Assignment-4 Solution

Q1. Encrypt your 'First Name' and 'Last Name' using the following algorithms:(4-points)

i) Augustus Caesar ii) Julius Caesar

ANSWER:

First Name: DEBASHISH
Last Name: ROY

i) Augustus Caesar

For Augustus Caesar here is the substitution rules for the letters:
A → C, B → D, C → E, D → F, E → G, F → H, G → I, H→ J, I → K, J → L, K → M, L → N, M → O
N → P, O → Q, P → R, Q → S, R → T, S → U, T → V, U → W, V → X, W → Y, X → Z, Y → A, Z → B

D → F	S → U	H → J
E → G	H -> J	R → T
B → D	I → K	O → Q
A → C	S → U	Y → A

ii) Julius Caesar
For Julius Caesar here is the substitution rules for the letters:
A → D, B → E, C → F, D → G, E → H, F → I, G → J, H → K, I → L, J → M, K → N, L → O, M → P
N → Q, O → R, P → S, Q → T, R → U, S→V, T→W, U→X, V→Y, W→Z, X→A, Y→B, Z→C

D → G	S → V	H → K
E → H	H → K	R → U
B → E	I → L	O → R
A → D	S → V	Y → B

Q2. Apply Vigenere algorithm to encrypt the plain text “nice weather”. Use first 3 letters of your First Name as a key for the encryption. Include your calculation (6-points, 3 Points will be deducted if submitted without calculation) [If your first name is less than 3 letters then add one or more 'x’ to make it 3]

Answer 2:

First 3 letters – DEB

N	I	C	E	W	E	A	T	H	E	R
D	E	B	D	E	B	D	E	B	D	E

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

(N+D) mod 26 = (13+3) mod 26 = 16 = Q	(I+E) mod 26 = (8+4) mod 26 = 12 = M	(C+B) mod 26 = (2+1) mod 26 = 3 = D	(E+D) mod 26 = (4+3) mod 26 = 7 = H

(W+E) mod 26 = (22+4) mod 26 = 0 = A	(E+B) mod 26 = (4+1) mod 26 = 5 = F	(A+D) mod 26 = (0+3) mod 26 = 3 = D	(T+E) mod 26 = (19+4) mod 26 = 23 = X
(H+B) mod 26 = (7+1) mod 26 = 8 = I	(E+SD) mod 26 = (4+3) mod 26 = 7 = H	(R+E) mod 26 = (17+4) mod 26 = 21 = V	

Q3. Create a block cipher grid. Here use 'JuliusCaesar' as the key to build the grid as in the Playfair System. In your submission, you need to include the Grid (3 Points) Now use the created block to encrypt the following texts (7-points): i) CAT ii) JOBS iii) VILLA iv) PIZZA v) KITE vi) JJL vii) LOOK

Answer:

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

i) CAT = CA TZ = UD ZC

ii) JOBS = IOBS = IO BS = LP KB

iii) VILLA = VI LL A = VI LX LA = VI LX LA = XU IW UE

iv) PIZZA = PI ZZ A= PI ZX ZA = XR VY VD

v) KITE = KI TE = HS OD

vi) JJL = II L = IX IL = RI SI

vii) LOOK = LO OK = EW QG

Q4.

```
PS C:\> get-filehash C:\Users\Predictor\Desktop\myinfo.txt -algorithm sha1

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            9E8CAD37BB874FA8AE3C5F95581B2CEBAA1C0C2C                               C:\Users\Predictor\Desktop\myinfo.txt


PS C:\> get-filehash C:\Users\Predictor\Desktop\myinfo.txt -algorithm sha256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          B2CA24CF9A26B3CE14D41D1E67F0A925BA071A7E4AB5627419C07229FC05BFA1       C:\Users\Predictor\Desktop\myinfo.txt
```

i) To determine the integrity of data SHA is used. If the sent data is corrupted or altered by an unauthorize entity then SHA algorithms help us to determine the change. SHA1 has output size of 160 bits and SHA256 has an output size of 256 bits

ii) These algorithms help us to preserve integrity for a transmitted data. The HASH values are random and unique. To create a collision situation the attackers, need to generate all the possible random numbers. With the inclusion of SHA512 the generation all the random numbers have become highly unlikely.

iii) SHA1 has 160 bits and one Hexa decimal digit takes 4-bits. So, for SHA1 we have 160/4 = 40 Hex Digits SHA256 has 256, so for SHA256 we have 256/4 = 64 Hex Digits

Q5. If we want to encrypt 20 letters that are stored in UNICODE format, then how many data blocks will be created if the encryption algorithm is AES/DES/3DES? (3 Points)

20 Letters in Unicode will take 20 * 16 = 320 bits

Data block size for AES is 128-bit, for DES it is 64-bit and for 3DES it is 64-bit.

So, for AES the required number of blocks = 320/128 = 2.5 = 3 Blocks

For DES the required number of blocks = 320/64 = 5 Blocks

For 3DES the required number of blocks = 320/64 = 5 Blocks

Q6. If we use "Simple Hash Function Using Bitwise XOR" to calculate a HASH value for $(D593)_{16}$ we will get a HASH value which will be a 4-bit (C1, C2, C3, C4) Hexadecimal digit. Find out the values (C1, C2, C3, C4) (4 Points)

Answer:

$(D593)_{16}$ ->>

$(D)_{16}$ in Binary:	1 1 O 1	
$(5)_{16}$ in Binary:	0 1 0 1	
Bitwise XOR between $(D)_{16}$ and $(9)_{16}$:	1 0 0 0	--- (1)
$(9)_{16}$ in Binary:	1 0 0 1	--- (2)
Bitwise XOR between (1) and (2):	0 0 0 1	--- (3)
$(3)_{16}$ in Binary:	0 0 1 1	--- (4)
Bitwise XOR between (3) and (4):	0 0 1 0	--- (5)

Therefore, C1 = 0, C2 = 0, C3 =1, C4 = 0

Q7. Let's say we have a 5-Byte long one-time pad key:

11100001 11100111 01100111 00100001 10000010

This key is used to get an encrypted bit pattern: 10000100 10001001 00001101 01001110 11111000

XOR operation is used for encryption. Your task is to decrypt the bit pattern and find out the ASCII letters using Table-1. (5 Points)

a	01100001	n	01101110
b	01100010	o	01101111
c	01100011	p	01110000
d	01100100	q	01110001
e	01100101	r	01110010
f	01100110	s	01110011
g	01100111	t	01110100
h	01101000	u	01110101
i	01101001	v	01110110
j	01101010	w	01110111
k	01101011	x	01111000
l	01101100	y	01111001
m	01101101	z	01111010

Table-1: ASCII values for lowercase letters

Key:	11100001	11100111	01100111	00100001	10000010
Cipher:	10000100	10001001	00001101	01001110	11111000
Decryption Using XOR:	01100101	01101110	01101010	01101111	01111010
ASCII Letters:	e	n	j	o	z