REVA UNIVERSITY
Bengaluru, India

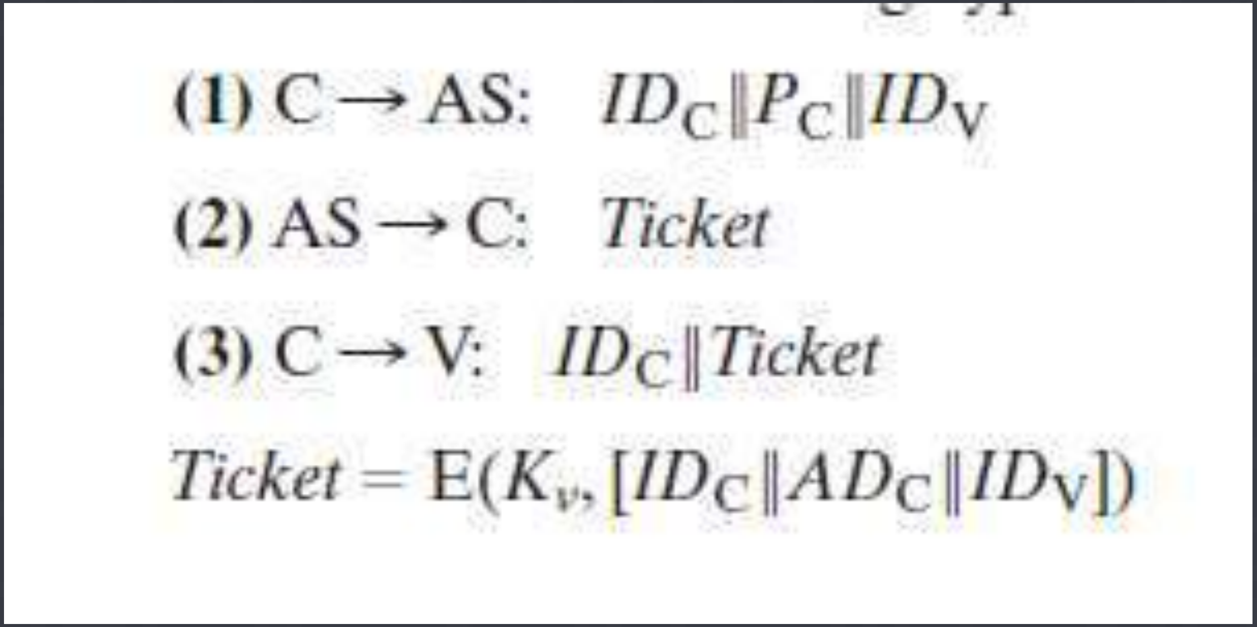
School of Computing and Information Technology

Course Delivery

Prof. Raghavendra Nayaka P
B.Tech – VI Semester

Kerberos

- ***A SIMPLE AUTHENTICATION DIALOGUE***



$$(1)\ \mathrm{C} \rightarrow \mathrm{AS}: \quad ID_{\mathrm{C}} \| P_{\mathrm{C}} \| ID_{\mathrm{V}}$$

