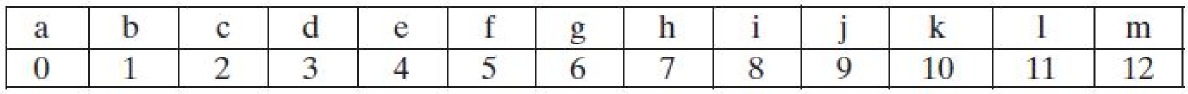
Sri Lanka Institute of Information Technology
Introduction to Cyber Security
Lab Sheet 2
Year 2, Semester 1

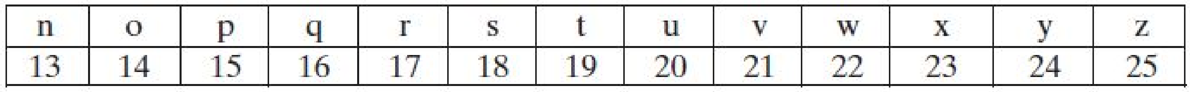
Caesar cipher

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2... 'z'=25.



a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12



n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

We can now represent the Caesar cipher encryption function, E(k, p), where p (plaintext) is the character we are encrypting, and k is the key (the shift) applied to each letter.

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

The decryption function D(k, C) is simply;

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

Exercise 1: Encrypt the following plaintext into ciphertext using Caesar cipher.

i. Key = 3

Plaintext	E	N	C	R	Y	P	T	I	O	N
Ciphertext										

ii. Key = 13

Plaintext	C	R	Y	P	T	O	L	O	G	Y
Ciphertext										

iii. Key = 24

Plaintext	W	H	E	R	E	A	R	E	Y	O	U
Ciphertext											

Exercise 2: Decrypt the following ciphertext into plaintext using Caesar cipher.

i. Key = 4

Ciphertext	T	E	W	W	Z	S	V	H
Plaintext								

ii. Key = 12

Ciphertext	U	‘	X	X	F	T	U	Z	W	M	N
Plaintext											

Ciphertext	A	G	F	F	T	M	F				
Plaintext											

Exercise 3: Develop a python or C language program to encrypt and decrypt any plaintext or ciphertext.

