ENCRYPTION AND DECRYPTION

AIM:
To conduct an experiment to demonstrate the working of Data Encryption – Decryption.

APPARATUS REQUIRED:
PC with network simulator software.

THEORY:
❖ Consumers entering highly confidential information
❖ Four requirements of a secure transaction
❖ Privacy – information not read by third party
❖ Integrity – information not compromised or altered
❖ Authentication – sender and receiver prove identities
❖ Non-repudiation – legally prove message was sent and received.

Encryption/Decryption Methods
❖ Plaintext – unencrypted data
❖ Cipher-text – encrypted data

plaintext:  abcdefghijklmnopqrstuvwxyz

ciphertext: mnbcvxzasdfghjklpoiuytrewq
EXPERIMENTAL SETUP:

Concept of Encryption and Decryption:
Procedure:

1. In terminal window enter
   - cd networks
   - cd layer
   - cd phy_Lyr
   - ./main
2. In main window (TCP/IP layer) select application layer.
3. Enter the destination and source IP address in the transmitter and receiver system.
4. Enter the plain text message.
5. The secret key used to the plaintext is converted into ciphertext.
6. The same key is used in the receiver side, the ciphertext message is converted into plaintext.

RESULT:

Thus the working of the data encryption and decryption was understood and output was verified.
IMPLEMENTATION OF STOP AND WAIT AND SLIDING WINDOW PROTOCOL

AIM:
To conduct an experiment to demonstrate the working of stop and wait and sliding window protocol.

APPARATUS REQUIRED:
PC with Network simulated software RS232 cable.

THEORY:

Stop and Wait Protocol:
- Idea of stop-and-wait protocol is straightforward
- After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
- If the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame.

Sliding Window Protocol:
- Sender assigns a sequence number denoted as Seq Num to each frame.
  - Assume it can grow infinitely large
  - Sender maintains three variables
  - Sending Window Size (SWS)
  - Upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit
  - Last Acknowledgement Received (LAR)
  - Sequence number of the last acknowledgement received
EXPERIMENTAL SETUP:

Stop and wait - Flow Control

Sliding Window - Flow Control
Stop and Wait Protocol-Output: Node 1

Stop and Wait Protocol-Output: Node 2
Sliding Window Protocol-Output Node:1

Sliding Window Protocol-Output Node:2
PROCEDURE:

1. In main window, enter
   - Cd network
   - Cd layer
   - Cd Phy_Lyr
   - ./main

2. In TCP/IP layer, select data link layer stop and wait and sliding window.

3. Enable the client connection with server, go to data link layer, first click reset and lets begin to enable the working window in both system.

4. Choose the number of frame, enter the same start end and pad character in both the system

5. **STOP AND WAIT:**
   
   From the transmission mode, send the ‘1’ data frame to receiver node. In receiver node, if data is delivered, the receiver node send the acknowledgement to the transmitter node.

6. **SLIDING WINDOW:**
   
   From the transmission mode, send multiple data frame to receiver node. In receiver node, if data is delivered, the receiver node send the acknowledgement to the transmitter node.

RESULT:

Thus the working of the stop and wait and sliding window protocol was understood and output was verified.
IMPLEMENTATION OF GOBACK-N AND SELECTIVE REPEAT PROTOCOLS

AIM:
To conduct an experiment to demonstrate the working of Go back-N and Selective repeat protocols.

APPARATUS REQUIRED:
PC with Network simulated software RS232 cable.

THEORY:
- In the Go-Back-N Protocol, the sequence numbers are modulo $2^m$, where $m$ is the size of the sequence number field in bits.
- The send window is an abstract concept defining an imaginary box of size $2^m - 1$ with three variables: $S_f$, $S_n$, and $S_{size}$.
- The send window can slide one or more slots when a valid acknowledgment arrives.
- The receive window is an abstract concept defining an imaginary box of size 1 with one single variable $R_n$. The window slides when a correct frame has arrived; sliding occurs one slot at a time.
- In Go-Back-N ARQ, the size of the send window must be less than $2^m$; the size of the receiver window is always 1.
- In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of $2m$. 
**Go–Back-N Damaged Frame**

Sender

- Data 0
- Data 1
- Data 2
- Data 3
- Data 4
- Data 5

Receiver

- Data 0
- Data 1
- Data 2
- ACK 3
- NAK 3
- Discarded
- Discarded

Error in frame 3

---

**Selective Reject**

Sender

- Data 0
- Data 1
- Data 2
- Data 3
- Data 4
- Data 5

Receiver

- Data 0
- Data 1
- Data 2
- NAK 2
- Data 3
- Data 4
- Data 5

Resent
Selective Retransmission-Output: Node 1

Selective Retransmission-Output: Node 2
Go Back N-Output: Node 1

Go Back N-Output: Node 2
PROCEDURE:

1. In main window, enter
   - Cd networks
   - Cd layers
   - Cd Phy_Lyr
   - ./main

2. In TCP/IP layer, select data link layer sliding window.

3. Enable the client connection with server, go to data link layer, first click reset and let's begin to enable the working window in both system.

4. Choose number of frames to transmit.

5. Choose start, end and pad characters, by default other the data.

6. Enter a maximum of 8 bytes of data on the first system, click on the SEND button.

7. If user wants to include error click on ERROR button, include the error in the frame then click on the SEND button.

8. The receiving section (second node) receives 7 frames.

9. Then receiver enters sequence number and click on the REJ button, the sending end will receive the warning as shown in Screen.

10. Go-Back-N Protocol: The frames will be retransmitted from specified sequence number to all frames as shown in Screen.

11. Selective Repeat: The frames will be retransmitted the particular frame as shown in Screen.

RESULT:

Thus the working of the Go back-N and Selective repeat protocols was understood and output was verified.