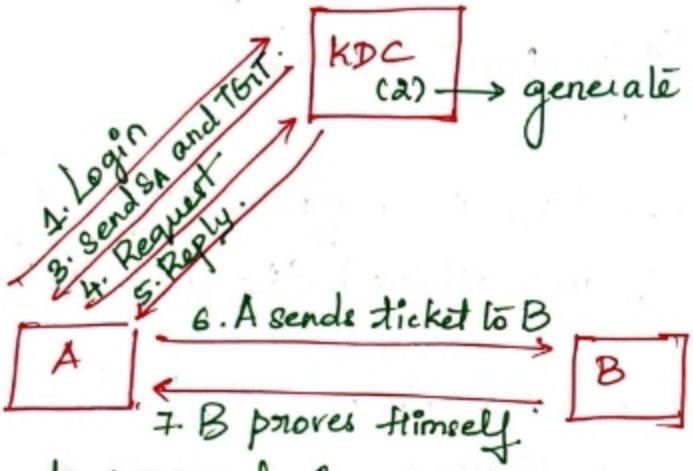
Semester : VI Subject : CSS Academic Year: 2023- 2024

## KERBEROS:

It performs the following tasks:

* Kerberos login.
* Kerberos Ticket




~~Step1: Kerberos login.~~

KDC → Key Distribution Center.
$S_A$ → Session key of A.
TGT → Ticket Granting Ticket
$K_A$ → Symmetric key of A.
$K_B$ → Symmetric key of B.
$K_{AB}$ → Session key for both A and B.

### Step 1: Kerberos Login.

A $\xrightarrow{\text{login}}$ KDC

h[password] ⇒ $K_A$ is derived from password.
$K_A$ is the hash value of the password.

$K_A$ is known by A and KDC.

Semester: VI Subject: CSS Academic Year: 2023 2024

**Step 2: KDC generates $S_A$.**
After A logins KDC generates session key for A.

**Step 3: Send $S_A$ and TGT.**
$S_A = E("A", S_A, K_A)$ → $S_A$ is encrypted using $K_A$ (Sender).
⇒ A will decrypt with $K_A$ } (Receiver end)
A will get $S_A$.

$TGT = E("A", TGT, S_A)$ → TGT is encrypted using $S_A$ (Sender)
⇒ A will decrypt using $S_A$ and get TGT (Receiver end).

**Step 4: Request**
A sends request to TGT ⟹ A wants to communicate with B.
REQUEST = (TGT, authenticator).
authenticator = E(timestamp, $S_A$).
= E(TGT, E(timestamp, $S_A$))
KDC will decrypt using $S_A$ and will receive timestamp and TGT.

**Step 5: Reply → KDC issues a ticket to A and B.**
Reply = E("B", $K_{AB}$, Ticket to B, $S_A$).
Ticket to B = E("A", $K_{AB}$, $K_B$).
Reply = E("B", $K_{AB}$, E("A", $K_{AB}$, $K_B$), $S_A$)
A will decrypt with $S_A$, he will get $K_{AB}$ and Ticket to B.
A cannot decrypt Ticket to B, because he don't have $K_B$.

Semester : VI Subject : CSS Academic Year: 2023-2024

**Step 6 : A sends ticket to B**

A ⟶ B. ( Ticket to B, authenticator).

(E("A", $K_{AB}$, $K_B$), E (timestamp, $K_{AB}$))

1. B will decypt using $K_B$ and get $K_{AB}$.
2. B will decypt using $K_{AB}$ and get timestamp.

**Step 7 : B proves Himself.**

Now both got $K_{AB}$.

E (timestamp + 1, $K_{AB}$).

B will send the timestamp by encypting using $K_{AB}$.
A will decypt using $K_{AB}$.
B proved that he got the same session key as A has got. Now they are ready to communicate.