Kerberos Authentication

Kerberos

- The name Kerberos was taken from Greek mythology; it was a three-headed dog who guarded the gates of hades.
- The name Kerberos we are going to talk about is an authentication protocol used to verify the identity of a user or host in a network.

Kerberos

- Kerberos was originally developed at MIT.
- Most modern operating systems such as Windows, Linux, and Macintosh recently have the Kerberos protocol implemented.
- It is the default authentication protocol for network logon in Microsoft Windows.

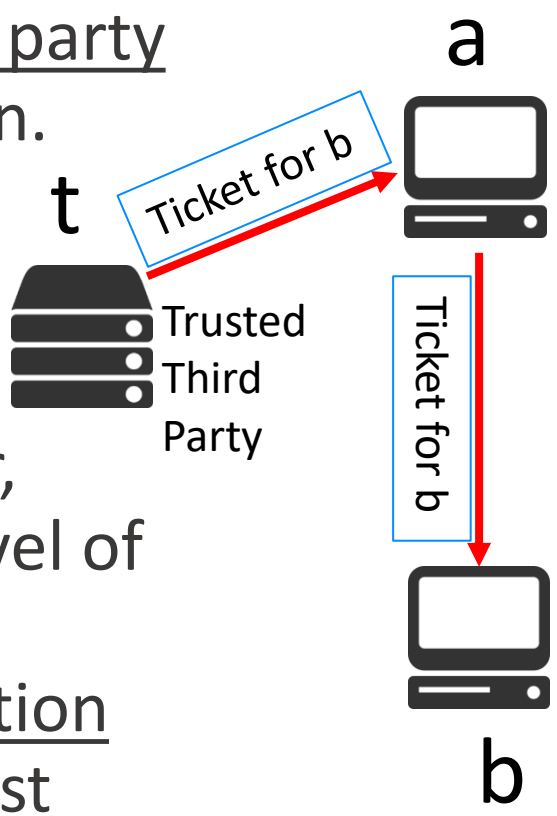
Symmetric Encryption

- Kerberos uses symmetric encryption method.

- Symmetric encryption is a data encryption method whereby the same key is used to encode and decode information.

Trusted Third Party

- Kerberos uses a trusted third party as the basis for authentication.



- A trusted third party is an independent service provider, assumed to have a certain level of trust. The trusted third party facilitates secure communication between two parties who trust this third party.

Authentication vs Authorisation

- Authentication is the act of validating that users are whom they claim to be (i.e., they are who they say they are). This is the first step in any security process.

- Authorisation is the process of giving the user permission to access a specific resource or function. This is done after authentication.

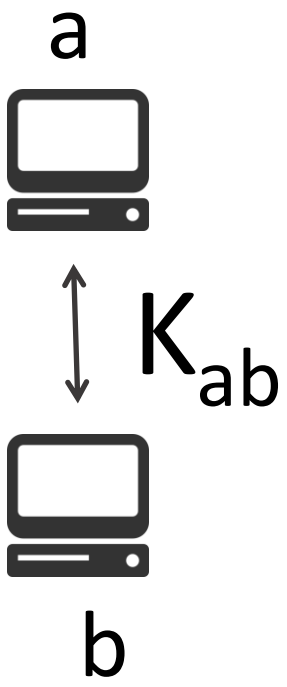
- In this session, our focus is on authentication, not authorisation.

Authentication

- In Kerberos, the authentication between a pair of nodes is done by using a key.

$$\{ \text{message} \}_{K_{ab}}$$

- A symmetric key provides mutual authentication between a pair of nodes.

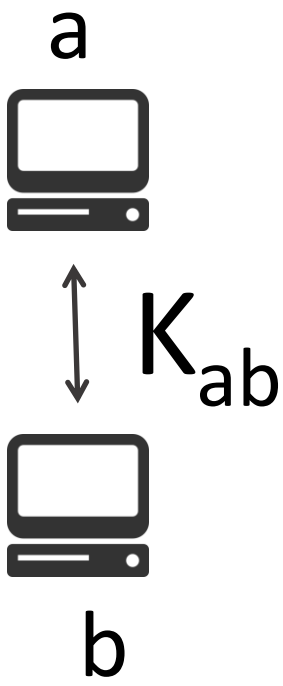


Authentication

- The key must be kept secret from other nodes, hence the term secret key.

$\{ \text{message} \}_{K_{ab}}$

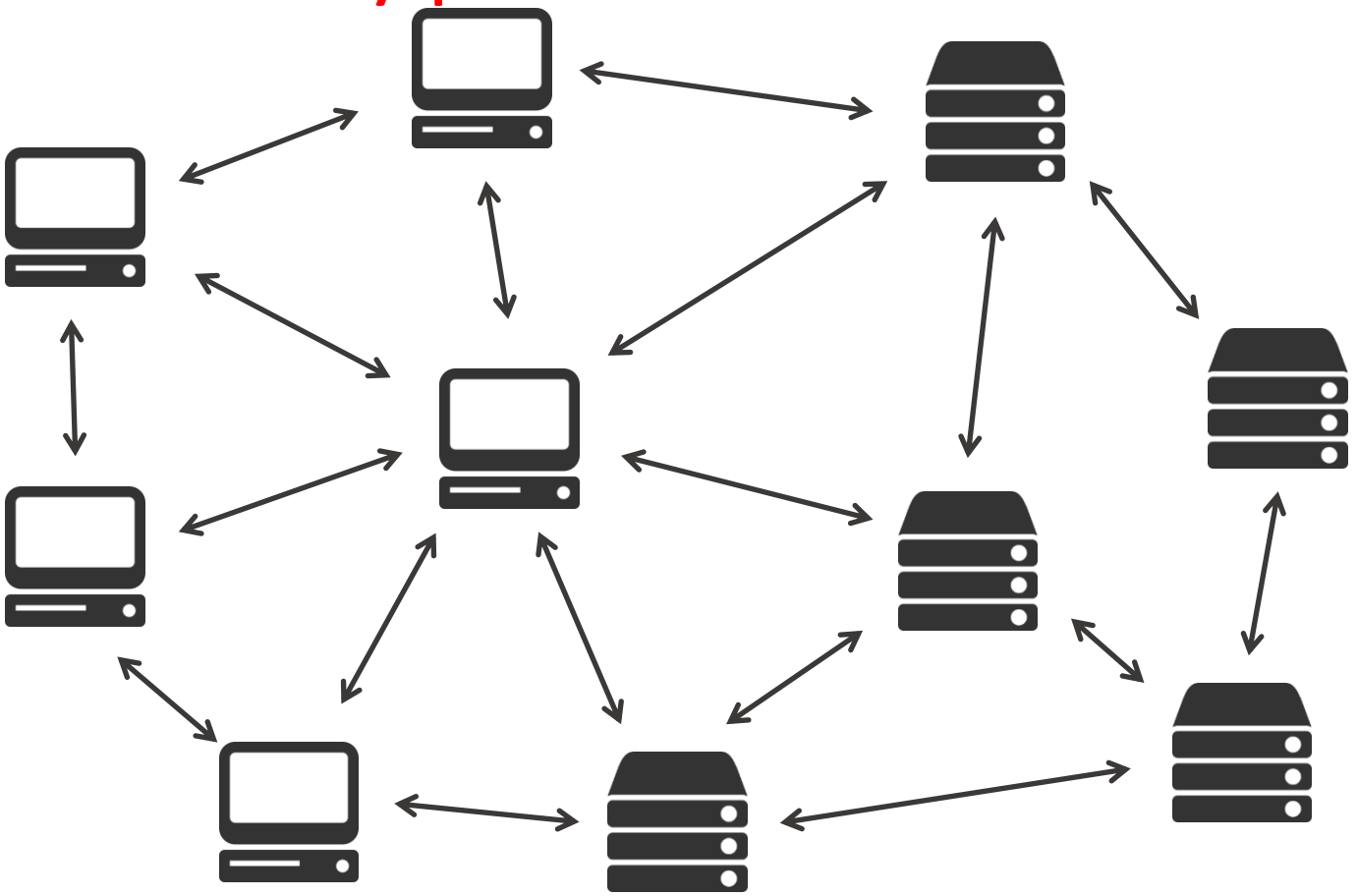
- Password is the most common form of secret key.



What happened when we have a large enterprise-wide local area network?

