CISC4080 Computer Algorithms Homework (3)[1]

[1] Distinguish yourselves, folks!

Part A: Basic Number Theory (10 points)

Prove the following statements (10 points)

- 1. If $a|b$ and $a|c$, then $a|(mb+nc)$, where $m,n \in \mathbb{Z}$
- 2. If $m|(a-b)$, then . $a\,mod\,m = b\,mod\,m$, where $m \in \mathbb{Z}^+$
- 3. If $a\,mod\,m = b\,mod\,m$, then m|(a-b), where $m \in \mathbb{Z}^+$

Part B: A Shift Cipher (20 points)

How do Banks communicate each other in wire-transfer?

The main cryptosystem used in financial industry is AES: advanced encryption standard. It is officially called private key cryptosystem, where a private key, which is a number or a combination of a sequence of numbers. In the communication, only the two parities: Bank A and Bank B know the private key. The key is usually very long numbers to prevent possible brute-force attack (try all cases) . The key used in AES has 128-bits.

Shift cipher basics

Its baby model is called Shift cipher in cryptography. Cryptography is knowledge about "secrete writing", where "crypt" means secrete and "graphy" means writing.

The basic idea is to replace original message, which is usually called plaintext with ciphertext, which is the encrypted message. The process to convert plaintext to ciphertext is called encryption. Alternatively, the process to retrieve the original message from ciphertext is called decryption.

- The encryption process is a function $c = e(x)$, where x represents input message and c is its corresponding encrypted message (ciphertext)
- The decryption process is the inverse of the previous function that retrieves the plaintext: $x = d(c)$

Julius Caesar gave the one of the earliest shift ciphers. He shifted each letter by three places (slots) in the alphabet (e.g., A–>D, B–>E,..., and Z–>C). The last of the alphabet wrapped around to the beginning. This idea can be generalized to shift k slots to encrypt a message and shift back k slots to decrypt the message. It is called *shift cipher* or *Caesar cipher.*

The plaintext : "MEET YOU IN THE PARK" has corresponding ciphertext " PHHW BRX LQ WKH SDUN" under a shift cipher, where each letter moves three slots. To retrieve the original message, we need to move 3 slots back for each letter in the ciphertext.

- Considering alphabet {A,B,C,D,...,Z} is generally represented by the set $D = \{0, 1, 2, ..., 25\}$ through mapping $A \rightarrow 0$, $B \rightarrow 1 \cdots Z \rightarrow 25$ respectively, the encryption and decryption are equivalent to the following functions:

  Encryption: for each $x \in D$, it is encrypted as $y = (x+k)\,mod\,26$,$(f(x) = (x+k)\,mod\,26)$ where k is the number slots that each letter will move, $0 < k \leq 25$. The number k is also called the key for the shift cipher. *The key must be only known by the message sender (Alice) and receiver (Bob).*

  Decryption: for each y, it is decrypted as , $x = (y-k)\,mod\,26$ (it is encryption function's inverse function: $f^{-1}(x) = (x-k)mod\,26$)

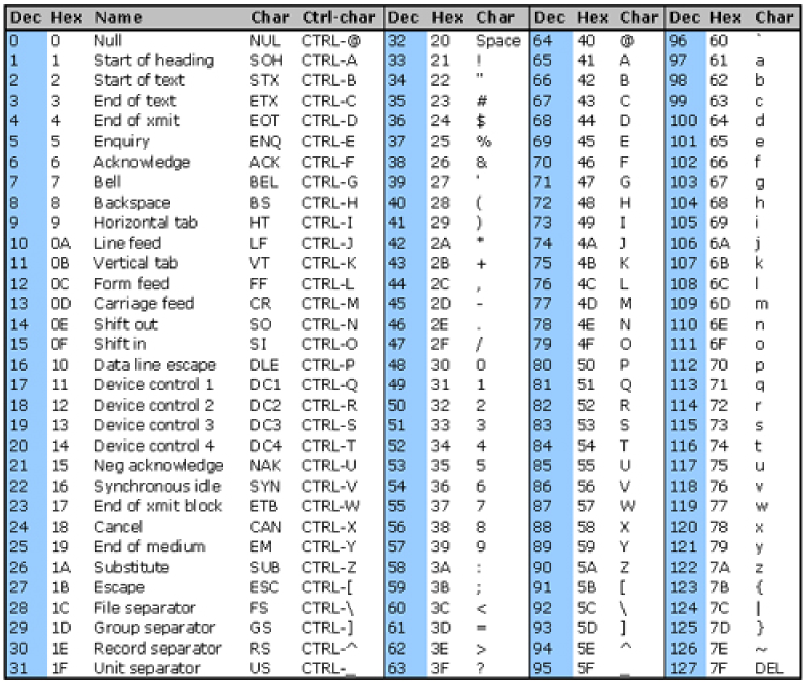
- a *mod* b represents the remainder when a is divided by b. For example, 12 mod 3 =1, 29 mod 26 =3. 23 mod 26 =23 (this is because $23 = 0 \times 26 + 23$), similarly, 57 mod 26 =5 ($57 = 2 \times 26$+5)

- "MEET YOU IN THE PARK" is represented as " 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10"

- It becomes ciphertext when each letter moves 3 slots ($k = 3$) as " 15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13"

Implement your shift cipher

In the real implementation, the alphabet is not limited to include only 26 characters. Instead, it includes all possible characters that are a subset of the ASCII codes. The key k (# moving slots) can be any numbers. There are only 95 *printable* characters that range from 32 (space: ' ') to 126 '~').



Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Fig 1. ASCII codes

- The following results may give you more information about this cipher.

```
Enter your message:
hold long position in tomorrow 's transaction for Euro

Enter your shift cipher key:  123

Encrypted message:
%,)!<),+$<-,0&1&,+<&+<1,*,//,4<C0<1/}+0} 1&,+<#,/<a2/,

Decrypted message:
hold long position in tomorrow 's transaction for Euro
```

Implement the shift cipher such that it can encrypt and decrypt any message for any key you choose.

Your implementation should meet the following requirement.

1. You can code this shift cipher in C++/Java or other languages you feel comfortable.
2. The encrypted message can be represented as a series of digits just like the following example, or a series of characters like the previous example. The digital-one output is easy because you don't need to consider the case for non-printable characters.

```
Enter your message:
hold long position in tomorrow 's transaction for Euro

Enter your shift cipher key:  10743

Encrypted message:
282289286278210286289288281210290289293283294283289288210283288210294289287289292292289297210217293210294292275288293275277294283289288210280289292210247295292289

Decrypted message:
hold long position in tomorrow 's transaction for Euro
```

What should you turn in?

1. A hardcopy of all your homework printout in class (Nov 05, 2013).

2. A folder contains all your homework assignments. If there is a programming assignment, you need to include workable source codes and related output in this folder. Please name your folder as first-name_last-name_CISC4080_homework_3. For example, John_Smith_CISC4080_homework_3 if your name is John Smith.

3. Send the zipped file (.zip instead of .rar) of your folder to xhan9@fordham.edu before 11:59 pm Nov 05, 2013.