**Question 1**

**(a)**

CIA is of utmost importance in any setting but even more so in an online banking setting.

Confidentiality: This step is very crucial to any member joining a online banking because it means that users information wouldn’t be given to anyone that isn’t authorized to use it or have possession of it. It also means that the there isnt any misuse of the personal data that is being collected by the bank from the user in question. This step would be very high in the importance scale

Integrity: This step helps protect the authorized persons data from any user who is unauthorized to see it or use it, it can also be used to protect the authorized user into not doing anything that they should not press or do for example accidental deletion of data or data lose that would happen randomly from the authorized user. This step is medium in the importance scale

Availability: This step means that the services and offers that the online bank is asking for are constantly available for the user to use and access at any time they require, this also means that the user would be uninterrupted use if they are authorized and only if they are authorized may they see everything that the online banking offers, this step is also a high importance in the scale.

**(b)**

Passive attacks are employed to be non-disruptive and go unnoticed by the attacker as to not draw attention. The purpose behind them is ussuay to gain access to data on the system without being detected. These are very popular attacks and are used to steal private data such as credit card info, usernames and passwords, and other personal data that can be used to impersonate the users.

They are typically employ some malware or hack which will listen to the systems communication or records system communications like a keyboard input for passwaords.

The defining thing about passive attacks is that they do not aim to harm the system in any way for example to lock the user out or encrypt user data, it is purely of data collection nature.

**(c) (i)**

In the rail fence cipher, the plaintext is written downwards diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached, down again when the top rail is reached, and so on until the whole plaintext is written out. The ciphertext is then read off in rows.

A close-up of a calculator

Description automatically generated with low confidence

**(ii)**

This coding method asks the user to have a plaintext that is paired with a randomly generated secret key, this also encrypts each plaintext with a corresponding bit from the random key. This cannot be cracked and can only be solved using the otp.

**(iii)**

A row transition cipher makes the user use a key that is a set of numbers and a plaintext word , after this it asks the user to encrypt the word using the key, this can be done by following the first digit of the key and aligning it with the letter that is corresponding with it and continuing to the 2nd and 3rd digit etc.

**Question 2**

**(a)**

**Key:** 9 0 1 7 23 15 21 14 11 11 2 8 9

**Plaintext:** sendmoremoney

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 9 | 0 | 1 | 7 | 23 | 15 | 21 | 14 | 11 | 11 | 2 | 8 | 9 |
| Plaintxt | S | E | N | D | M | O | R | E | M | O | N | E | Y |
|  | 18 | 4 | 13 | 3 | 12 | 14 | 17 | 4 | 12 | 14 | 13 | 4 | 24 |
|  | 27 | 4 | 14 | 10 | 35 | 29 | 38 | 18 | 23 | 25 | 15 | 12 | 33 |
| Cipherext | B | E | O | K | J | D | M | S | X | Z | P | M | H |

**(b)**

The feistel cipher alternates between substitution and permutation, therefore it is a product that alternates between confusion and diffusion functions. Therefore it isn’t really a specific cipher and is instead a design model for block ciphers.

Its features are it’s Block Size, key size, number or founds, subkey generation algorithm, round function F, fast software encryption & decryption, and ease of analysis

Each round does some function F using K( which is a subkey of the key) and R, then set L equal to F(K,R)XOR L, then finally swap L and R.

Diagram

Description automatically generated

**(C)**

**(i)**

Diffusion and confusion were both introduced by Claude Shannon to capture the basic building blocks for any cryptographic system

First diffusion is the statistical structure of the plaintext so that it is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits.

Second Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, therefore even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key.

**(ii)**

Symmetric encryption ciphers consist of two main categories: block ciphers and stream ciphers.

A block cipher is one that allows you to use a key to encrypt data in big groups(blocks) of a set size such a 128 bits or 256 bits. DES, AES, and 3DES all use Block ciphers.

A stream cipher is a cipher that encrypts and decrypts with the flow of data. Therefore unlike block ciphers which require forming blocks prior to the encryption, stream ciphers encrypt data in long, pseudorandom streams. RC4 and A5 use stream ciphers.

Diagram

Description automatically generated

**(iii)**

Strict avalanche criterion and Bit independence criterion appear to strengthen the effectiveness of the confusion function in a Feistel Cipher in the function f, therefore the more nonlinear it is the more difficult any type of crypt analysis will be.

SAC states that nay output bit j of an S-box should change with a probability of ½ when any single input bit i is inverted for all i , j.

BIC : 2 bits should change independently when any single input bit is inverted

**Question 3**

**(a)**

Cbc uses a block cipher then chains them, therefore the input to the encryption algorithmis the xor od the next block of plaintext and the preceding block of cipher text

A block cipher is one that allows you to use a key to encrypt data in big groups(blocks) of a set size such a 128 bits or 256 bits. DES, AES, and 3DES all use Block ciphers.

The bit independence criterion states that any two output bits should change independently when any input bit is changed.

A piece of paper with writing on it

Description automatically generated with medium confidence

**(b)**

Public and private keys form the basis for public key cryptographywhich also known as asymmetric cryptography. In public key cryptography, every public key matches to only one private key. Together they are used to encrypt and decrypt messages, so If you encode a message using a person’s public key then they can only decode it using their matching private key.

Each public key comes paired with a unique private key. This defines one of the main differences between the two types of keys. The private key ensures only you can get through the front door. In the case of encrypted messages, you use this private key to decrypt messages

Together, these keys help to ensure the security of the exchanged data. A message encrypted with the public key cannot be decrypted without using the corresponding private key.

**(C)**

**(i)**

|  |  |  |  |
| --- | --- | --- | --- |
| 65 | 0F | C0 | 4D |
| 74 | C7 | E8 | D0 |
| 70 | FF | E8 | 2A |
| 75 | 39 | CA | 9C |

**(ii)**

|  |  |  |  |
| --- | --- | --- | --- |
| 65 | 0F | C0 | 4D |
| 74 | C7 | E8 | D0 |
| 70 | FF | E8 | 2A |
| 75 | 3F | CA | 9C |

|  |  |  |  |
| --- | --- | --- | --- |
| 65 | 0F | C0 | 4D |
| C7 | E8 | D0 | 74 |
| E8 | 2A | 70 | FF |
| 9C | 75 | 3F | CA |