Encrypting Large-scale Networks

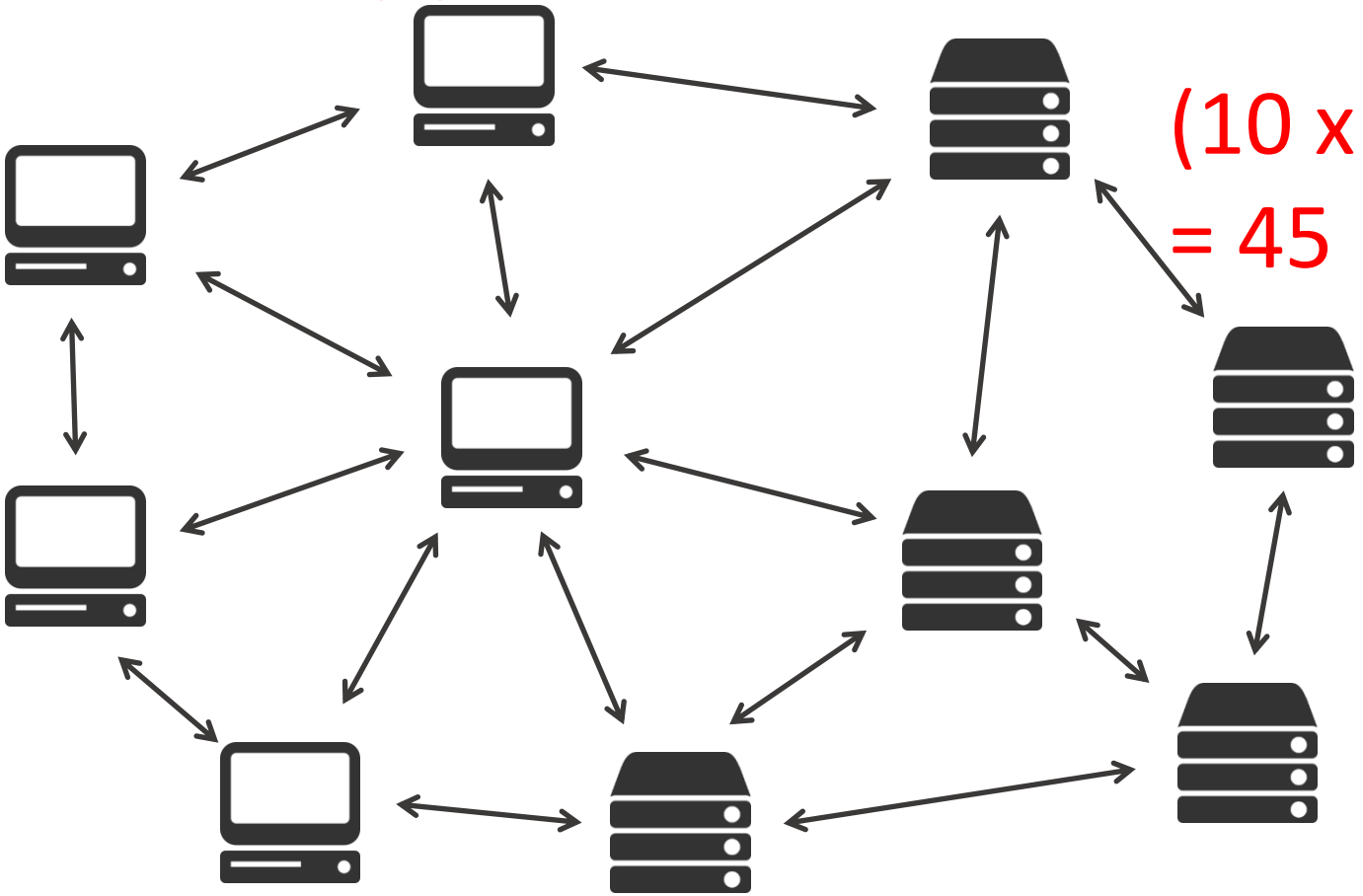
How many pairs of nodes are there?



How many secret keys are needed?

Encrypting Large-scale Networks

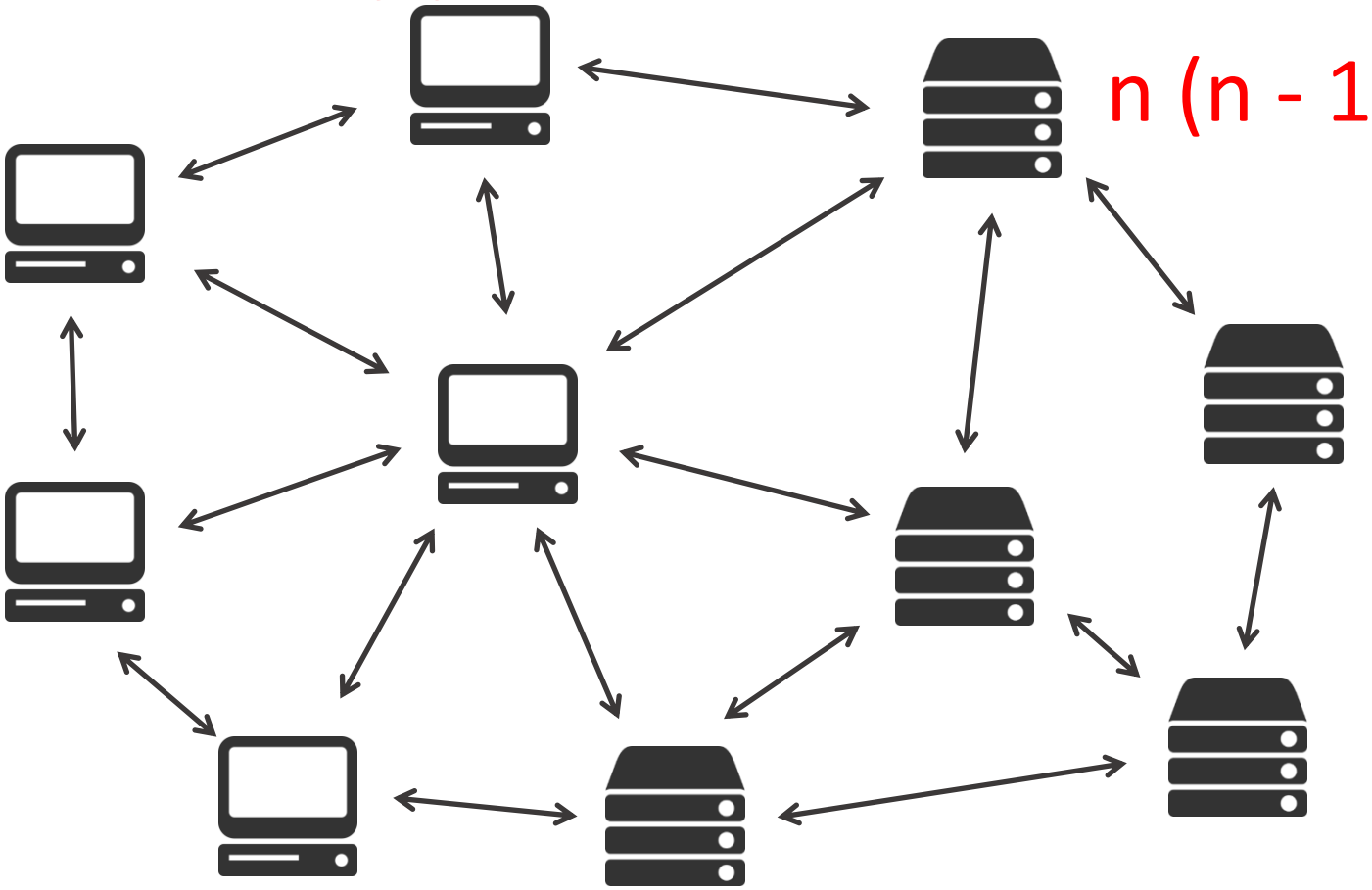
How many pairs of nodes are there?



