Protocol 3 (Kerberos Version 4)

(underlined are items which do not appear in the previous protocol)

1. Authentication Service Exchange: to obtain ticket-granting ticket (once per user logon session):

$$\begin{array}{ll} 1. \quad C \rightarrow AS: & ID_c, ID_{TGS}, \underline{TS_1} \\ 2. \quad AS \rightarrow C: & E_{k_c}(\underline{K_{c,TGS}}, \underline{ID_{TGS}}, \underline{TS_2}, \underline{Lifetime_2}, Ticket_{TGS}) \end{array}$$

$$Ticket_{TGS} = E_{k_{TGS}}(\underline{K_{c,TGS}}, ID_c, AD_c, ID_{TGS}, TS_2, Lifetime_2)$$

2. Ticket - Granting Service Exchange: to obtain service-granting ticket (Once per type of service):

$$\begin{array}{ll} 1. \quad C \rightarrow TGS: & ID_v, Ticket_{TGS}, \underline{Authenticator_c} \\ 2. \quad TGS \rightarrow C: & E_{K_{c,TGS}}(\underline{K_{c,v}}, \underline{ID_v}, \underline{TS_4}, Ticket_v) \end{array}$$

$$\begin{aligned} Ticket_{TGS} &= E_{k_{TGS}}(\underline{K_{c,TGS}}, ID_c, AD_c, ID_{TGS}, TS_2, Lifetime_2) \\ Ticket_v &= E_{k_v}(\underline{K_{c,v}}, ID_c, AD_c, ID_v, TS_4, Lifetime_4) \\ Authenticator_c &= E_{K_{c,TGS}}(ID_c, AD_c, TS_3) \end{aligned}$$

3. Client/Server Authentication Exchange: to obtain service (Once per service session)

$$\begin{array}{ll} 1. \quad C \rightarrow V: & Ticket_v, \underline{Authenticator_c} \\ 2. \quad V \rightarrow C: & \underline{E_{K_{c,v}}(TS_5 + 1)} \end{array}$$

$$\begin{aligned} Ticket_v &= E_{k_v}(\underline{K_{c,v}}, ID_c, AD_c, ID_v, TS_4, Lifetime_4) \\ Authenticator_c &= E_{K_{c,v}}(ID_c, AD_c, TS_5) \end{aligned}$$