VIT | Vidyalankar Institute of Technology
Accredited A+ by NAAC

CSS

Prof. Amit K. Nerurkar
Assistant Professor
Department of Computer Engineering
Vidyalankar Institute of Technology, Wadala

VIVA/USER **Authentication** : checking validity of user

eg. Password, HOTP, Biometrics, smart card.

VIVA **Entity Authentication** :

- Both ~~Party~~ S^X & R^X has to verify each other.

eg Mutual Authentication

Authentication Protocols

VWIMP (VIVA & Interview)

① One way authentication

- A & B communicates
- B authenticates A

② Mutual authentication
(Also called as 3rd party authentication)

- A & B communicates
- A authenticates B
- B authenticates A

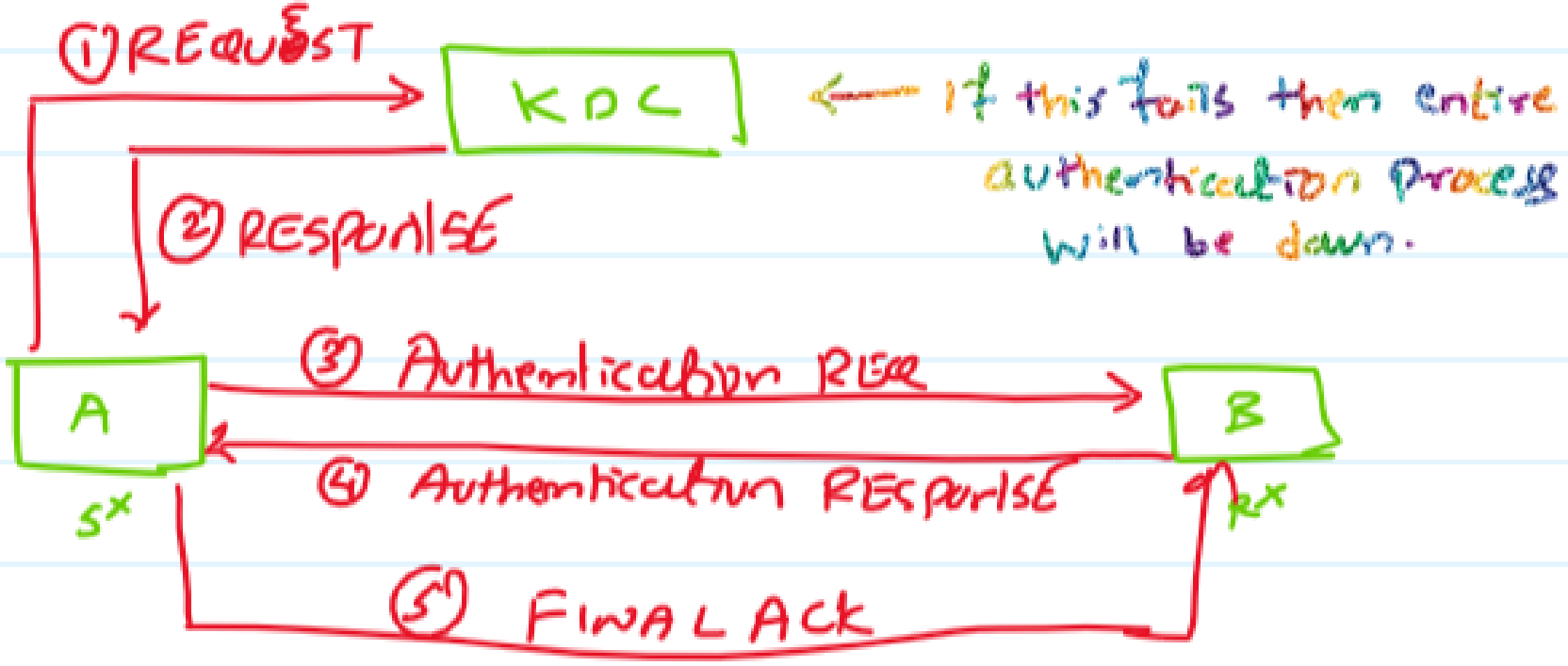
eg. KDC
- Needham Shroeder
- Kerberos

Key Distribution center

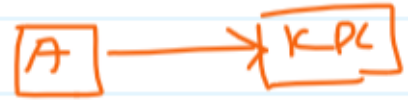
eg.1 One factor
- password

eg.2 Two factor
- password+OTP
- Card + PIN

Needham Schroeder : 1st Mutual authentication algo developed in 1978, uses KDC ie 3rd party authentication.



