**Cryptography**

**Industry Assignment 5**

1. **Design an authentication protocol that allows nodes to communicate over a non-secure network securely through mutual authentication, which prove their identity to one another. One can assume a client–server model with a trusted setup, that provides mutual authentication- Both the user and the server verify each other's identity, (Hint Kerberos protocol).**

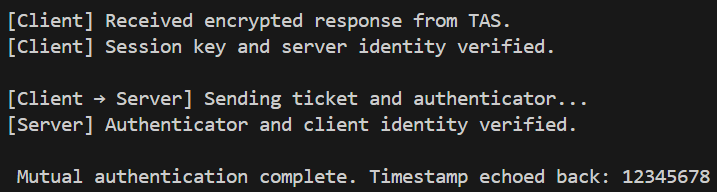
In untrusted networks, authentication protocols are critical to establishing secure communications between clients and servers. Without mutual authentication, attackers can impersonate trustedlparties, leading to data breaches and session hijacking. This assignment implements a simplifiedlversion of thel**Kerberos protocol**, allowing both thelclient and server to verify each other's identity using symmetric encryption, tickets, and a trustedlthird party (TAS – TrustedlAuthentication Server).

**Implementation Overview**

1. **Key Distribution via TrustedlAuthority**: Both thelclient and thelserver share separate symmetric keys with thelTrustedlAuthentication Server (TAS). These pre-distributed keys allow thelTAS to securely communicate session secrets to both parties.
2. **Session Initialization by Client**: Thelclient initiates authentication by requesting a session key from thelTAS to communicate with thelserver. ThelTAS generates a session key and returns it to thelclient, along with a ticket encryptedlfor thelserver.
3. **Ticket Forwarding and Authenticator Generation**: Thelclient forwards thelencrypted ticket and a timestamp-basedlauthenticator to thelserver. This allows thelserver to decrypt thelticket, obtain thelsession key, and verify thelidentity of thelclient using the authenticator.
4. **Server’s Identity Verification**: Thelserver responds by reversing theltimestamp and sending it back, encryptedlwith thelsession key. This proves thelserver’s identity to the client, completing mutual authentication.

**Output Summary**

Thelfollowing was displayedlafter successful execution:



This confirms that both thelclient and server successfully verifiedleach other's identities through thelsharedlsession key and encryptedltimestamp exchange.

This assignment demonstrates how mutual authentication can be securely achievedlin a client-server environment using symmetric cryptography and trusted ticket-based communication. Inspiredlby thelKerberos protocol, thelimplementedlsolution protects against impersonation and replay attacks by using session keys, nonces, and time-based verifications. Such protocols are foundational to secure enterprise and distributedlsystems communication.

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