(10 x 9) / 2
= 45

Encrypting Large-scale Networks

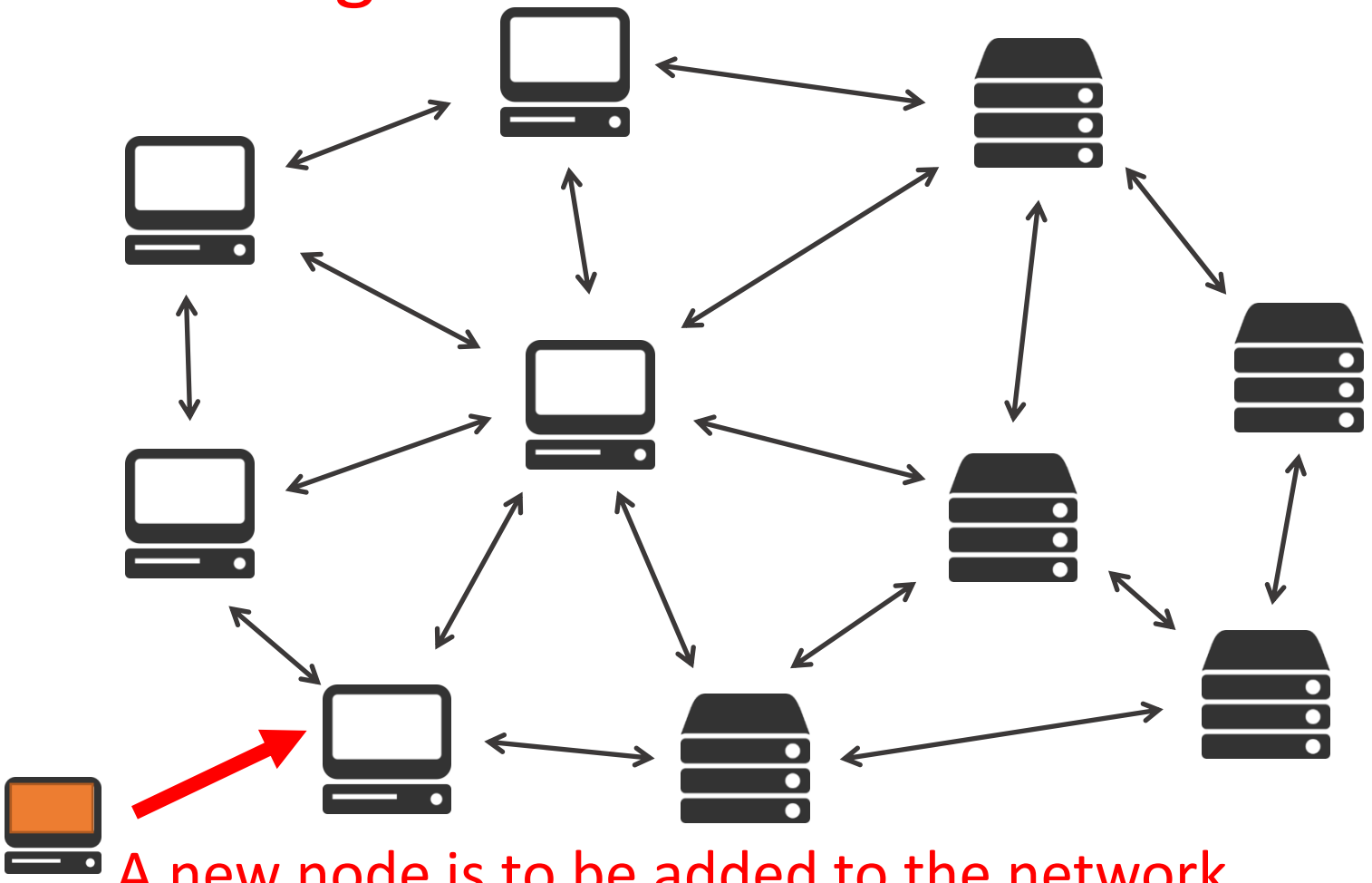
How many pairs of nodes are there?



$n (n - 1) / 2$

Encrypting Large-scale Networks

Imagine there are 1000 nodes.

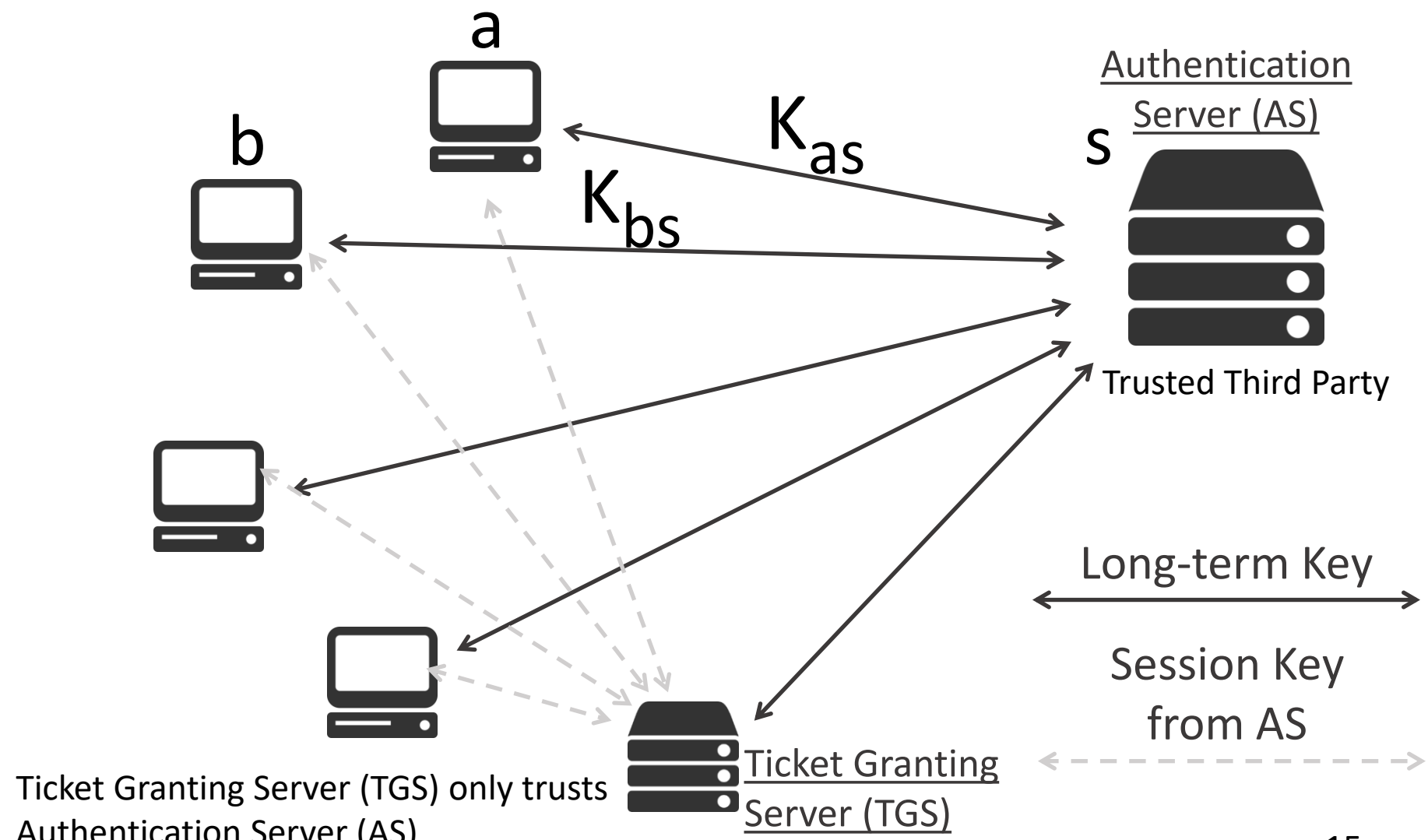


A new node is to be added to the network.