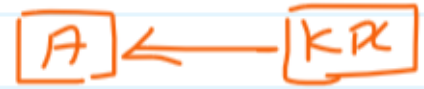
I A sends Request to KDC telling its wants to communicate with B.



(ID_A, ID_B, N_1)

ID_A: Identity of A (S^x) N_1: Nonce (Random no.)
ID_B: Identity of B (P^x)

II KDC will now create RESPONSE packet for A, which also contains Response for B.



FORMAT: $E(Key, [msg])$

msg is encrypted using key

→ $E(K_a, [K_s, ID_A, ID_B, N_1] \,||\, E(K_b, [K_s, ID_A]))$

($[K_s, ID_A, ID_B, N_1]$: A; $E(K_b, [K_s, ID_A])$: B)

K_a: A's secret key ← A ke password pe hash applied
K_b: B's secret key ← B ke password pe hash applied
K_s: Session key ← Randomly created

III Now A will decrypt this message using K_a & will get (K_S, ID_A, ID_B, M_1) & encrypted message of B. A will forward the encrypted message of B to B.

$$E(K_B, [K_S, ID_A])$$

IV B decrypts message using K_b & understands A wants to communicate (IDA) for which K_S is session key.

Now B creates a random Nonce N_2 & encrypts using K_S & sends to A.

$$E(K_S, [N_2])$$

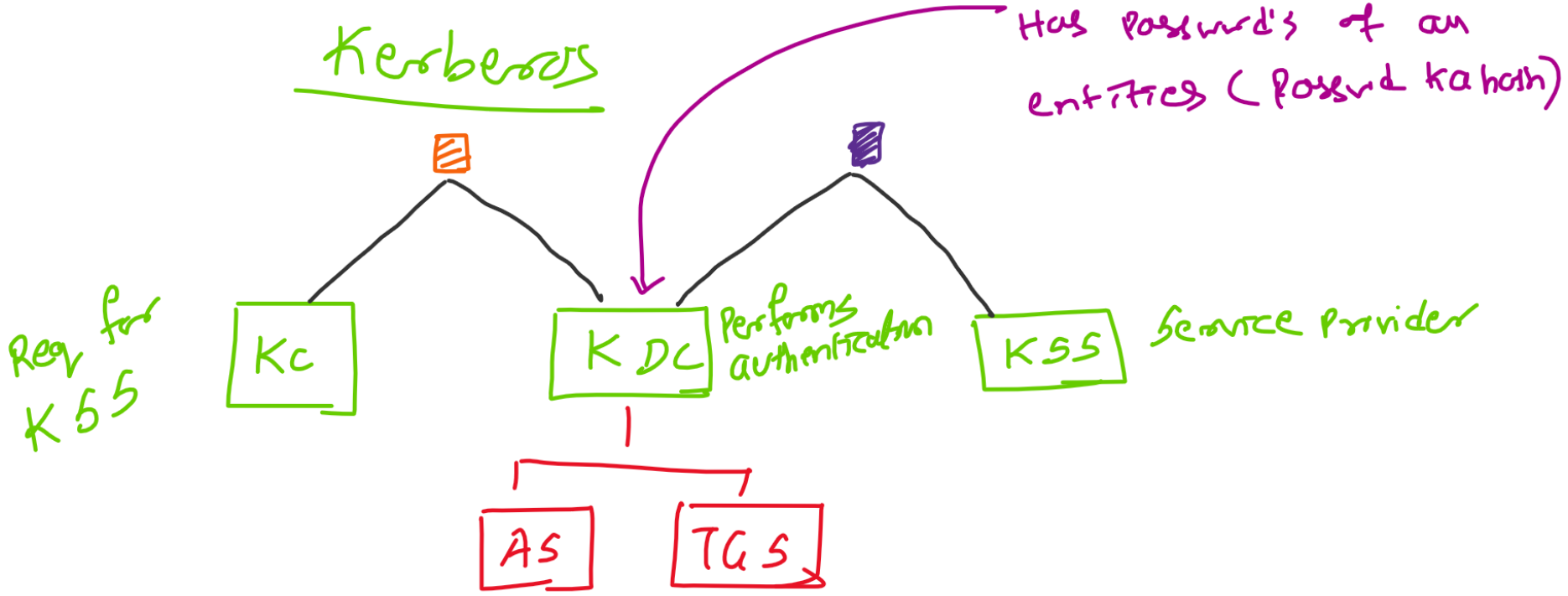
V A decryptes message using K_S & gets N_2.

