CAESAR CIPHER ENCRYPTION

IN C AND C++

A PROJECT REPORT

BY

Name : Mohammad Areeb Ahmad

E-mail id : m.areeb.ahmad@gmail.com

Date : April 22,2020

Certificate Of Declaration

This is to certify that I, Mohammad Areeb Ahmad have worked on the “Caesar Cipher Encryption in C and C++” on 22nd of the month of April, 2020. This project has been undertaken to my interest and it doesn’t include influence of any other organization.

Name : Mohammad Areeb Ahmad

E-mail id : m.areeb.ahmad@gmail.com

- **Overview :**

Encryption refers to changing the plain text to a coded message text often referred to as a cipher text using a particular key of encryption. The same key could be used to decrypt the message and get the plain text back from the cipher text. The Caesar cipher encryption is one of the oldest method to encrypt the information sent by the sender. This method is being used since the ancient Roman civilization. As the name hints, Caesar cipher dates back to the kingdom of ancient Rome under Julius Caesar. It was during his reign that this encryption method was first used. The messages sent by the officials of the king's office were encrypted using a shift key, about which no other person had the idea except the sender and the receiver of the message. The original message was replaced using a shift key number to use use next alphabet instead of the original one. This ensured that the message was not decrypted by any intermediate source.

A 'Shift Key' is used in the encryption process. The original message is converted into the cipher message by using shift keys. Shift key adds the number of shift value to the original message to get the encrypted message.

Here, in this case we have done the encryption using ASCII Value (American Standard Code for Information Interchange).

Every alphabet, be it in upper case/ lower case, digits, space and special symbols are represented using a specified number. This entire representation is called ASCII value representation.

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

- ## Objectives of The Project :

The objective of the project is to recreate and understand the ancient encryption method properly so that the present method could be understood in a better way.

- **Languages Used :** C and C++ Programming Languages.
- **Software Used :** Dev C++

- ## Details and Discussion :

The Caesar Cipher has been implemented using string arrays and for loop.

1. **<u>String Array :</u>**
   When data is stored in continuous memory location, it is called and Array. Typically, an array can store only one type of data-type. This makes it different from structures and unions.
   The index of the string array represents the maximum number of characters the array can hold of the string data-type. The string array of 'n' index number can store a maximum of (n-1) characters because the string array terminates with a NULL character represented by \0.
   Use of sign of 'Ampersand' is not allowed while dealing with string array as strings are pointers itself and does not require ampersand, which is represented by '&'.
   The syntax for declaration is :

   String Array_Name[SizeOfArray];
   Or
   String Array_Name[SizeOfArray]={'c','h','a','r','a','c','t','e','r','s'}

By default, the string array ends with a null value(\0).

2. For loop :

For loop is used in order to counter the need of repeating conditions. This loops helps us to execute a particular statement/group of statements till a particular condition goes false.

The syntax of declaration is :

loop variable declaration;
for(loop variable initialization; loop condition; loop variable updation)
{

Block of statements to be executed
(When the condition is true);

}

- **C Language :**

(Use of printf and scanf functions has been made in C order to get the input and the output in the program.)

In C language, we first include the stdio.h header file to get the input and output in our program, stdio.h represents, standard input output header file.

We then declare the variable i(loop variable) and shift (the shift key) of integer data-type.

The string array is then declared and initialized with 0 value.

We then ask for the user's input in the form of plain text.

Followed by the value of the shift key.

We then encounter a loop, which ranges till 99 that is less than 100. We did not take the 99 index value in the loop condition because the string array by default ends with a null character or \0.

The output is then given in the form string. This output is now the cipher text as it has been encrypted with the value of shift key as given by the user.

- **C++ Language :**

(Use of objects such as cin and cout has been made in C++ in order to get the input and the output in the program.)

In c++, we first include the iostream for input and output of the program, iostream means input output stream.

We then declare the variable i(loop variable) and shift (the shift key) of integer data-type.

The string array is then declared and initialized with 0 value.

We then ask for the user's input in the form of plain text.

Followed by the value of the shift key.

We then encounter a loop, which ranges till 99 that is less than 100. We did not take the 99 index value in the loop condition because the string array by default ends with a null character or \0.

The output is then given in the form string. This output is now the cipher text as it has been encrypted with the value of shift key as given by the user.

- **Challenges To The Project :**

  - The entire encryption and decryption methodology is based on just one value of the shift key.
  - Finding/ leaking of the shift key could lead to disastrous consequences to the security of the message.
  - The message could be then used for malicious actvities.