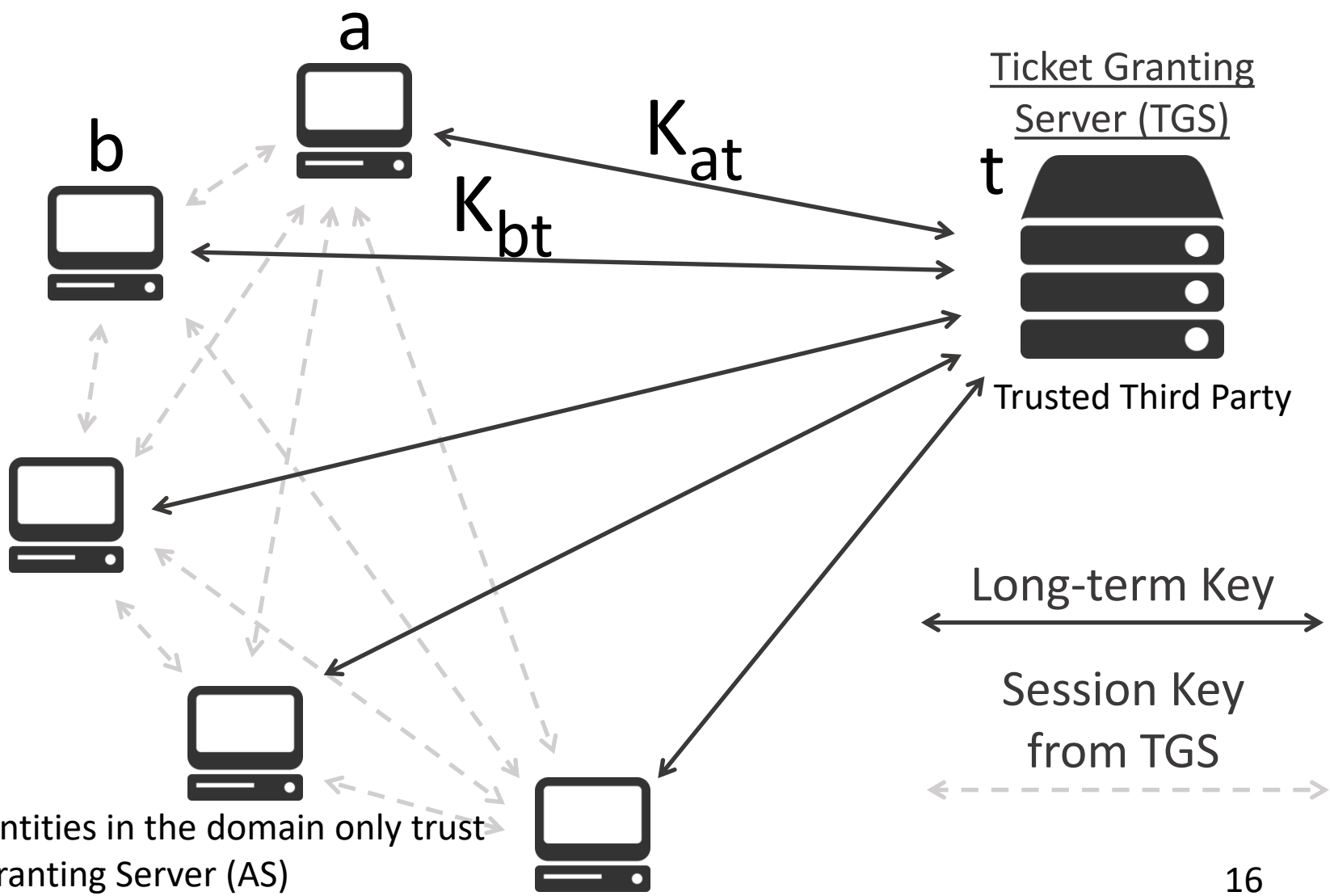
Since assigning a secret key to every pair of nodes is not practical, how should the nodes authenticate each other in a large network?

Introducing the concept of ‘Trusted Third Party’

Register with Authentication Server



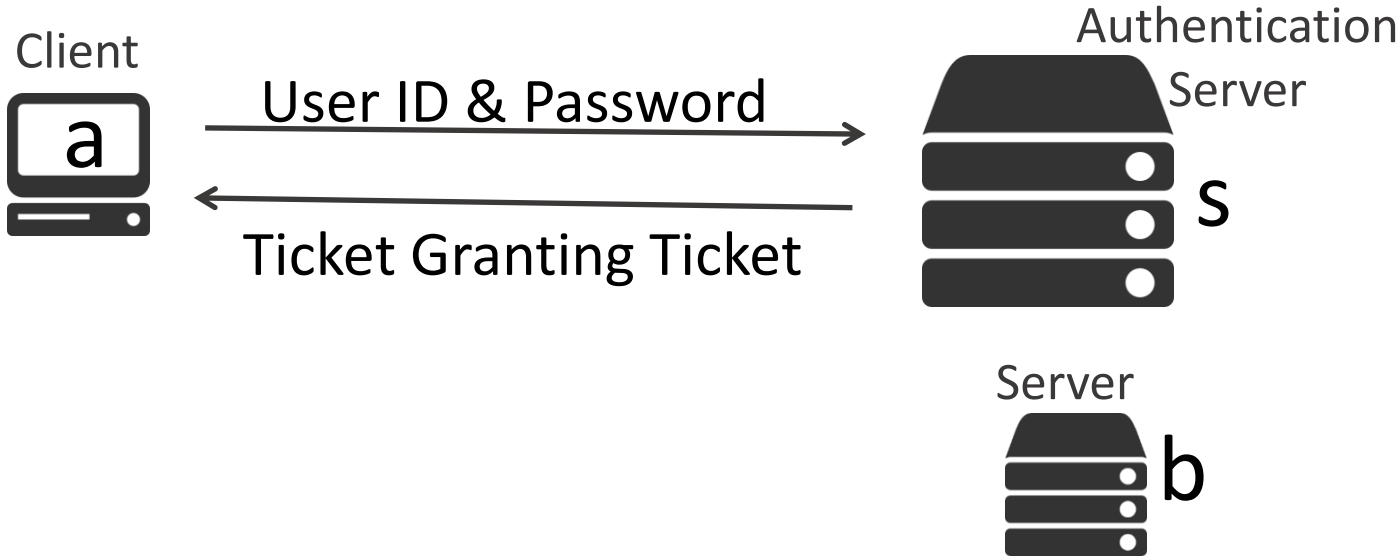
Register with Ticket Granting Server



All the entities in the domain only trust Ticket Granting Server (AS)

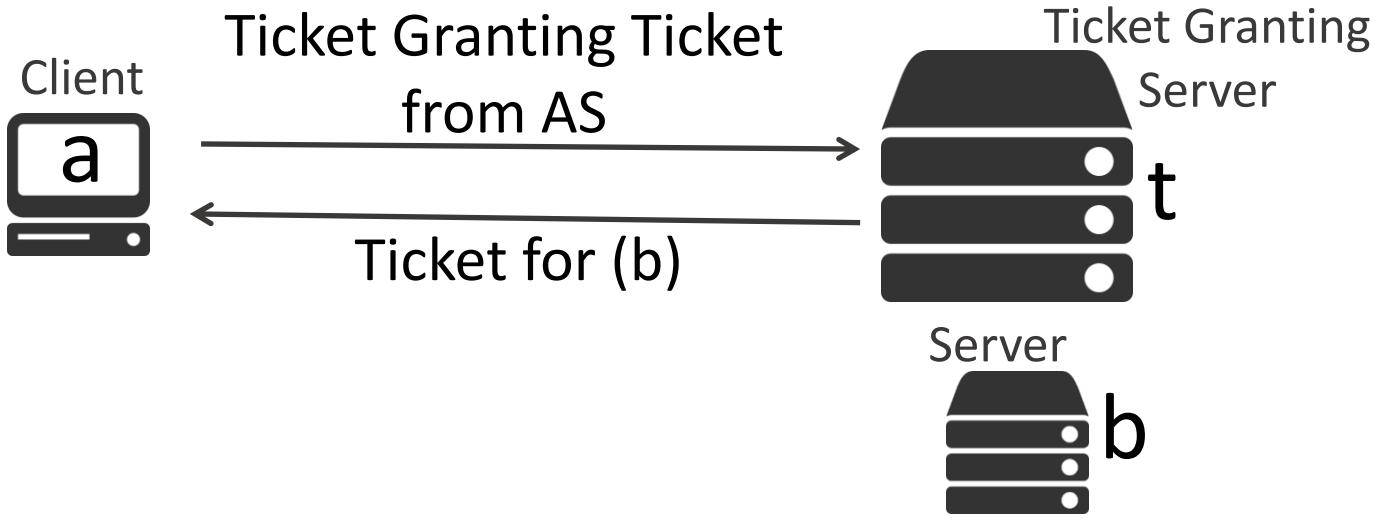
How does it work?

