3/28/2011 - Spring 2011

CS 101 Lab 8

Encryption *Paul Cao*

The superior man, when resting in safety, does not forget that danger may come. When in state of security he does not forget the possibility of ruin. When all is orderly, he does not forget disorder may come. Thus his person is not endangered and his states and all their clans are preserved."

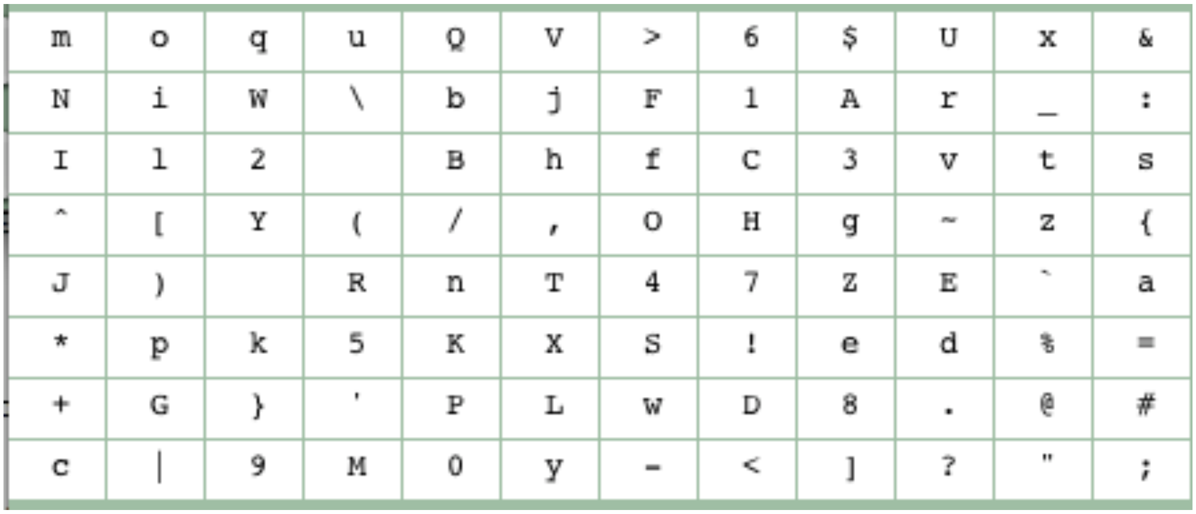
-Confucius (551 BC - 479 BC)

The lab report is due before class on Wednesday 3/30/2011. You need to write your answers for all the exercises in a word file. Submit your word file through the lab6 dropbox on angel.

The purpose of this lab is to experiment data encryption through a simple block encryption algorithm.

Data encryption plays a major role in compute applications, ranging from simple logins for system accounts to secure transmission of information over a network. The purpose of data encryption is to transform data into a secure form so they can be accessed only by those who have authorization to do so. In this lab, we assume that the datum is a string of characters. This datum is input to the encryption algorithm, which outputs another string in encrypted or encoded form. The encoded string can in turn be input to a decryption algorithm to recover the original string.

The algorithm used in this lab works as the following. It employs a data structure called an encryption matrix. The encryption matrix is a two-dimensional grid of characters. The grid has 8 rows and 12 columns. Thus, there are just enough cells in the grid to hold the 96 printable characters. The characters are inserted into the encryption matrix in random order, as shown in the figure below.



m	o	q	u	Q	V	>	6	$	U	x	&
N	i	W	\	b	j	F	1	A	r	_	:
I	1	2		B	h	f	C	3	v	t	s
^	[	Y	(	/	,	O	H	g	~	z	{
J	)		R	n	T	4	7	Z	E	`	a
*	p	k	5	K	X	S	!	e	d	%	=
+	G	}	'	P	L	w	D	8	.	@	#
c	|	9	M	0	y	-	<	]	?	"	;

