Comp90043-Assignment 1

Feedback and Solutions:

This Assignment is worth 7.5% of the total marks for the subject.

Each question in Part A carries 2.5 marks, making a total of 7.5 marks$ for the assignment.

The division within each question is as follows:

Q1a, c: 1 mark each, Q1b: 0.5 mark

Q2a: 1 mark and Q2bi,ii,iii 0.5 each.

Q3a: 0.5 mark and Qb,c 1 mark each.

Model Solutions:

Q1. a [1 mark]. The algorithm is discussed in class as well as found in textbook. Most of you have got this question correct.

The points that you need to focus are
1) Input and output variables correctly defined or not.
2) They need to show some example runs from the execution
These were discussed during the forum and class.

b [0.5 mark].

The definition of the function should be correctly defined.
Need check gcd = 1 for the correct output

```
Function :=Inverse (a, n)
G,x,y:=XGCD(a,n) %  g = x a + y
If g =1 then return “x”;
Else return “does not exist”
end function.
```

c. [1 mark] Apply extended Euclid’s result on given data
i..e there exits x, and y such that
a x+ b y = 1 ----------(1)

now c | a => a = a1 c;
d | b => b = b1 d
Applying the above in (1) we get
C (c1 x) + d (b1 y) = 1 ------(2)

Taking modulo d on (2) (c1 x) is inverse of c mod d
Similarly taking mod c => (b1 y) is inverse of d mod c.
Then using the logic mentioned in my Wednesday lecture, (c,d) = 1.

To get full mark, you need to have all the arguments.

Q2. [1 mark (0.5+0.5)]

(a) The definition of risks and attacks were discussed in first chapter. Refer to RFC2828 and the text for details. A standard answer would require an example each to illustrate risk and attack.

An example involving Microsoft security patches: These patches are released because of risks in the operating system. If someone is lucky, an attack may not occur even if the patches were not applied to the system. So the attack refers to actual misusing of the vulnerability. Definitely installing patches reduces or eliminates the risks.

(b) [0.5 each]
(i) p = (a^(-1)c –b)mod 29.
ii) 28*29-1
(iii) Cipher Text Only attack: Complexity is either polynomial in cipher text size or O(29^2).
We would look for explanations for reduction in the complexity for CPA attack when compared to Cipher Text Only attack. Please read carefully the relevant discussion on this from lectures.

Q3.
a[0.5 mark]

The number of valid keys is same as the number of invertible matrices over of size m over Z_26.

Z_26 is made up of Z_13 x Z_2.

Using CRT, AN invertible matrix over Z26 can be represented by the direct of invertible matrices over Z13 and Z2.
Conversely given a invertible matrix over Z13 and Z2, you can get an invertible over Z26. So counting # of invertible of matrices over Z26 simplifies to Z13 and Z2 respectively.
To get full mark, as discussed in the class you need have correct answer for m=1,2,3.

when m =1, # of keys = (12)
m =2, # keys (13^2-1)*(13^2 -13)* (2^2-1)*(2^2-2).
M =3 # keys (13^3-1)*(13^3-13)* (13^3 -13^2) (2^3-1)*(2^3-2)*(2^3-2^2).
= 634038189056

The general expression is also possible.

b.[1 mark]

An explanation of finding key using simultaneous equations need to be given by using known plain text and cipher text relations.

C [1 mark]

K:=
8 16 19]

23 16 9]
24 7 23]

Inverse
25 11 18]
11 2 15]
 9 6 14]

Workings should be shown in the answers to get full marks.

Text1:="PHILOSOPHERSASKCANHUMANINGENUITYCONCOCTACIPHERWHICHHUMANINGENUITY CANNOTRESOLVE

Most of you got this correct,

Part B: Questions for Self Study (No need to submit answers for this part)

Q1.
Similarities:
1. A strong encryption algorithm or function.
2. Two keys are used in both modes.

Differences:
1. Symmetric cryptography operations are usually faster.
2. Asymmetric uses different keys for encryption and decryption.
3. Symmetric key must be secret to all but sender/receiver, for asymmetric typically one can be made public.
4. Symmetric encryption and decryption are usually faster than asymmetric.

A model solution is given below. Please refer to the textbook for a detailed explanation.

CFB
 Encryption fn:
$I_1 = IV$
$I_j = LSB_{b-s}(I_j\text{-}1)||C_j\text{-}1 \quad j=2,\ldots,N$
$O_j = E(K,I_j) \quad j=1,\ldots,N$
$C_j - P_j + MSB_s(O_j) \quad j=1,\ldots,N$

Decryption fn:
$I_1 = IV$
$I_j = LSB_{b-s}(I_j\text{-}1)||C_j\text{-}1 \quad j=2,\ldots,N$
$O_j = E(K,I_j) \quad j=1,\ldots,N$
$P_j - C_j + MSBs(O_j) \quad j=1,\ldots,N$

OFB:
Encryption fn:
$I_1 = Nonce$
$I_j = O_j\text{-}1 \quad j=2,\ldots,N$

$O_j = E(K, I_j)$ j=1,…,N
$C_j = P_j + O_j$ j=1,…,N-1
$C_N = P_N + MSB_u(O_N)$

Decryption fn:
I_1 = Nonce
$I_j = LSB_{b-s}(I_j\text{-}1)||C_j\text{-}1$ j=2,…,N
$O_j = E(K, I_j)$ j=1,…,N
$P_j = C_j + O_j$ j=1,…,N-1
$P_N = C_N + MSB_u(O_N)$

b: size of a block
u: remaining size of block such that u < b
T: counter

One counter mode is also discussed in the textbook:
CTR
Encryption fn:
$C_j = P_j + E(K, T_j)$ j=1,…,N-1
$C_N = P_N = MSB_u[E(K, T_N)]$
Decryption fn:
$P_j = C_j + E(K, T_j)$ j=1,…,N-1
$P_N = C_N = MSB_u[E(K, T_N)]$

Q4. (b)

The answer is straightforward, please refer to the textbook.

Q4. (c)

*
The question assumes that there was an error in block C4 of the transmitted ciphertext.
ECB mode: In this mode, ciphertext block Ci is used only as input for the direct dencryption of plaintext block Pi. Therefore, a transmission error in block C4 will only corrupt block P4 of the decrypted plaintext.
CBC mode: In this mode, ciphertext block Ci is used as input to the XOR function when obtaining plaintext blocks Pi and Pi+1. Therefore, a transmission error in block C4 will corrupt blocks P4 and P5 of the decrypted plaintext, but will not propagate to any of the other blocks.
CTR mode: In this mode, ciphertext block Ci, as well as the encrypted counter ti, are used only as input for the direct decryption of plaintext block Pi. Therefore, a transmission error in block C4 will only corrupt block P4 of the decrypted plaintext.

*

3. Questions related to Classical Ciphers):

1. For key of length n, each can be one of 26 possible characters, there are 26n possible keys in total.
2. “yahkqpt".
3. “yahkqpt" – “unimelb" = “enzymes";

“enzymes" + “rmituni" = “vzhrgra"