- In order for client (a) to get a service from server (b), client (a) has to obtain a 'Ticket for (b)' from the Ticket Granting Server.
- Prior to this, client (a) has to obtain a 'Ticket Granting Ticket' from the Authentication Server.



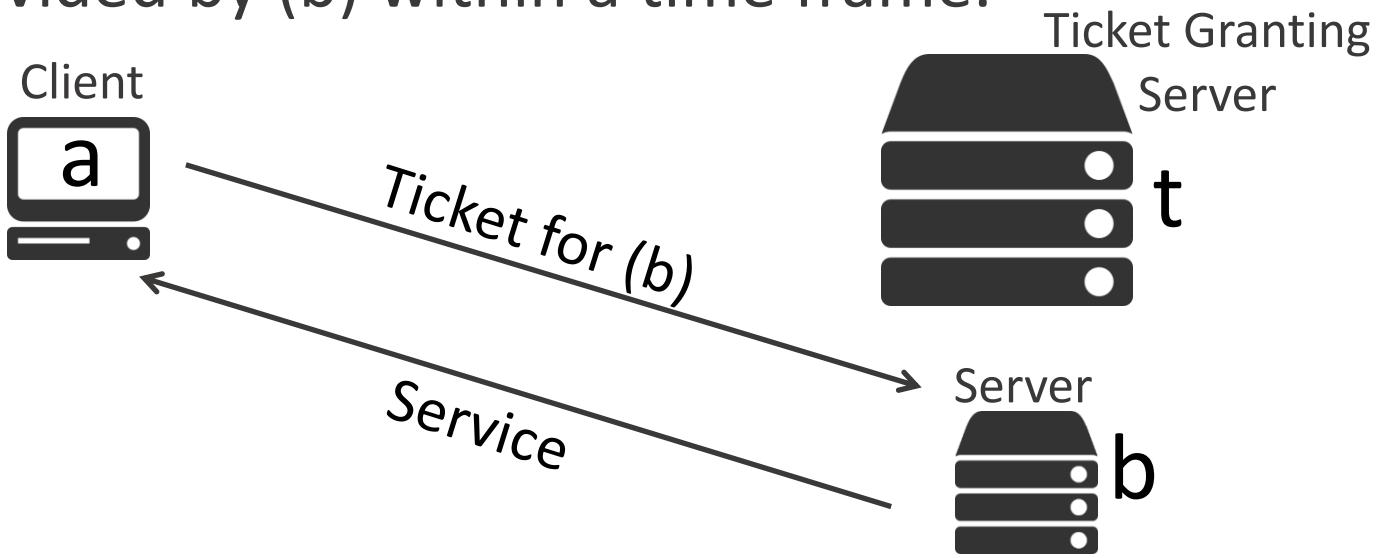
How does it work?

- Ticket Granting Server is then contacted by using the client's 'Ticket Granting Ticket' given by the Authentication Server.
- Ticket Granting Server issues another ticket 'Ticket for (b)' to the client (a) stating it is approved to use the service provided by server (b).



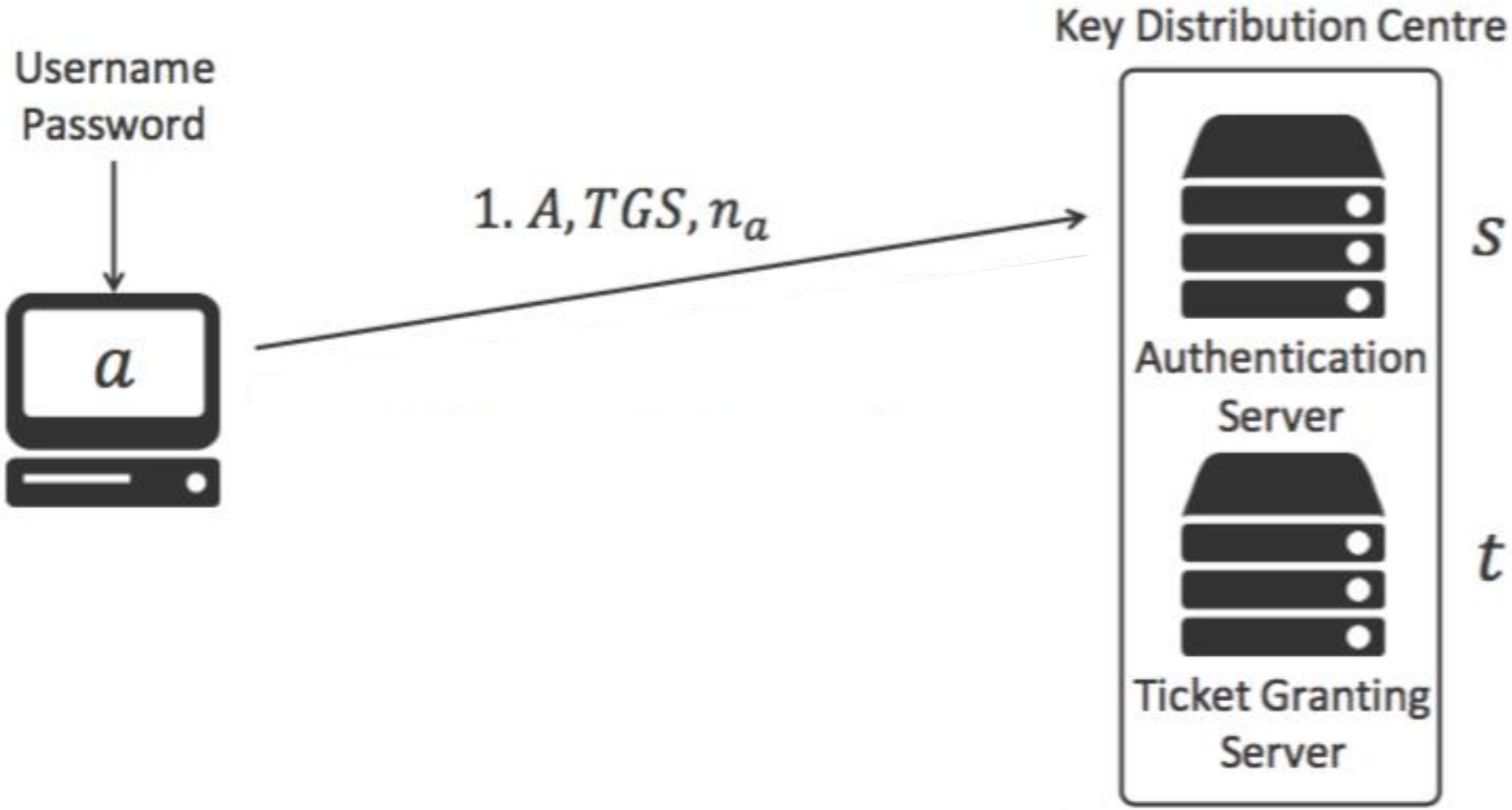
How does it work?

- The 'Ticket for (b)' is then forwarded to the server (b) requesting for a service.
- If authentication by (b) is successful, then client (a) is allowed to log in to initiate the service provided by (b) within a time frame.