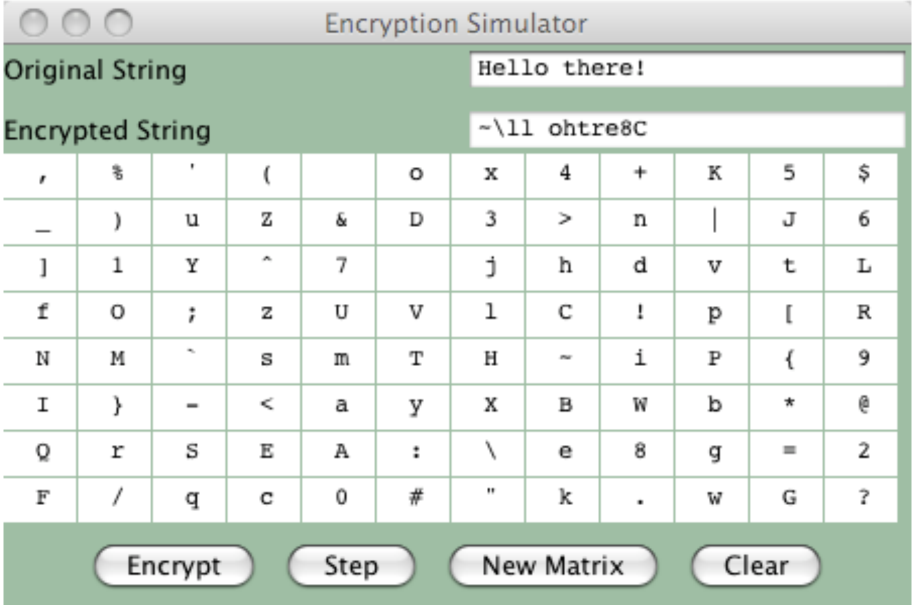
Informally, the encryption algorithm uses the encryption matrix as follows:

1. Scan through the input string from left to the right, two characters at a time
2. Locate the positions of a given pair of characters in the encryption matrix.

3. If these positions are in the same row or the same column, then swap the characters in the input string to form an encoded pair of characters.
4. Otherwise, locate the characters at the remaining corners of the rectangle formed by these positions, and use these characters to form an encoded pair of characters.
5. Concatenate all of the encoded pairs of characters to form the output string.
6. If the length of the input string is odd, append the last character of the original input string to the output string.

You will discover how to decrypt the encoded message in the lab.

1. Running the encryption simulator
Launch the encryption simulator by clicking the lab software's **Encryption Simulator** button. Enter the string "Hello there!" in the **Original String** filed and click the **Encrypt** button. The encrypted string should appear in the **Encrypted String** field. A sample run is shown below. In your simulator, try to encrypt the same message and observe the encrypted string.



Original String: Hello there!

Encrypted String: ~\ll ohtre8C

,	%	'	(		o	x	4	+	K	5	$
_	)	u	Z	&	D	3	>	n	|	J	6
]	1	Y	^	7		j	h	d	v	t	L
f	O	;	z	U	V	l	C	!	p	[	R
N	M	`	s	m	T	H	~	i	P	{	9
I	}	-	<	a	y	X	B	W	b	*	@
Q	r	S	E	A	:	\	e	8	g	=	2
F	/	q	c	0	#	"	k	.	w	G	?

Q1:/ Is your encrypted string the same as shown above? Briefly explain the reason.

2. Stepping through the process
Click **Clear** to clear the data fields and enter the string "Hello again." Then click **New Matrix** to generate a new encryption matrix. Instead of clicking **Encrypt,** repeatedly click the **Step** button and observe the changes in the encryption matrix. As you step through the encryption process, each pair of encoded

characters (the ones shaded in the matrix) is added to the encrypted string. Visually locate the rectangle formed by each pair of original characters and their encodings.

Q2:/ Describe what happens in the following situations
A pair of characters falls in the same row or column in the matrix

The last character (the odd one) is process

Q3:/ According to your observation so far, please rewrite the step 4 of the encryption algorithm to specify the order in which the characters found at the remaining corners of the rectangle are used.

Q4:/ When repeating characters, such as AABBCC are being encrypted, describe what is peculiar about the encoded string and explain why this happens.

3. Decryption
Enter a short phrase and encrypt it. Now copy the encrypted string and click the **Clear** button. Enter the encrypted string as the original string and click the **Encrypt** button.

Q5:/ What is the result? Explain briefly.

When you finished the lab, please log-off the computer.