CS351
Ass1

Ryan Nathaniel

$1 Affine Cipher

1st most freq = B
2nd most freq = V

A(0)?

Plaintext		Ciphertext
E(4)	→	B(1)
T(19)	→	V(20)

$$4\alpha + b \equiv 1 \pmod{26}$$
$$19\alpha + b \equiv 20 \pmod{26}$$
$$15\alpha \equiv 19 \pmod{26}$$
$$\rightarrow 15\alpha \equiv 45 \pmod{26}$$
$$\alpha \equiv 3 \pmod{26}$$

[19+26 = 45]

Key = (3, 15)

Cipher Key

Sub→
$$4\alpha + b \equiv 1 \pmod{26}$$
$$4(3) + b \equiv 1 \pmod{26}$$
$$12 + b \equiv 1 \pmod{26}$$
$$b \equiv -11 \pmod{26}$$
$$b \equiv 15$$

[26 - 11 = 15]

Test 1

$$4\alpha + b \equiv 1 \pmod{26}$$
$$4(3) + 15 \equiv 1 \pmod{26}$$
$$12 + 15 \equiv 1 \pmod{26}$$
$$27 \equiv 1 \pmod{26}$$
27 % 26 = 1 ✓

Test 2

$$19\alpha + b \equiv 20 \pmod{26}$$
$$19(3) + 15 \equiv 20 \pmod{26}$$
$$57 + 15 \equiv 20 \pmod{26}$$
$$72 \equiv 20 \pmod{26}$$
72 % 26 = 20 ✓

Both Test Passed, Affine Cipher Key is (α = 3, b = 15)

Ron Nathan

$2 $\quad$ $\text{Key} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} = K$

MEET ME AT THE USUAL
12 4 4 19 12 4 0 19 19 7 4 20 18 20 0 11

SPOT AT TEN RATHER THAN
18 15 14 19 0 19 19 4 13 17 0 19 7 4 17 19 7 0 13

EIGHT OCLOCK
4 8 6 7 19 14 2 11 14 2 10

Let $K = 2$, $K = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$

$$MK = \begin{bmatrix} 12(9)+4(5) & 12(4)+4(7) \\ 4(9)+19(5) & 4(4)+19(7) \\ 12(9)+4(5) & 12(4)+4(7) \\ 0(9)+19(5) & 0(4)+19(7) \\ 19(9)+7(5) & 19(4)+7(7) \\ 4(9)+20(5) & 4(4)+20(7) \\ 18(9)+20(5) & 18(4)+20(7) \\ 0(9)+11(5) & 0(4)+11(7) \\ 18(9)+15(5) & 18(4)+15(7) \\ 14(9)+19(5) & 14(4)+19(7) \\ 0(9)+19(5) & 0(4)+19(7) \\ 19(9)+4(5) & 19(4)+4(7) \\ 13(9)+17(5) & 13(4)+17(7) \end{bmatrix}$$

$D_{MK} = n_E \times 2$

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

$(23 \times 2) \times (2 \cdot 2)$ cont...

$K = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ Ron Nathaniel

$2 cont.

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

$mK =$

14	0(9)+19(5)	0(4)+19(7)
15	7(9)+4(5)	7(4)+4(7)
16	17(9)+19(5)	17(4)+19(7)
17	7(9)+0(5)	7(4)+0(7)
18	13(9)+4(5)	13(4)+13(7)
19	8(9)+6(5)	8(4)+6(7)
20	7(9)+19(5)	7(4)+19(7)
21	14(9)+2(5)	14(4)+2(7)
22	11(9)+14(5)	11(4)+14(7)
23	2(9)+10(5)	2(4)+14(7)

= " Y Y B T Y Y R D O H G A C E D Z
24 24 1 19 24 24 17 3 14 7 6 0 24 3 25

D V N H R D J A V P R D F E O
3 21 13 7 17 3 9 0 20 15 17 3 5 4 14

T L C H C Y W C F G S N M Q A "
19 11 27 2 24 22 2 5 6 18 13 12 16 0

row = (12, 4)

Ron Nathan

$3

"YYBT YY RD OHG ACEDZ

OVNH RD JAV PRDFEO

TLCH CYWCF GSNMQA"

A] random == 1Ces

Ron Nathaniel

$ 4

Mathematically, this scheme would work. However, a Man in the Middle, who has access to read from the channel, can very easily utilize these SAME principles to find the original secret key. XORing the Request and Response together calculates the secret key. Since this is just bitwise OR on the same subject twice, it will return to the original subject, but an intruder could use these intermediate numbers to get the key used on the subject. To show:

Key = 0x222

Person A {
random = 0x333
req = Key ^ random
[Person A sends Req down channel]

Person B {
[Person B recieves Req]
res = Key ^ req
[Person B sends Res down channel]

Person A {
[Person A recieves Res]
random == Res

Man in Middle

Key = req ^ res
Key = 0x222

Very simply, the original secret key is calculated.

Ron Nathan

$ 5

$$ A Availability and Integrity

Availability is violated as Carol should Never be able to access Angelo's check in the first place. If she had access, Availabity was not enforced.

Integrity is violated as the figures on Angelo's check are unreliable and incorrect now. If Angelo were to review the check now, the data would be wrong.

$$ B Integrity

Integrity is vidated as Criag posed as Roger, sending word to Rachel in Roger's name. When Rachel reads the letter, she will be reading unreliable and Falsified data.

Ron Nathaniel

$ 5 cont.

$$ C Availability

Availability is violated as, while legal to register any available domain name, it is now Hurting the publishing house to have a fitting name.

$$ D Integrity and Availability

Integrity is violated as, not only was Peter lying and disguising as Jonah, but now Jonah will be unsure of what is correct and incorrect when seeing his balance.

Availability is violated as Jonah, who needs Access and is Authorized to the card, lost Access, and Peter, who does not need Access and is unAuthorized

$$ E Confidentiality and Integrity

Confidentiality as Manny's Pin was not for Henry.

Integrity as the Trojan Horse was malware disguised as a normal document.

Ron Nathaniel

$6

No, a collision resistant function for hashing would not be a good encryption tool. It is a double-edged sword, that makes encryption very difficult. If CRHash(x) != CRHash(y), then we have no way of verifying Equality, in the example of Stored Passwords. If they are equal, Then there is no Decryption method for it. Using this hashing function would not be a good idea.

$7

This is a very similar problem to $4. The man in the middle can intercept and relay as normal, losing his presense. Of course, it is him who gets all the original keys. If they were encrypted with a symmetrical encryption method, the MITM can now decrypt the keys to retrieve the original message.