Information Assurance and Security (IT352) Lab Program-2(a)
Write appropriate diagrams, equations and partial source code
Copy is not allowed. All copied submission considered as Malpractice

Use any of the following programming languages: Python, Java, C++, or C to implement Electronic Code Book (ECB) mode of data transmission by considering runtime input values. Frist read the plaintext (alphanumeric) to be encrypted from the terminal, and key value (alphanumeric) from the terminal. Divide the plaintext such that plaintext size equals to key size in terms of number of character present in the key (not bits). Consider space also as one character during creation of plaintext block. Display created plaintext block onto terminal. Use the corresponding ASCII value of the character to perform encryption and decryption operations/ Encrypt each plaintext block with same key value repeatedly until completion of all blocks. Below mentioned steps to shows the Encryption and Decryption operations of one plaintext block and one ciphertext block.

- $\text{Ciphertext} \leftarrow (\text{Plaintext}_i + \text{Key}_i) \bmod 255$
- $\text{Plaintext} \leftarrow (\text{Ciphertext}_i - \text{Key}_i) \bmod 255$

Print all results on the terminal, including intermediate steps of computation. Store the same onto a file with the filename Rollnumber_IT352P2a.txt.

Information Assurance and Security (IT352) Lab Program-2(b)
Write appropriate diagrams, equations and partial source code
Copy is not allowed. All copied submission considered as Malpractice

Use any of the following programming languages: Python, Java, C++, or C to implement Cipher Block Chaining (CBC) mode of data transmission by considering runtime input values. Frist read the plaintext (alphanumeric) to be encrypted from the terminal, key value (alphanumeric) and Initialization Vector (IV) value from the terminal. Divide the plaintext such that plaintext size equals to IV size in terms of number of character present in the IV (not bits). Consider space also as one character during creation of plaintext block. Display created plaintext block onto terminal. Encrypt each plaintext block with same key value repeatedly until completion of all blocks. Below mentioned steps shows the Encryption and Decryption operations of one plaintext block and one ciphertext block. Use the corresponding ASCII value of the character to perform encryption and decryption operation.

Encryption :

$\text{Intermediate Result} \leftarrow \text{Plaintext}_i \text{ Ex-OR } \text{IV}_i$

$\text{Ciphertext} \leftarrow (\text{Intermediate Result}_i + \text{Key}_i) \bmod 255$

Decryption :

$\text{Intermediate Result} \leftarrow (\text{Ciphertext} - \text{Key}_i) \bmod 255$

$\text{Plaintext} \leftarrow (\text{Intermediate Result}_i \text{ Ex-OR } \text{IV}_i) \bmod 255$

Print all results on the terminal, including intermediate steps of computation. Store the same onto a file with the filename Rollnumber_IT352P2b.txt.

Information Assurance and Security (IT352) Lab Program-2(c)
Write appropriate diagrams, equations and partial source code
Copy is not allowed. All copied submission considered as Malpractice

Use any of the following programming languages: Python, Java, C++, or C to implement Counter Mode of data transmission by considering runtime input values. Frist read the plaintext (alphanumeric) to be encrypted from the terminal, key value (alphanumeric) and Initialization Vector value from the terminal. Below mentioned steps shows the encryption operations as part of the counter mode operation. Use the corresponding ASCII value of the character for implementation of Counter Mode by encrypting one plaintext character at time.

Encryption :

Output of Encryption ← $(\text{CounterValue}_i + \text{Key}_i)$ Mod 255

Ciphertext ← Plaintext_i Ex-OR Output of Encryption

Print all results on the terminal, including intermediate steps of computation. Store the same onto a file with the filename Rollnumber_IT352P2c.txt.

.

Information Assurance and Security (IT352) Lab Program-2(d)
Write appropriate diagrams, equations and partial source code
Copy is not allowed. All copied submission considered as Malpractice

Use any of the following programming languages: Python, Java, C++, or C to implement Feedback Mode of data transmission by considering runtime input values. Frist read the plaintext (alphanumeric) to be encrypted from the terminal, key value (alphanumeric) and Initialization Vector value from the terminal. Below mentioned steps shows the encryption operations as part of the Feedback Mode operation. Use the corresponding ASCII value of the character for implementation of Feedback Mode by encrypting two plaintext character at time.

Encryption:

Output of Encryption ← $(\text{CounterValue}_i + \text{Key}_i)$ Mod 255

Ciphertext ← Plaintext_i Ex-OR Output of Encryption

Print all results on the terminal, including intermediate steps of computation. Store the same onto a file with the filename Rollnumber_IT352P2d.txt.