<u>Vigenère square</u>

Example

Plaintext: Authentication

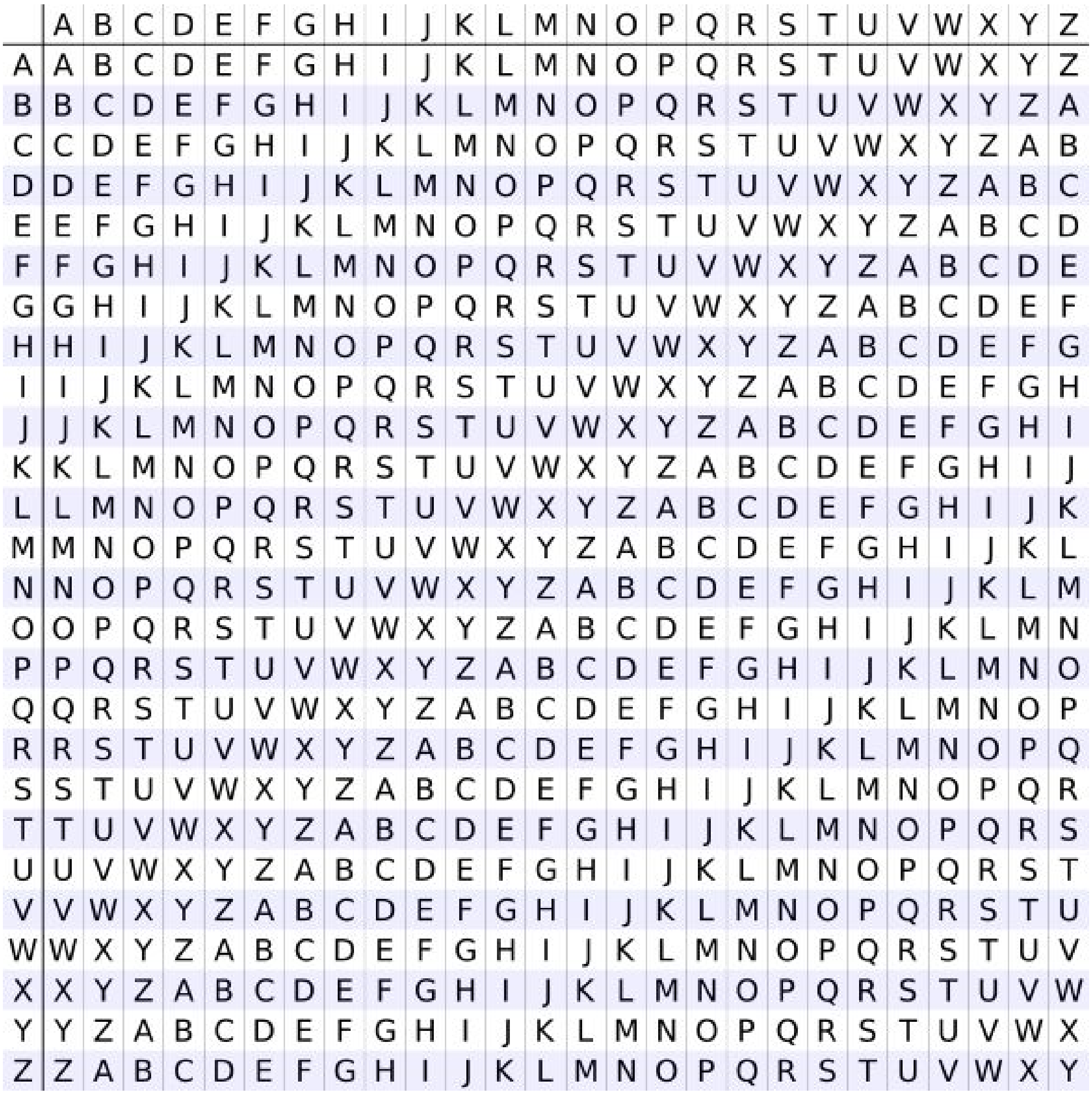
Key: MAP

Coded Message:

Plaintext	A	U	T	H	E	N	T	I	C	A	T	I	O	N
Key	M	A	P	M	A	P	M	A	P	M	A	P	M	A
Cipher text														

Ciphertext:

M	U	I	T	E	C	F	I	R	M
T	X	A	N						



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

Figure 2.1 – Vigenère square/ table

Exercise 4: Encrypt the following plaintext into ciphertext using Vigenère cipher table.

Plaintext: Thiswashardtobreakbecausetherewerenospace

Key: WORD

Exercise 5: Decrypt a ciphertext given by your friend using Vigenère cipher table. The message should contain more than 10 characters.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security
Lab Sheet 2
Year 2, Semester 1

Steganography

Exercise 6: Use Steganography to Embed a Secret Message in a Graphic

In this part of the lab, you create a secret message for your partner, embed it into a graphic file, and then give it to your partner to retrieve it. You embed the message in a graphic file using S-Tools. S-Tools is a steganography tool that hides files in BMP, GIF, and WAV files. You start by opening S-Tools and then drag graphics and sounds into the blank window. To hide files, you drag them into open graphics or sound windows. Data is compressed before being encrypted and then hidden.

Step 1: Download and install S-Tools.

If the S-Tools application is not installed on the PC, download it from https://www.insecure.in/steganography.asp or another site and unzip the files to a folder.

Step 2: Create a secret message text file (both partners).

a. Open the Windows Notepad application and create a message.

b. Save the message in a folder on the desktop and name it **secret.txt.**

c. Close the Notepad application.

Step 3: Create a simple .bmp graphics file.

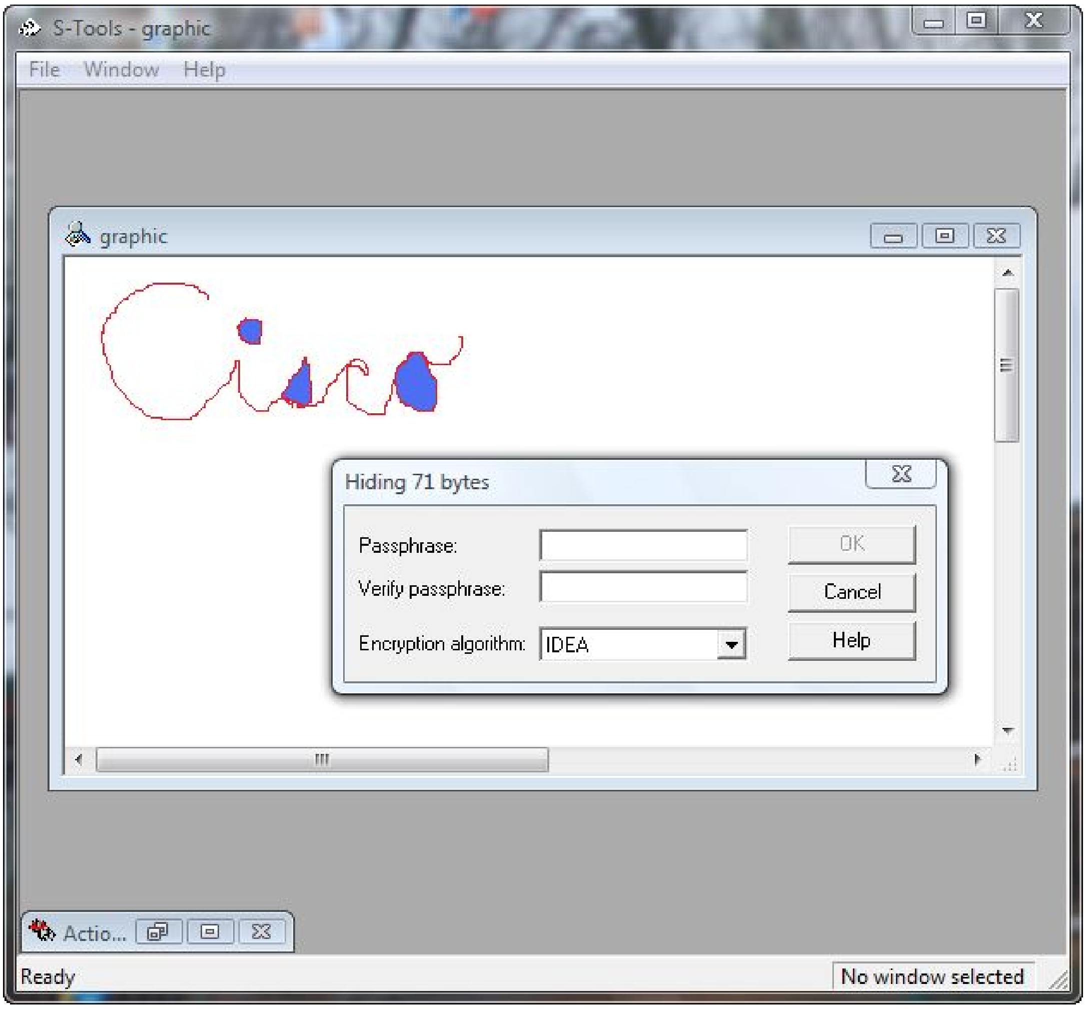
a. Open the Windows Paint application and create a simple graphic. For example, you can write your first name using the pencil tool or text tool and apply some color using the spray can or fill tool.