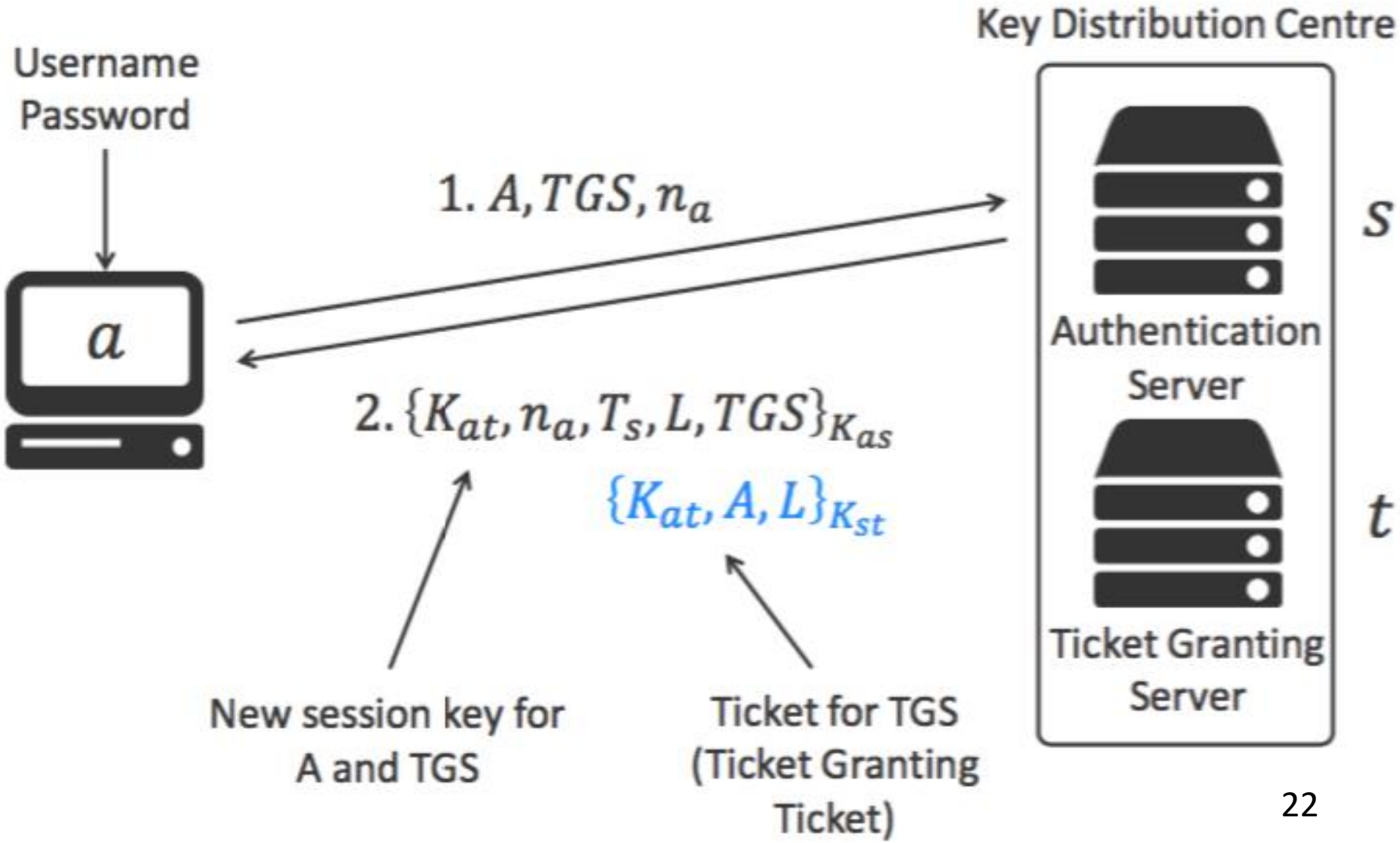


Let’s put all the concepts together for a detailed description about Kerberos Authentication.