$$(2)\ \mathrm{AS} \rightarrow \mathrm{C}: \quad Ticket$$

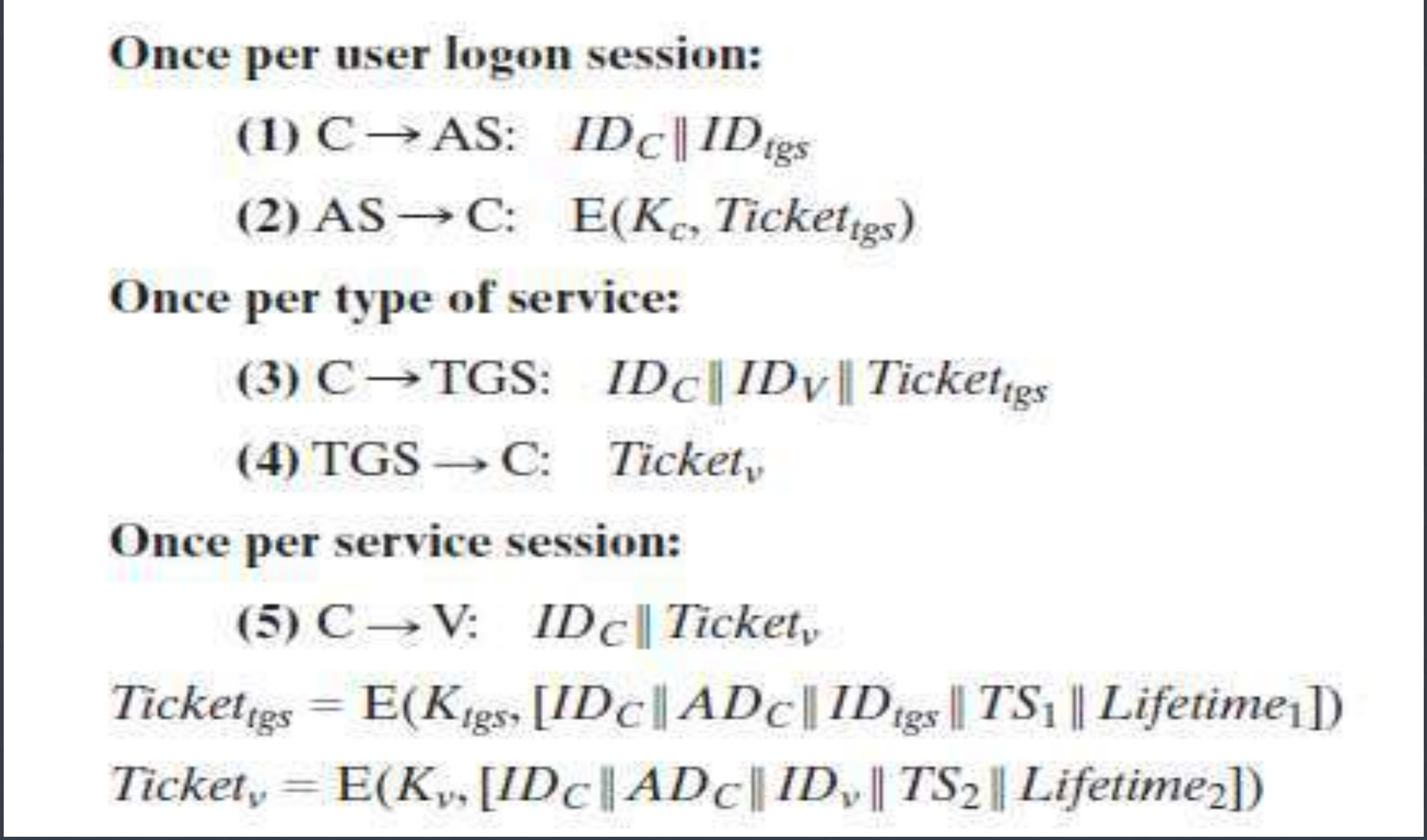
$$(3)\ \mathrm{C} \rightarrow \mathrm{V}: \quad ID_{\mathrm{C}} \| Ticket$$

$$Ticket = \mathrm{E}(K_v, [ID_{\mathrm{C}} \| AD_{\mathrm{C}} \| ID_{\mathrm{V}}])$$

Kerberos(contd.)

REVA UNIVERSITY
Bengaluru, India

- ***A MORE SECURE AUTHENTICATION DIALOGUE***



Once per user logon session:

(1) $C \rightarrow AS$: $ID_C \| ID_{tgs}$

(2) $AS \rightarrow C$: $E(K_c, Ticket_{tgs})$

Once per type of service:

(3) $C \rightarrow TGS$: $ID_C \| ID_V \| Ticket_{tgs}$

(4) $TGS \rightarrow C$: $Ticket_v$

Once per service session:

