**Offline Quiz for Advance Security 1**

**Instruction:** Duration 2hrs

**Total Marks:** 50 Marks

**Submission:** All submissions should be uploaded before 11:00 AM.

Answer ALL questions.

Robert Ichim

C17440254

Page 1 of 2

1. In relation to Feistel Cipher, write a summary of what you have learned in this area no more than one page.

(12 Marks)

The Fiestel Cipher is utilising the product cypher by executing in sequence both Substitution and Permutation. By doing this, the result will be significantly stronger cryptographically than other cyphers.

Substitution is when a plaintext element is replaced by a corresponding ciphertext.

Permutation is when the elements of the plaintext are rearranged from their original order instead of deleting or replacing elements.

The purpose of this cipher is to have it so that the total transformations are 2 to the power of k.

The way the cipher works is the inputs to the algorithms are plaintext. This plaintext is split into halves and each half is processed individually over n amount of rounds. After that is done, the two halves which have been processed are put back together.

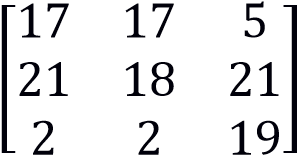
For this cipher to be secure, 16 rounds are reasonable, 1 being inadequate. Also, for the block size, a bigger block size means there is greater security but this comes at the cost of reduced speed in encryption and decryption. This means the more diffusion the better the encryption. 64 bits is the best balance when it comes to block size. The key size however, should be 128 bits. The greater the key the better security. More time spent on decrypting means harder to brute force which is good.

One thing to remember when designing a cipher with this approach in mind is that the more complex the cipher is, the harder it is to analyse and this means that finding vulnerabilities is significantly harder. This is usually something to consider when using it and implementing it.

The Data Encryption Standard (DES) for example, is very complex and therefore is hard to analyse.

1. Using the Hill Cipher, perform the encryption and decryption without using online tools and mention each step details.

PlainText = cashisneeded

K = 

Cashisneeded = (c a s)(h i s)(n e e)(d e d)

(2 0 18)(7 8 18)(14 4 4)(3 4 3)

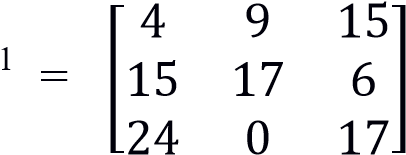
17(2) + 17(0) + 5(18) =

21(2)+ 18(0)+ 21(18) 🡺 (124 420 346) = (20 4 8) = (U E I)

2(2)+ 2(0) + 19(18) =

Same steps for the rest (don’t have time to type everything)

Encrypted, it is “**UEIHTIXNGEQT**”

K-

(14 Marks)

Encryption is (20 4 8)(9 17 0)(23 13 6)(4 16 19)

You Multiply that the same way we did above but you use the k -1 matrix instead of the k.

This will give you (c a s)(h i s)(n e e)(d e d)

1. Determine the GCD using the Euclidean algorithm without using online tools and mention each step details.

i) a = 72345, b= 43215 ii) a= 10292, b= 3486

(12 Marks)

1. a = 72345, b= 43215

72345 / 43215 = 1 **remainder 29130 ->** (72345 = 1 × 43215 + 29130)

43215 / 29130 = 1 **remainder 14085** ->*(*43215 = 1 × 29130 + 14085*)*

29130 / 14085 = 2 **remainder 960**  ->*(*29130 = 2 × 14085 + 960*)*

14085 / 960 = 14 **remainder 645** *->  (*14085 = 14 × 960 + 645*)*

960 / 645 = 1 **remainder 315**  ->(960 = 1 × 645 + 315*)*

645 / 315 = 2 **remainder 15**->  (645 = 2 × 315 + 15) (**This is GCD**)

315 / 15 = 21 **remainder 0** *->*(315 = 21 × 15 + 0)

So the **GCD is 15**

1. a= 10292, b= 3486

10292 / 3486 = 2 **remainder 3320** ->   (10292 = 2 × 3486 + 3320)

3486 / 3320 = 1 **remainder 166** ->   (3486 = 1 × 3320 + 166)(**This is GCD**)

3320 / 166 = 20 **remainder 0** ->   (3320 = 20 × 166 + 0)

The **GCD is 166**

1. Consider an online banking system in which users provide an account number and password to access the bank account and transfer money online. Mention example of CIA (confidentiality, integrity, and availability) requirements associated with the system. Also discuss the level of importance (low, medium high) of each requirement on the system.

.

(12 Marks)

Confidentiality is when you are restricting and preventing unauthorized access to personal privacy and proprietary information. Confidentiality is lost when this information becomes available without the proper authorisation. In this case, the bank account should only be accessed by the person who’s bank account it is and other people, should they have legal permission to do so.

This requirement is of high level of importance because it could lead to damages of the persons assets and also major financial loss.

Integrity is when the information is not modified or deleted by someone that is not authorized to do so.

In this case, if someone other than the user change the user’s password. Or they wire money from the account without the users consent.

Integrity is of high importance also. Should the user’s information be deleted or changed, it could lead to money loss and asset loss.

Finally, availability is when the access to the information is reliable and timely. This means that if the bank user is not able to access the bank system because of technical problems, the system lost its availability because the access to his information has been disrupted.

This is of Moderate risk because while the user is not able to access the account, there could be significant financial losses.

Page 2 of 2