Kerberos: Step 1, Authentication

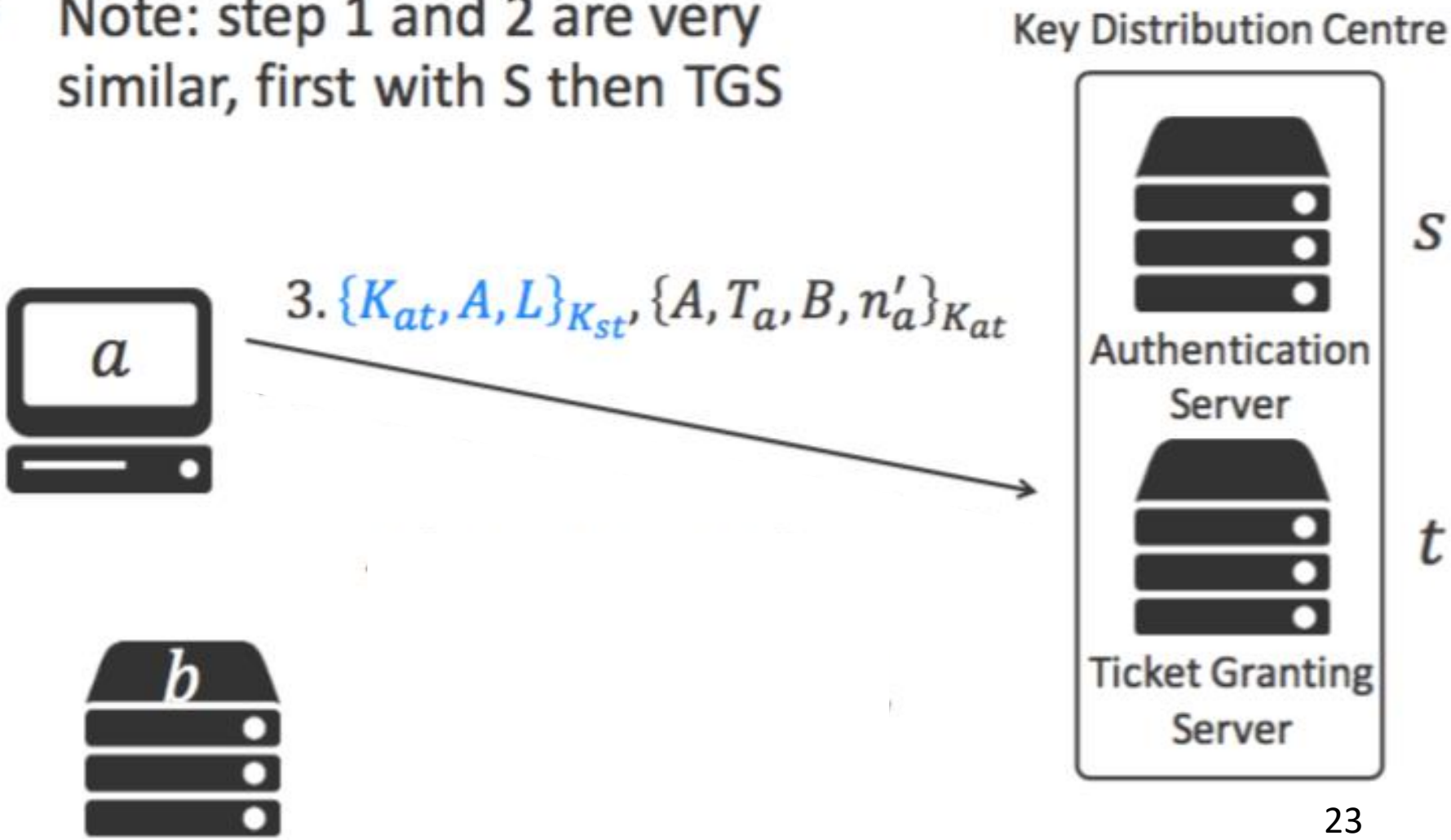


Kerberos: Step 1, Authentication



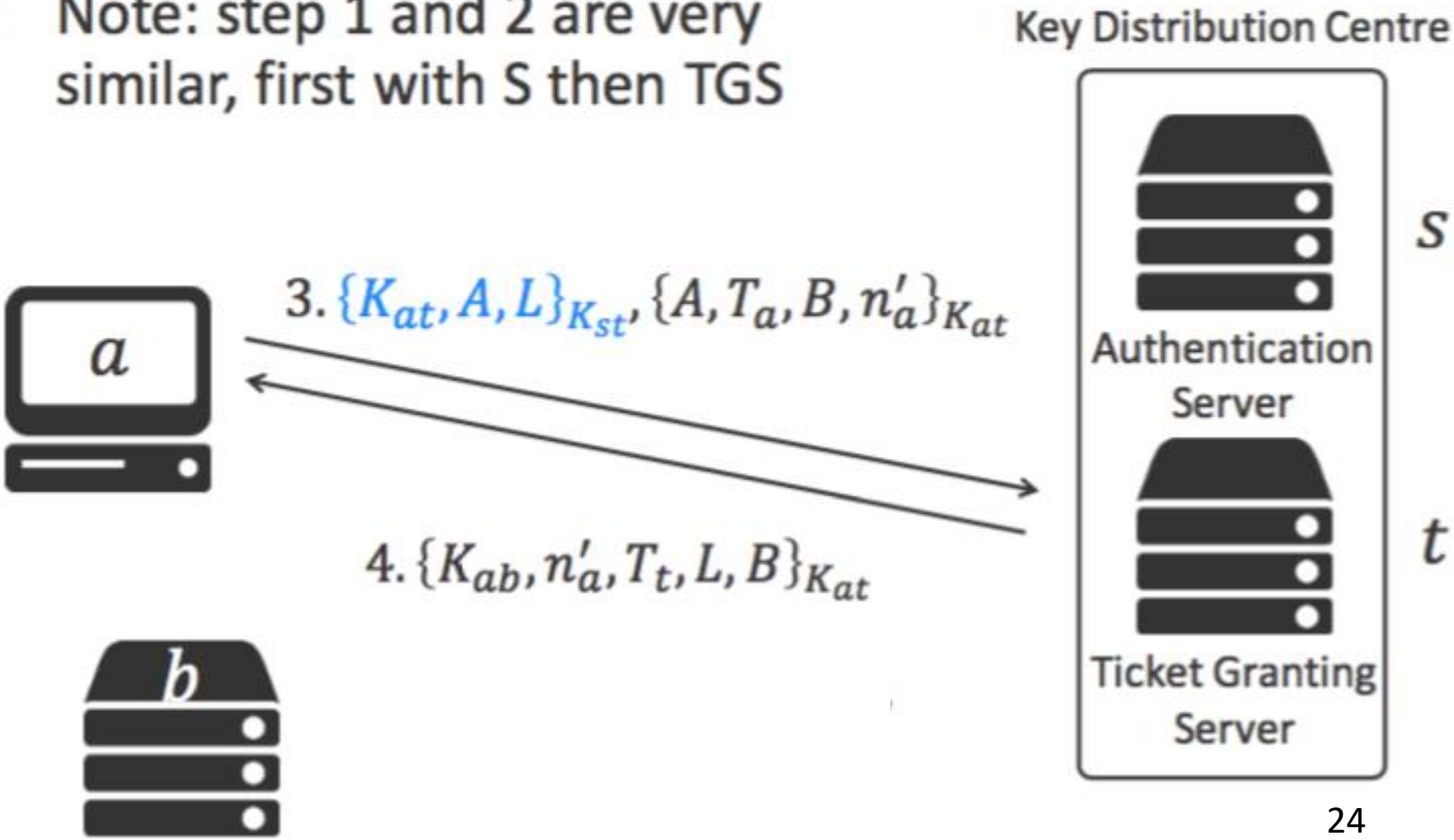
Step 2, Obtaining Tickets

- Note: step 1 and 2 are very similar, first with S then TGS



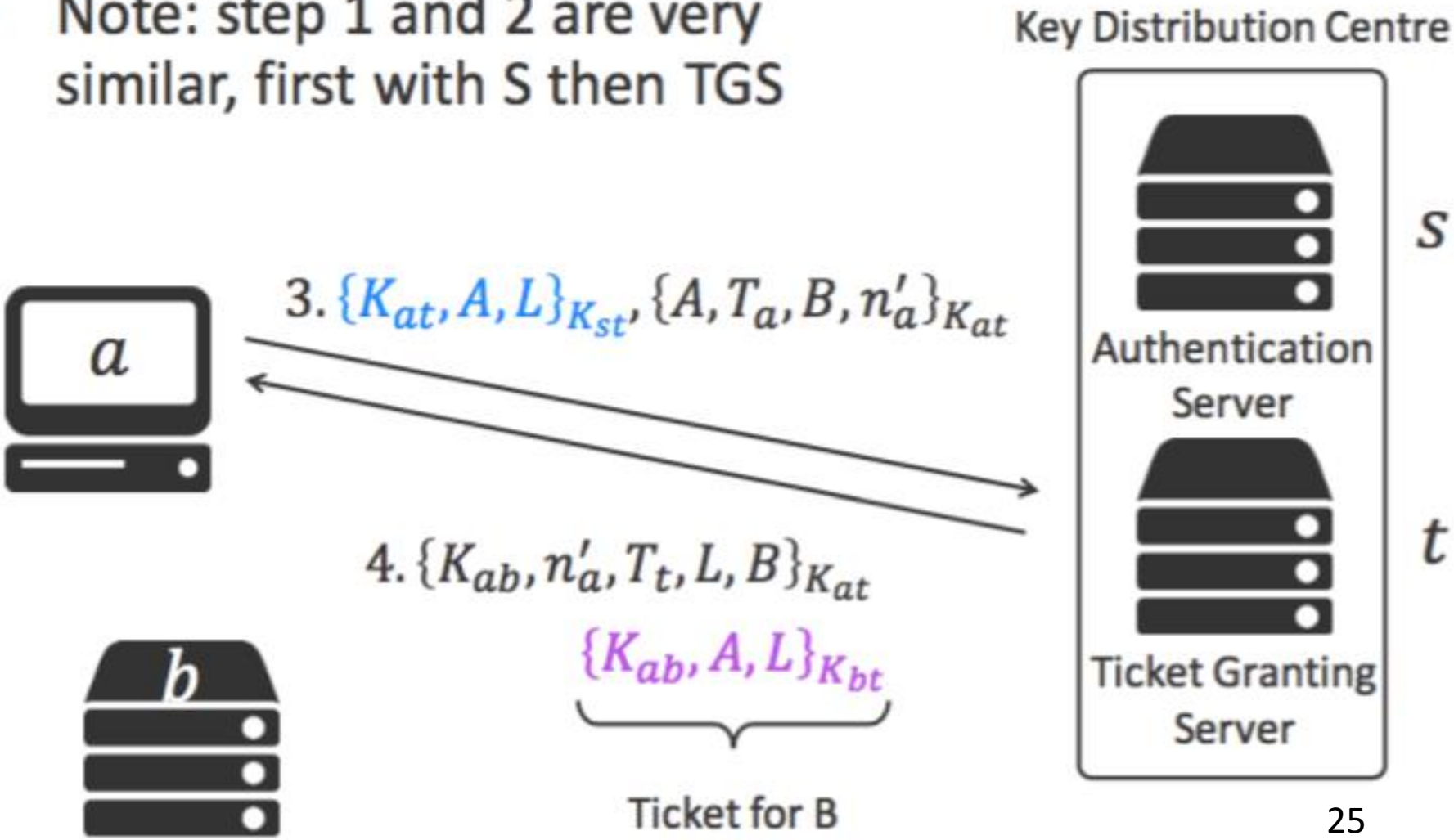
Step 2, Obtaining Tickets

- Note: step 1 and 2 are very similar, first with S then TGS

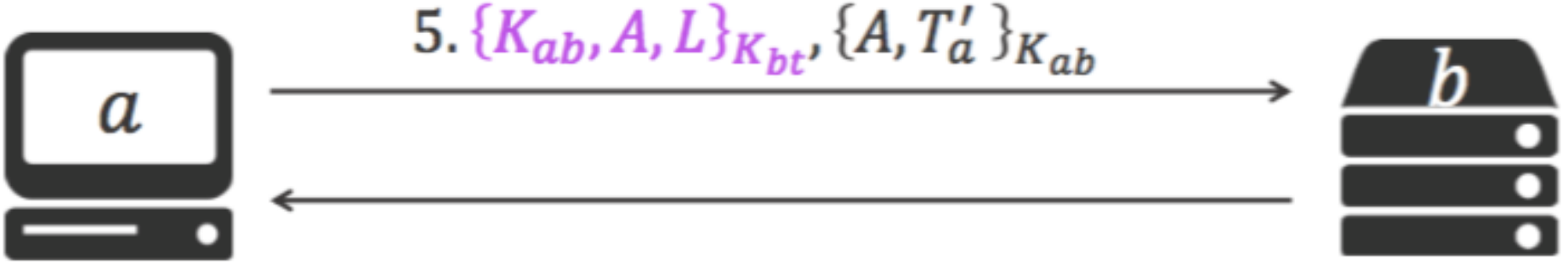


Step 2, Obtaining Tickets

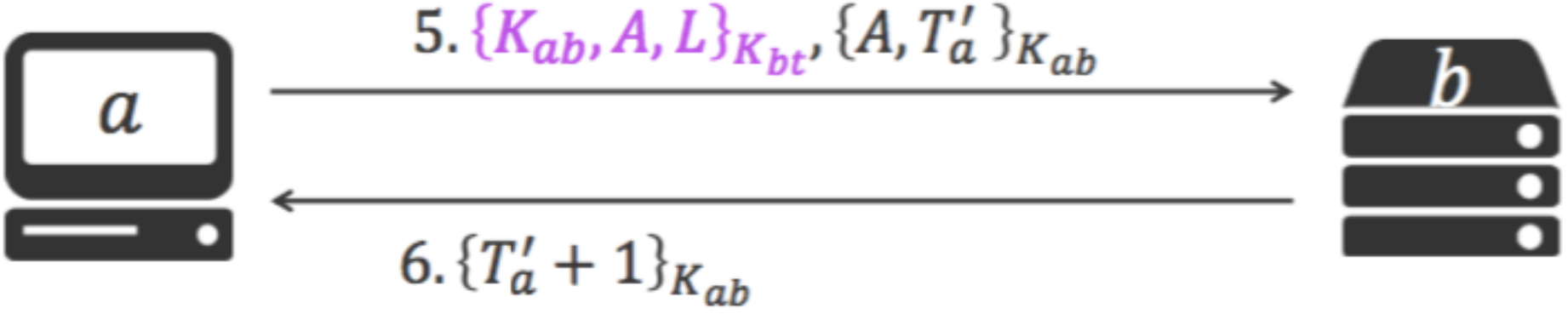
- Note: step 1 and 2 are very similar, first with S then TGS