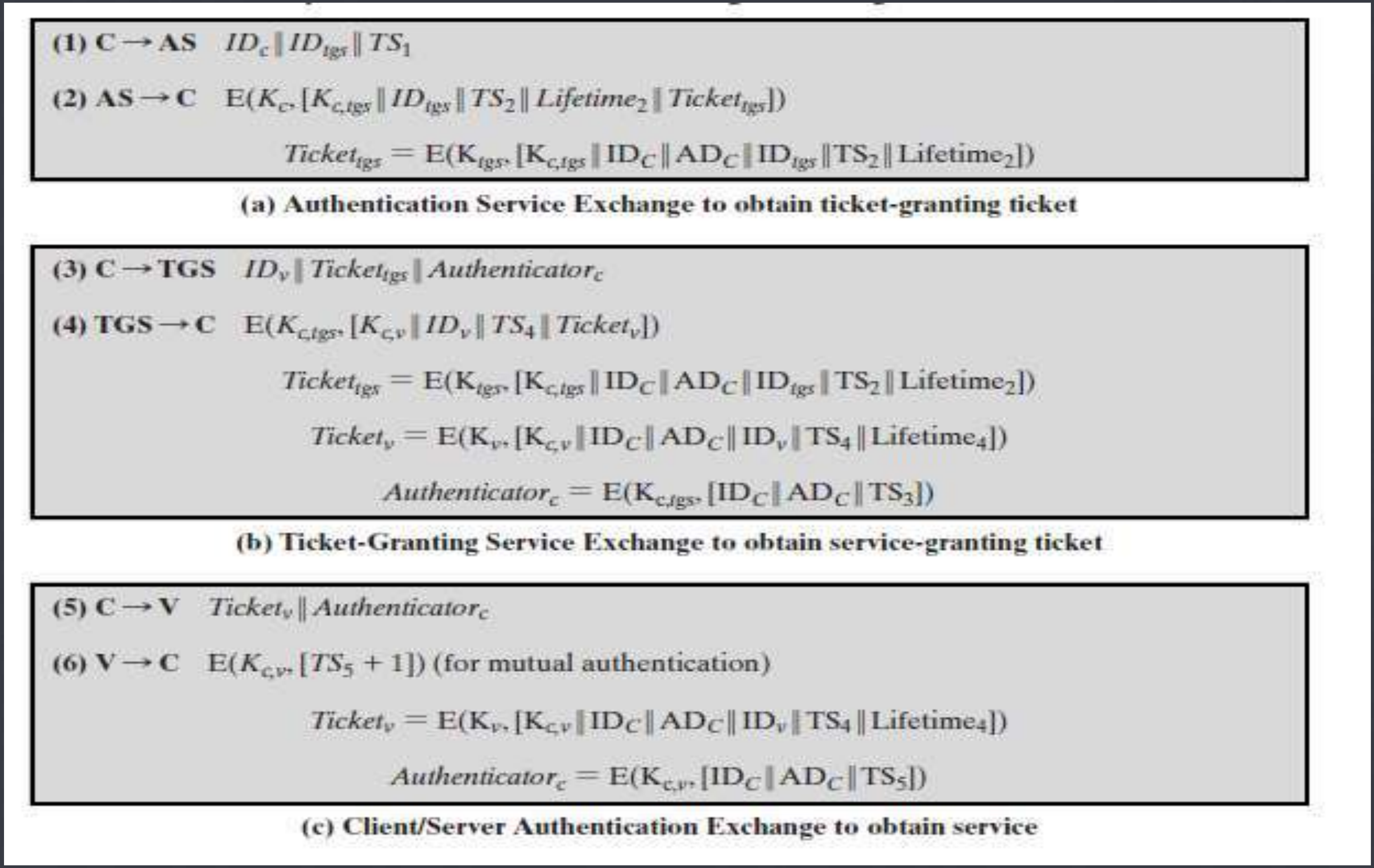
(5) $C \rightarrow V$: $ID_C \| Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$

$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$

Kerberos (contd.)

