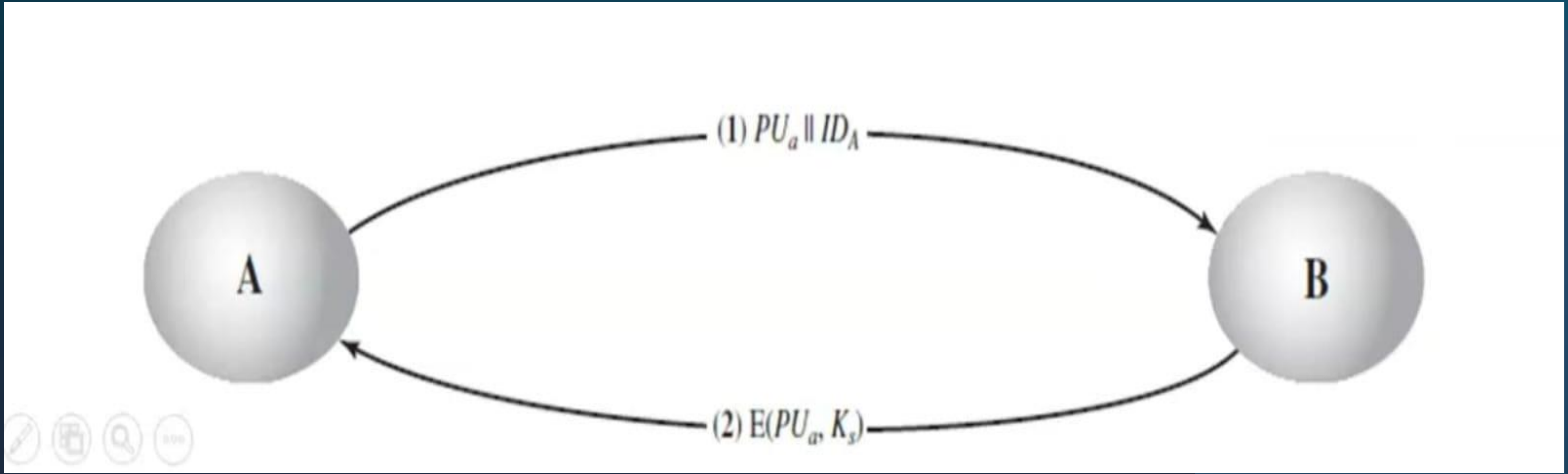
SYMMETRIC KEY DISTRIBUTION USING ASYMMETRIC ENCRYPTION

It is of 2 types

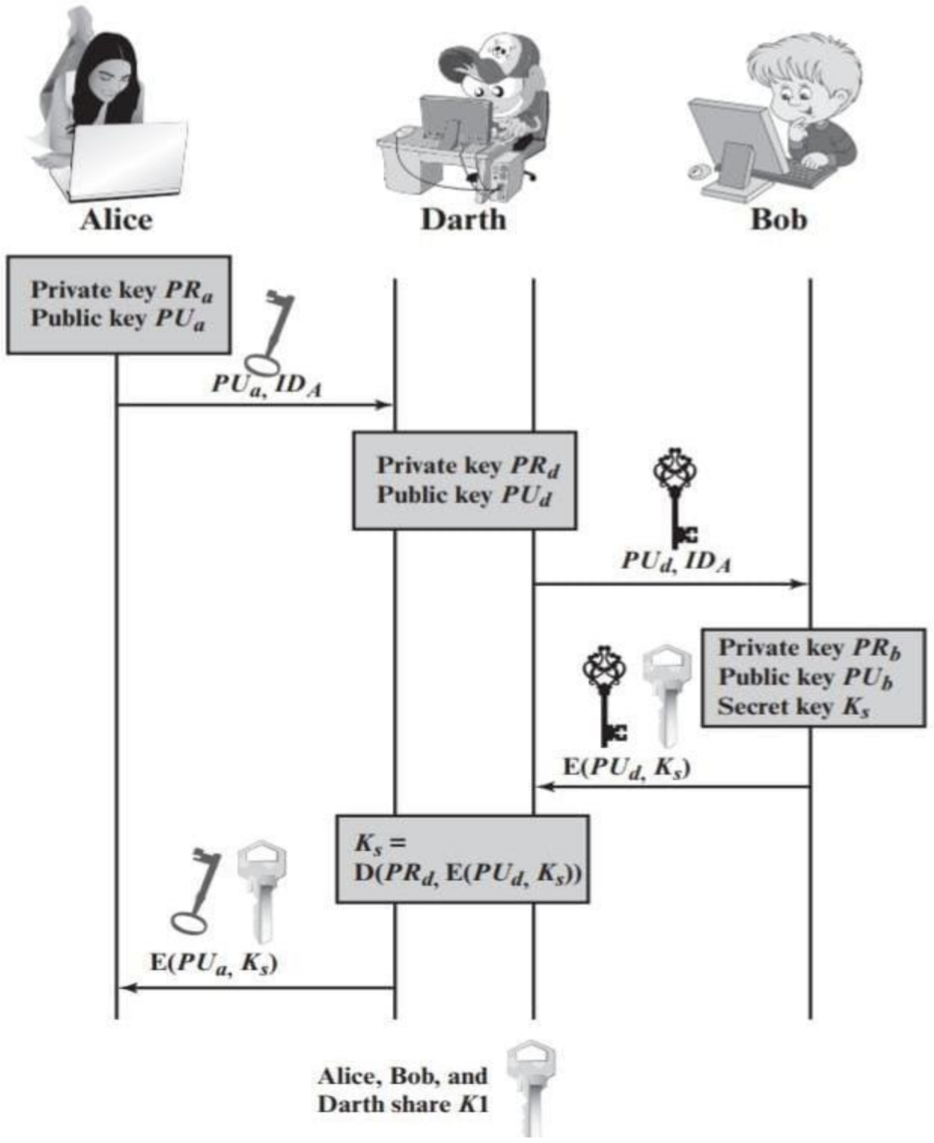
1. Simple Secret Key Distribution
2. Secret key Distrubution with Confidentiality and Authentication