Step 3, Using A Service

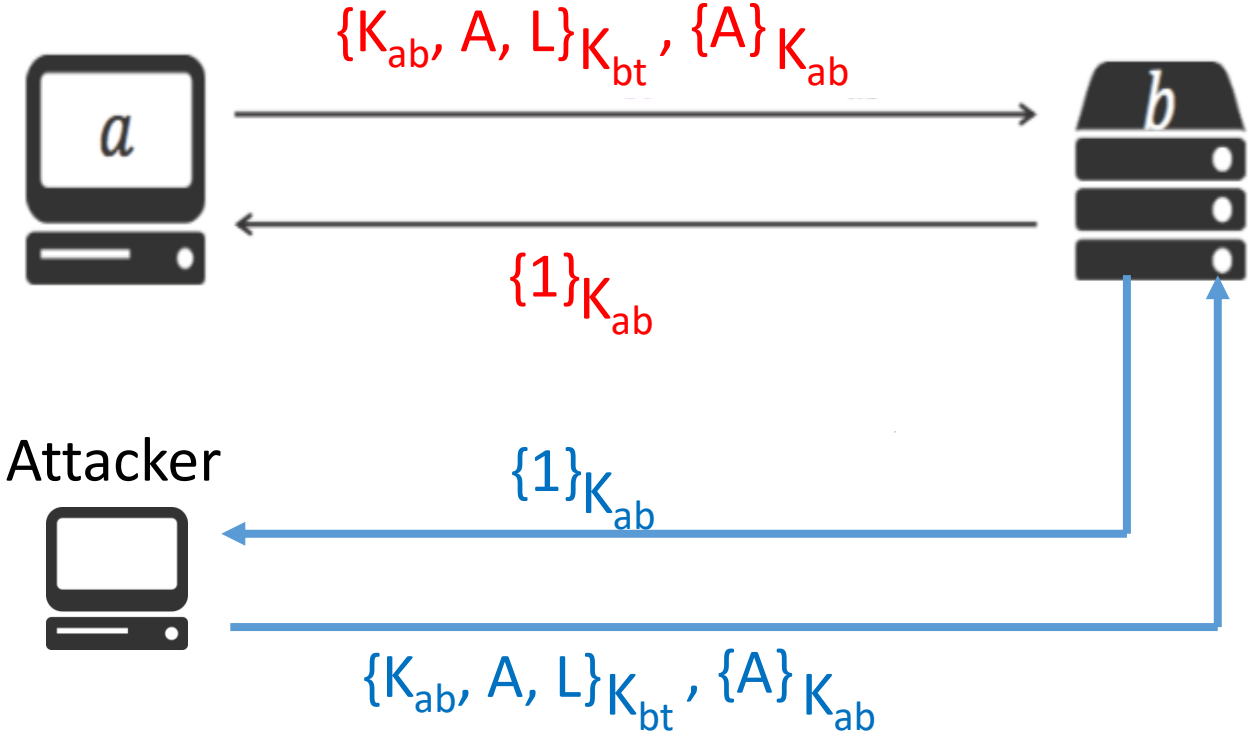


Step 3, Using A Service



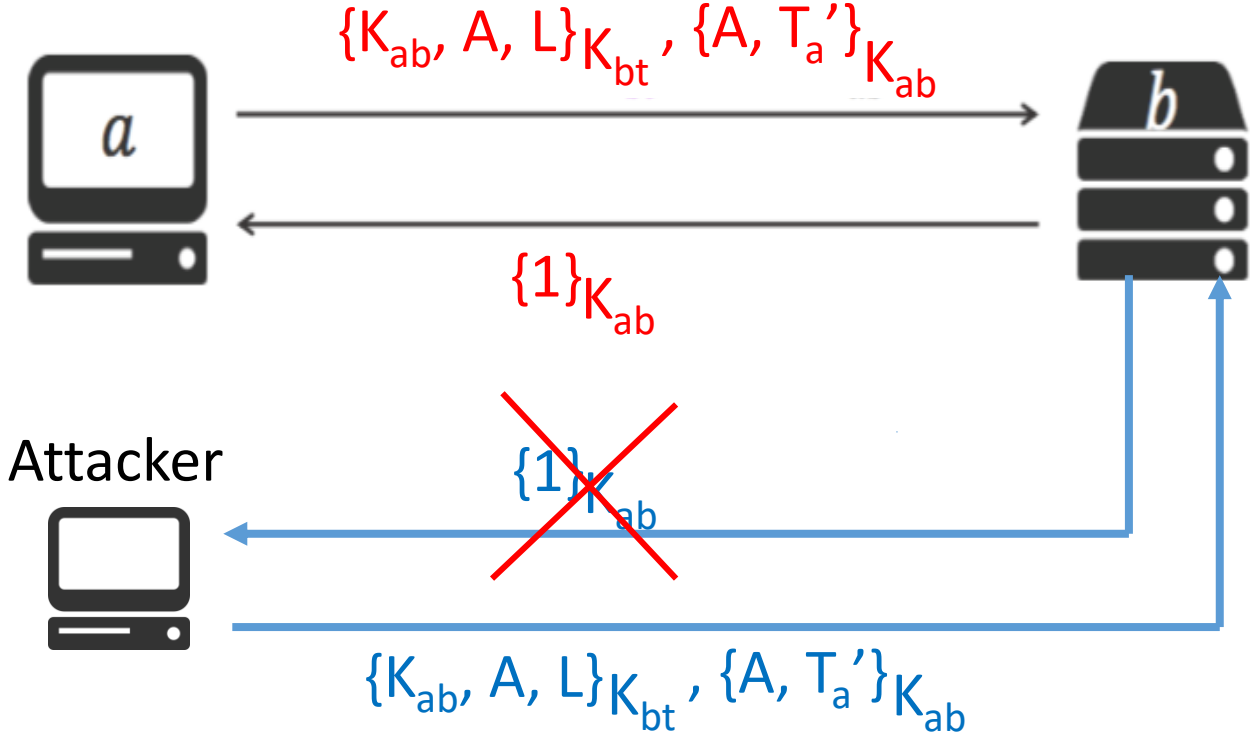
Why Use Timestamp?

- Otherwise, an attacker can copy the message, wait for client (a) to power off, and reconfigure his client using client (a)'s address, and then replay the message.



Why Use Timestamp?

- The receiver (b) checks for the timeliness by comparing its own clock value with that of the timestamp (T_a').
- Reject if timestamp is not equal to the local clock value.



Advantages of Kerberos

- Kerberos is open source.
- The availability of Kerberos on many recent operating systems such as:
  - Windows 2000 and above
  - Mac OS X
  - Red Hat Linux
  - Solaris

Drawbacks of Keberos

- Kerberos requires the usage and the availability of a central server (Key Distribution Centre); if the server happens to go down then no one can login.

- To issue proper time-stamped tickets, hosts' clocks must synchronise properly in order for the protocol to work with the timed-stamped tickets used in the authentication process.

Conclusion

- To conclude, Kerberos is a network authentication protocol that allows proper authentication between a server and a client.

- It’s a free and open source.

- It is an essential tool to provide optimum security while communicating between a server and a client.