- ***THE VERSION 4 AUTHENTICATION DIALOGUE***



(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \| Authenticator_c$

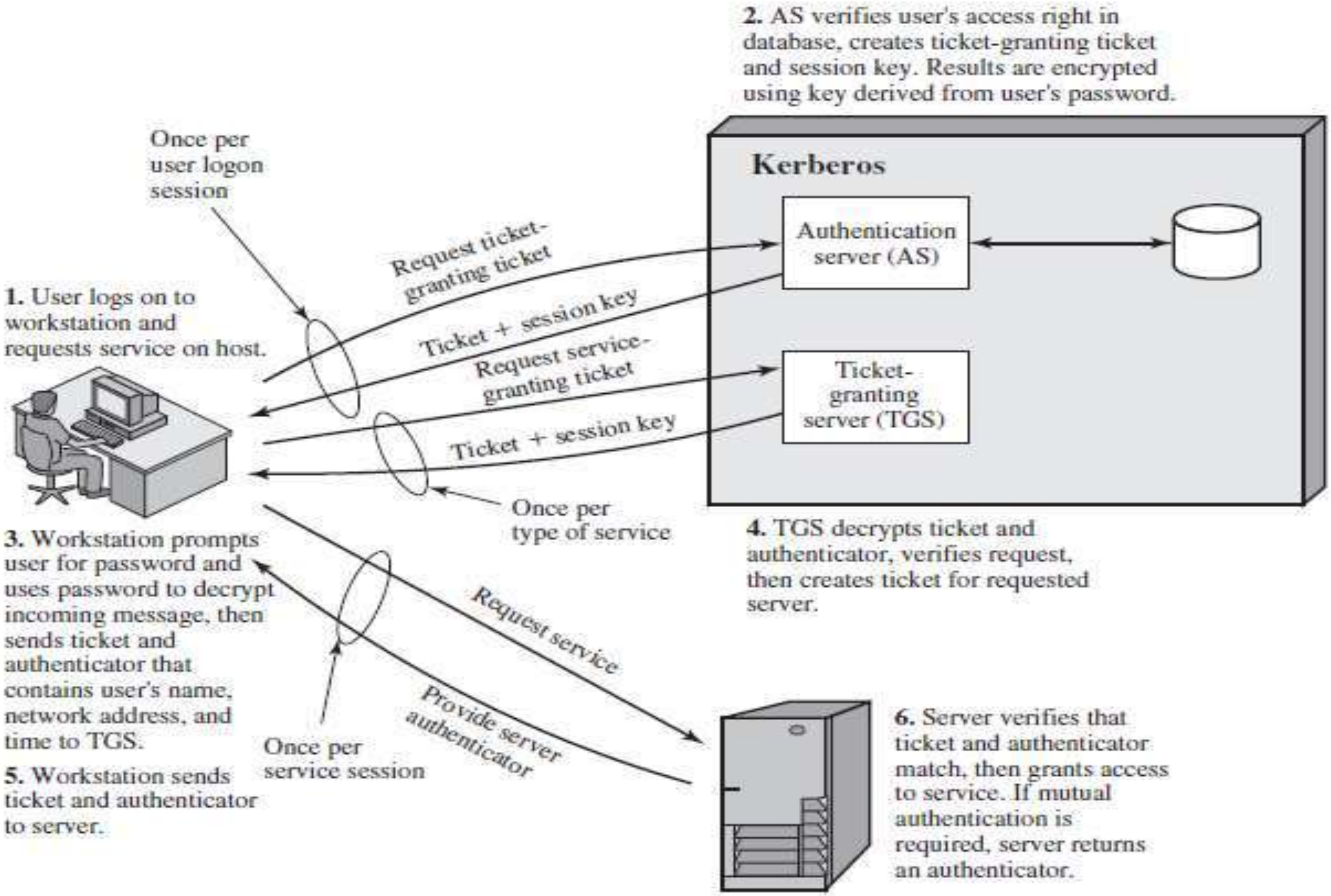
(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

Overview of Kerberos


Kerberos
Authentication server (AS)
Ticket-granting server (TGS)
Once per user logon session
Request ticket-granting ticket
Ticket + session key
Request service-granting ticket
Ticket + session key
Once per type of service
Request service
Provide server authenticator
Once per service session

2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.