b. Save the graphic as a .bmp file in a folder on the desktop and name it **graphic.bmp**.

c. Close the Paint application.

Step 4: Create a secret passphrase.

a. Choose a passphrase and record it here. Do not share the passphrase with your partner. This passphrase will be used later to protect the text file when it is embedded in the graphics file.



Hiding 71 bytes

Passphrase:

Verify passphrase:

Encryption algorithm: IDEA

Step 5: Embed the message into a graphic image file.

a. Open the S-Tools.exe application.

b. Locate the file named **graphic.bmp,** which you saved previously. Determine its size by right-clicking the file and selecting **Properties**. Record the file size, for example 2,359,350 bytes.

c. Drag the **graphic.bmp** file into the S-Tools window.

d. Drag the file **secret.txt**, which you created in Step 2, and place it inside the **graphic.bmp** window. The image should still be displayed. A dialog box is displayed showing the number of bytes being hidden. You can enter a passphrase and select the encryption algorithm to be used. The default algorithm is IDEA.

Step 6: Use the unencrypted passphrase to protect the embedded text file.

a. Enter the unencrypted passphrase from Step 4 in the **Passphrase** and **Verify passphrase** fields.

b. Choose **Triple DES** from the **Encryption Algorithm** field and click **OK**. This creates a second image with the name “hidden data”.

c. Right-click the hidden data graphic image and choose **Save As** from the menu. Name the file **graphic2** and save it as a bmp file.

d. Close the S-Tools application.

Step 7: Provide the graphic2.bmp file to your partner.

a. Provide a copy of your **graphic2.bmp** file to your partner. You can do this by sharing folders. You can also copy the file onto a removable drive (flash drive or floppy disk), or send it as an email attachment if you are performing the lab remotely.

b. Provide your partner with the Vigenere-encrypted passphrase from Step 4 and the cipher keyword that you used to create it.

Step 8: Reveal the embedded message from your partner.

a. Open the S-Tools application.

b. Locate the **graphic2.bmp** file from your partner, and determine how large it is using the same method as in Step 5. Record the file size here.

c. Has the file size changed?

d. Drag the file into the S-Tools window. The image should be displayed. Can you tell that there is a secret message embedded in the graphic image?

e. Right-click the image and choose **Reveal** from the menu.

f. Enter the passphrase into the **Passphrase** field.

g. Choose **Triple DES** from the **Encryption Algorithm** field and click **OK**. This displays a revealed archive.

h. Right-click the hidden message file and choose **Save As** from the menu. Name the file **secret2.txt**.

i. Close the S-Tools application.

j. Open the **secret2.txt** file from your partner to reveal the hidden message and write it here.

Sri Lanka Institute of Information Technology
Introduction to Cyber Security
Lab Sheet 2
Year 2, Semester 1

Follow the steps provided in the below link

Exercise 7(Homework) :

http://www.computersecuritystudent.com/FORENSICS/Steganography/lesson1/index.html and create a video of the process that you have followed.