

**SEMESTER ONE 2024/2025 ACADEMIC YEAR**

**SCHOOL COMPUTING AND IMFORMATICS TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE**

**MASTER OF SCIENCE IN COMPUTER SCIENCE**

**MCS 7102**

**DATA SECURITY AND PRIVACY**

**ASSIGNMENT ONE**

**AMPEIRE EDGAR**

**2024/HD05/21915U**

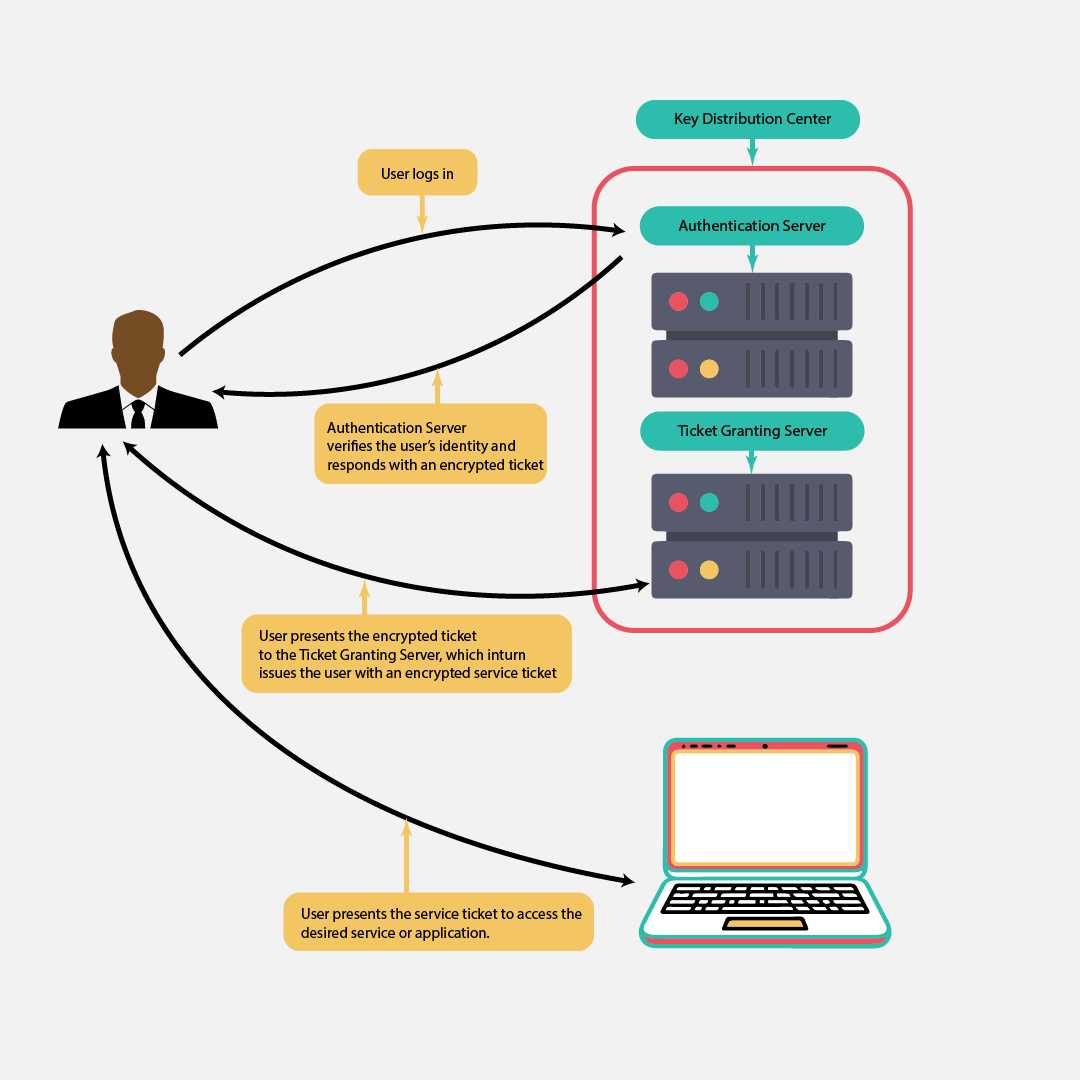
**2400721915**

**KERBEROS COMPUTER NETWORK PROTOCOL**

Kerberos is a network authentication protocol that provides secure communication over not secure networks. It uses the principle of tickets to allow secure communications between users and services.

**How does Kerberos Work?**

Kerberos uses symmetric key cryptography, which is a type of encryption where the same key is used for both encryption and decryption. In order to authenticate the provide users to services, Kerberos uses a Key Distribution Center (KDC) which consists of 2 components; Authentication Server, Ticket Granting Server

 The user enters the username and password to login, the authentication server verifies the user’s identity and then issues an encrypted ticket which contains a user’s secret key and also a session key to the user.

The user presents the received ticket to the Ticket Granting Server, which verifies and then issues an encrypted service ticket.

This is the service ticket that the user then presents to the application or server they want to access. Then that service or application verifies and grants the user secure access.

For a secure connection to be established, the user and the service have to verify each other, a principle known as mutual authentication which helps in preventing man in the middle and replay attacks.

**Drawbacks of Kerberos**

1. **Single point of failure.** If the key distribution server is not available or access the applications and servers.
2. **Scalability.** Key management in large networks which many users and applications and services is difficult and resource intensive, which limits scalability.
3. **Denial of service attacks.** The authentication server can be flooded with authentication requests which can cause poor response to legitimate requests or even crash whole Key Distribution Center.

**Conclusion.**

Kerberos is still widely utilized in various environments for securing communication in networks, if extensive counter measures are implemented on its drawbacks, it can still be a reliable protocol in providing secure communication in networks.