1. User logs on to workstation and requests service on host.

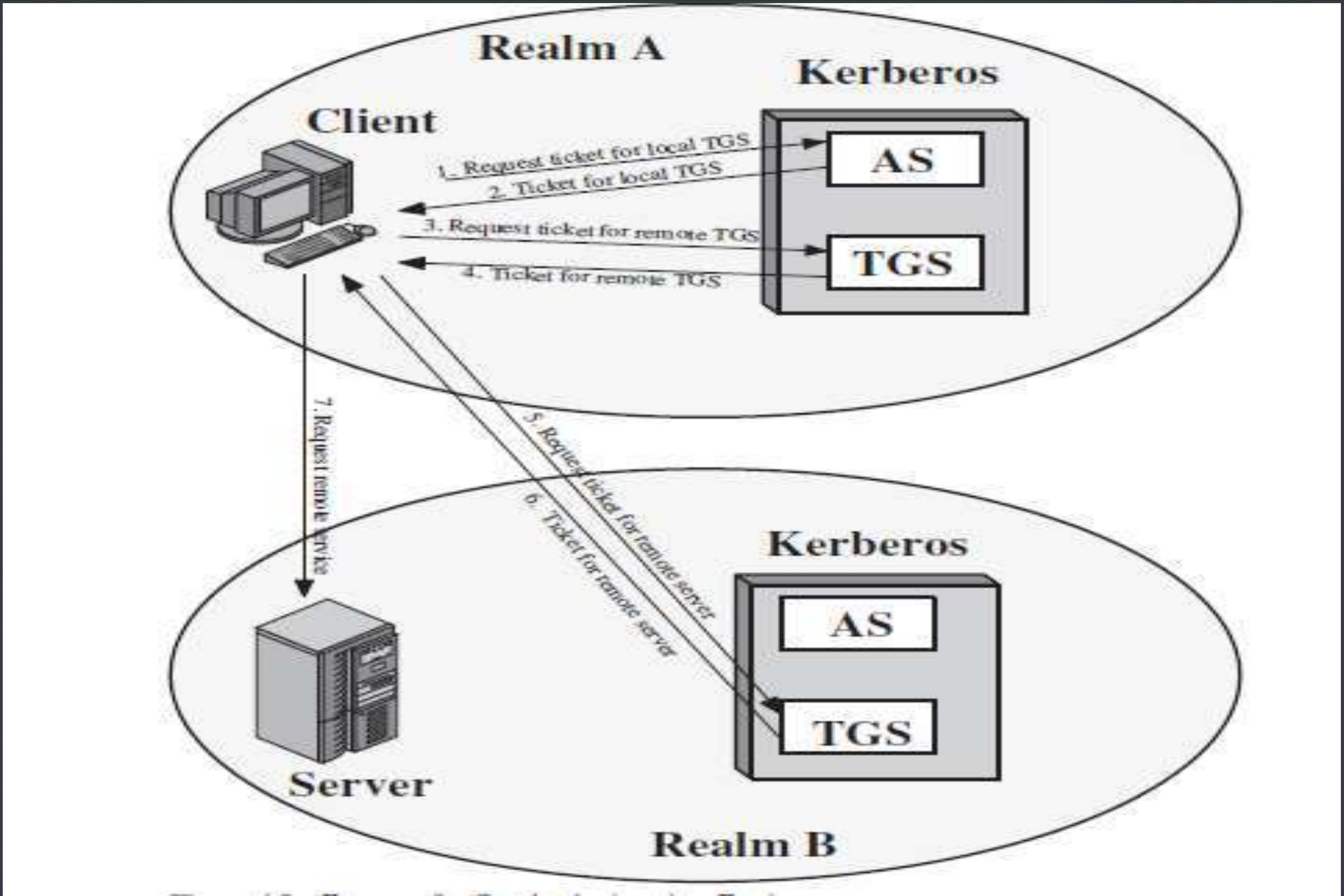
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.

4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.

