp on en ts fo rx th es se sy st em sx ar ex no wx co mm er ci al ly av ai la bl ex, an dx it se em sx ve ry li ke ly th at qu an tu mx cr yp to gr ap hy wi ll be an im po rt an tx te ch no lo gy lo ng be fo re qu an tu mx co mp ut er sx of us ef ul si ze ar ex co ns tr uc te dx.

Cipher text:

HMOLNAGMLTPHDZCFLIQBTLLCXBMKANUYNOCLMDSBSUBNXOESBIULRABKLTIUALUF
NDSEEFQCPDRSLWRALZCENDQLNFMRVFGNESSCIMAGOLNMSRRQLKHYANPMQGPMY
QCIPHMKLWRALZCENOLVLKATHPXLFGMUXSUKRMLENATLMZDLKC

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

(c) Vigenere Cipher:

This scheme of cipher uses a text string (say, a word) as a key, which is then used for doing a number of shifts on the plaintext.

For example, let's assume the key is 'point'. Each alphabet of the key is converted to its respective numeric value: In this case,

p → 16, o → 15, i → 9, n → 14, and t → 20.

Thus, the key is: 16 15 9 14 20.

Process of Vigenere Cipher:

- The sender and the receiver decide on a key. Say 'point' is the key. Numeric representation of this key is '16 15 9 14 20'.
- The sender wants to encrypt the message, say 'attack from south east'. He will arrange plaintext and numeric key as follows −

a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14

- He now shifts each plaintext alphabet by the number written below it to create ciphertext as shown below −

a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H

- Here, each plaintext character has been shifted by a different amount – and that amount is determined by the key. The key must be less than or equal to the size of the message.
- For decryption, the receiver uses the same key and shifts received ciphertext in reverse order to obtain the plaintext.

Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H
16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14
a	t	t	a	c	k	f	r	o	m	s	o	u	t	h	e	a	s	t

Answer:

Key Word: technology

Representation of the key “technology” is ‘19 4 2 7 13 14 11 14 6 24’

Plaintext:

Components for these systems are now commercially available, and it seems very likely that quantum cryptography will be an important technology long before quantum computers of useful size are constructed.

Cipher text:

VSOWBBPBZQYSTAUSDSYWLXGTFOCSTMUPGQTZSCQOYEPAHTOWZGPEI
CUQWEGYCFWXLEMWQCECVONHBIGLMYNPFJZMZVCWUMKOJEFGHAWXD
UPMEPAGSNVTMESIFYCYUHCYSTLDILBZSFGQTCIESXRHJWZRTFTYGSICYR
QZBYRKYEARR.