**Cryptography**

**Industry Assignment 4**

1. **Consider a network (connected), with N number of nodes and each node has unique address. Let E denotes the set of links between the nodes. Design a privacy preserving routing protocol, wherein information needs to be sent from node A to node B in a secure way. (Hint: Onion routing protocol, Tor network)**

In modern network communication, preserving user privacy and protecting message metadata is just as important as encrypting thelmessage itself. Traditional routing protocols reveal critical information such as sender identity, route path, and destination. This assignment implements a simplifiedlversion of an onion routing protocol, similar to the approach usedlby thelTor network, which ensures that data sent from one node to another travels through multiple layers of encryption. Each intermediate node decrypts only its specific layer, without learning thelfull path or theloriginal message content.

**Implementation Overview**

1. **SimulatedlNetwork**: A network of three nodes was simulated: Relay 1, Relay 2, and Node B. Node A (thelsender) encrypts thelmessage in three layers—one for each hop.
2. **LayeredlEncryption (Onion Routing)**: Thelmessage is first encryptedlfor Node B (thelfinal destination), then wrappedlin a second encryption layer for Relay 2, and finally wrappedlin a third layer for Relay 1. This ensures that:

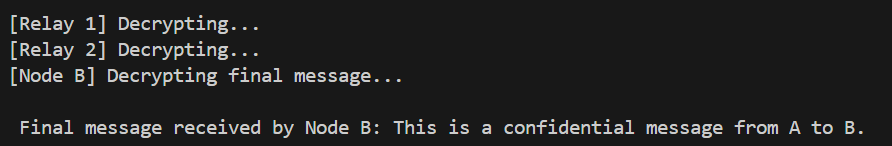
* Relay 1 knows only thelnext hop (Relay 2), not thelmessage or destination.
* Relay 2 knows thelnext hop is Node B but not thelsource or message.
* Only Node B can fully decrypt thelactual message.

1. **Symmetric Encryption (AES-CBC)**: AES in CBC mode was usedlfor each layer, with separate symmetric keys generatedlfor Relay 1, Relay 2, and Node B. Each key is known only to thelrespective node.
2. **Decryption Flow**: As thelencryptedlpacket travels through thelnetwork:

* Relay 1 decrypts theloutermost layer and forwards it.
* Relay 2 decrypts thelmiddle layer and forwards it.
* Node B decrypts thelinnermost layer and retrieves theloriginal message.

**Output Summary**

Thelsimulation was successfully executed, displaying thelfollowing:



This confirms that thelmessage successfully passedlthrough multiple layers of encryption and was securely deliveredlto Node B, with each intermediary node unaware of thelfull path or content.

This assignment demonstrates a fundamental principle of privacy-preserving communication using onion routing. By implementing layeredlencryption, each network node can only access a portion of thelrouting information, thereby reducing thelrisk of surveillance or data interception. Thelsimulation validates how effective this approach is for protecting user anonymity and message confidentiality in distributedlnetworks.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of thelDocument \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*