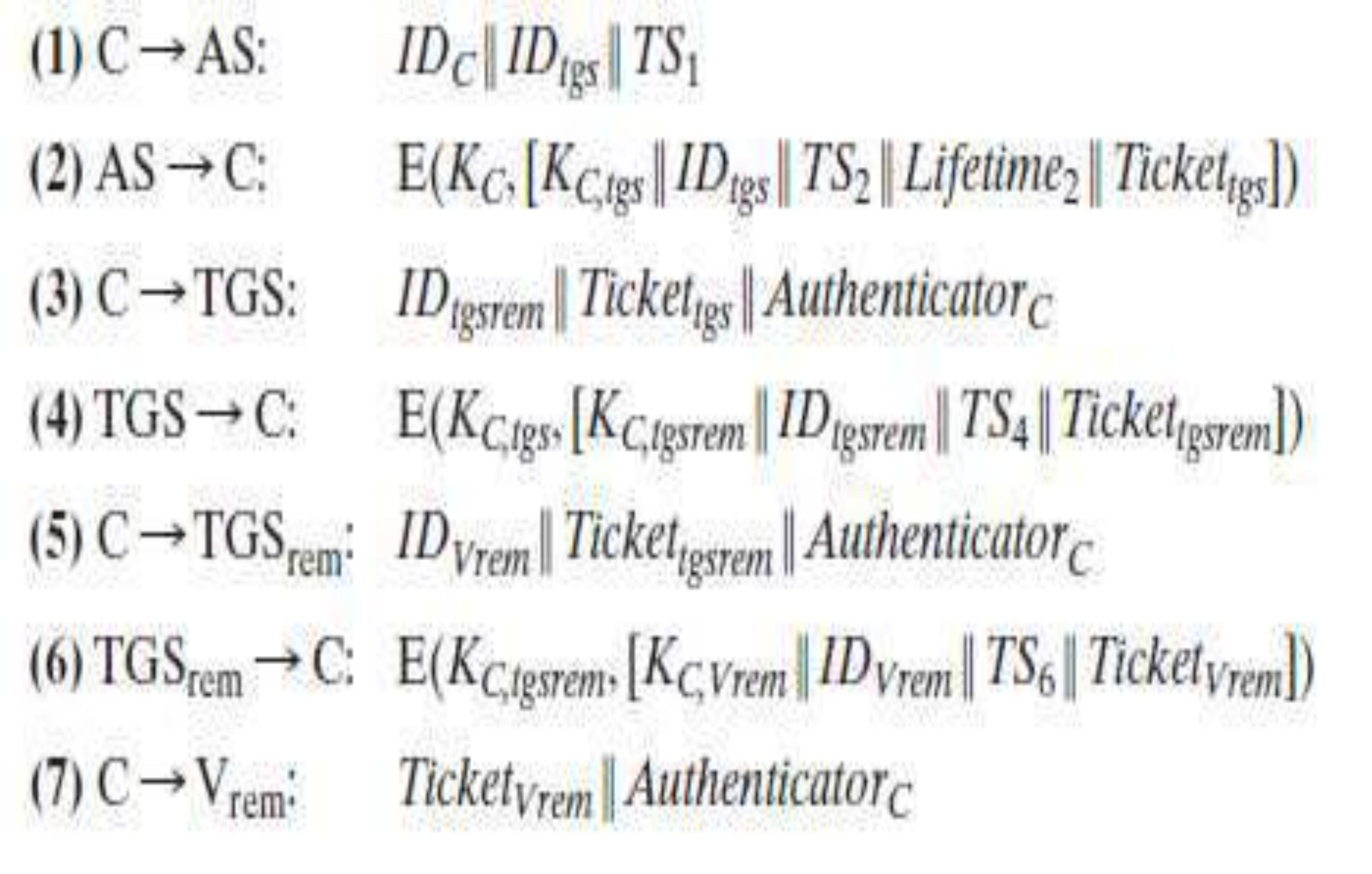
5. Workstation sends ticket and authenticator to server.

6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Request for Service in Another Realm


Realm A
Kerberos
Client
AS
TGS
1. Request ticket for local TGS
2. Ticket for local TGS
3. Request ticket for remote TGS
4. Ticket for remote TGS
5. Request ticket for remote server
6. Ticket for remote server
7. Request remote service
Kerberos
AS
TGS
Server
Realm B

Request for Service in Another Realm



(1) $C \rightarrow AS$: $ID_C \| ID_{tgs} \| TS_1$

(2) $AS \rightarrow C$: $E(K_C, [K_{C,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

(3) $C \rightarrow TGS$: $ID_{tgsrem} \| Ticket_{tgs} \| Authenticator_C$

(4) $TGS \rightarrow C$: $E(K_{C,tgs}, [K_{C,tgsrem} \| ID_{tgsrem} \| TS_4 \| Ticket_{tgsrem}])$

(5) $C \rightarrow TGS_{rem}$: $ID_{Vrem} \| Ticket_{tgsrem} \| Authenticator_C$

(6) $TGS_{rem} \rightarrow C$: $E(K_{C,tgsrem}, [K_{C,Vrem} \| ID_{Vrem} \| TS_6 \| Ticket_{Vrem}])$

(7) $C \rightarrow V_{rem}$: $Ticket_{Vrem} \| Authenticator_C$