Consider the Kerberized login discussed in the book.

a. What is the TGT and what is its purpose?

Step 1:

Across an untrusted network, such as the internet, Kerberos, a computer network security protocol, authenticates service requests between two or more trusted hosts. It authenticates client-server applications and confirms users' identities using secret-key cryptography and a reliable third party.

Step 2:

A Ticket Granting Ticket (TGT) or Ticket to Get Tickets (TGT) is a file produced by the Kerberos authentication protocol's key distribution centre (KDC). They are employed to give users access to the resources on the network. As soon as the user and server authenticate them, TGT files can offer secure data protection.

b. Why is the TGT sent to Alice instead of being stored on the KDC?

Step 1:

The Key Distribution center, a trusted third-party server, is where Kerberos functions (KDC). A primary is any user or service on the network.

Step 2:

By creating a special ticket-type key for creating a secure connection through which data is shared and transferred, a key distribution centre is a sort of symmetric encryption that permits access of two or more systems in a network.

The KDC can maintain its statelessness as a result. In actuality, the KDC provides the clients with access to the TGT database.

c. Why is the TGT encrypted with KA when it is sent from the KDC to Alice’s computer?

Step 1:

The ticket-granting server and the authentication server are the only ones with access to the key used to encrypt the TGT. A request for access to the Cisco access server is presented to the TGT by the TGS.

Step 2:

Since the TGT is already encrypted and is easily sent in subsequent exchanges (without any additional encryption), it appears that this serves no benefit.