Final Ack: N_2+1 & encrypt using K_S & Send to B

$$E(K_S, [N_2+1])$$

B now decrypts this using K_S.

Kerberos

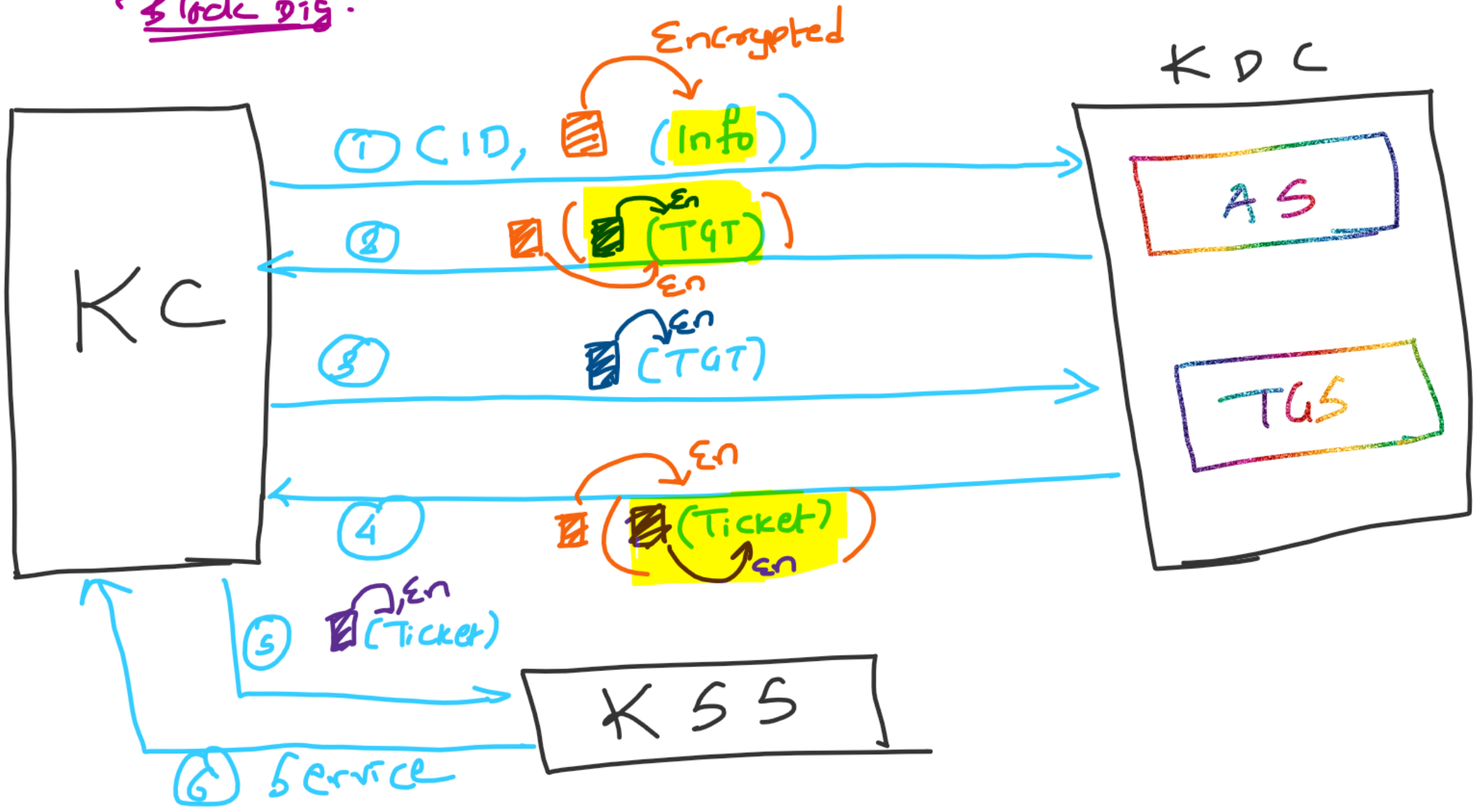


: Client's secret key [client ke passwd pe hash apply]

: Session key [TGS ke passwd pe hash apply]

: Server's secret key [server ke passwd pe hash apply]

Block Dig:


Encrypted
KDC
KC
(1) CID, (Info)
AS
(2) (TGT)
(3) (TGT)
TGS
(4) (Ticket)
(5) (Ticket)
KSS
(6) Service

Thank You

Name: *Amit K. Nerurkar*

Designation: *Assistant Professor*

College: *Vidyalankar Institute of Technology*