Simple Secret Key Distribution

- A generates {PUa,PRa} and transmits a msg to B consisting of {PUa,IDa}
- B generates a secret key Ks and transmits its to A , which is encrypted with A's public key {E(PUa,Ks)}
- A decrypts message using {D(PRa,E(PUa,Ks))} to recover secret key
- After completion of transfer of msg , A discards {PUa,PRa} and B discards {PUa}

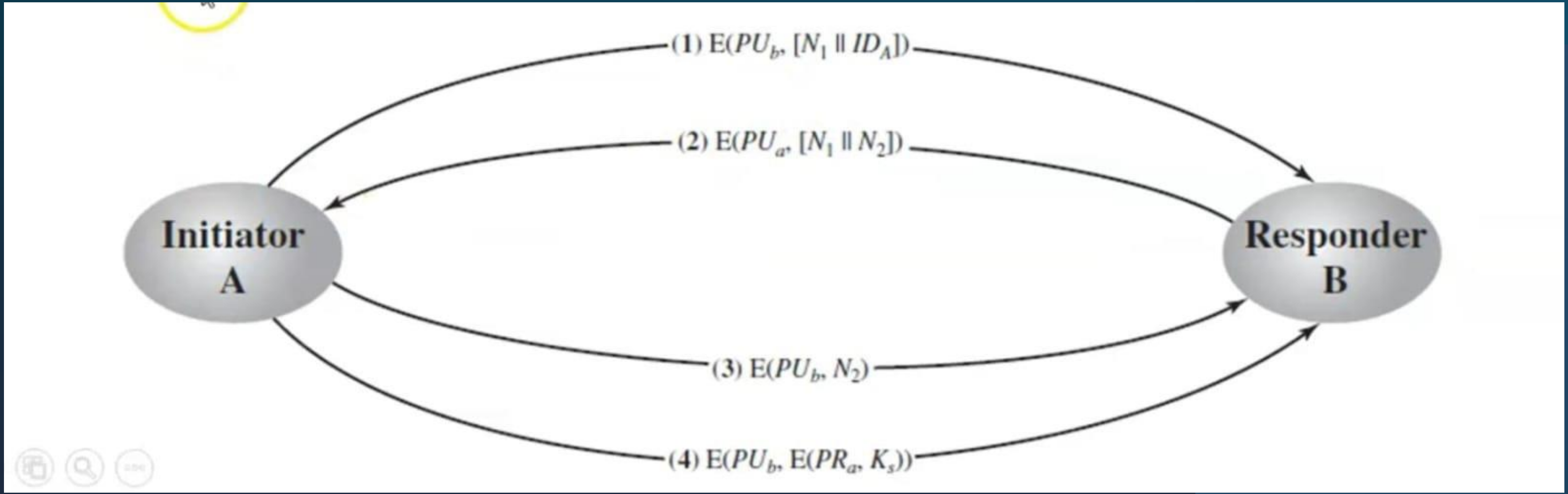

(1) $PU_a \| ID_A$
A
B
(2) $E(PU_a, K_s)$

MAN IN THE MIDDLE ATTACK



Secret key Distribution with Confidentiality and Authentication

- A uses B's public key to encrypt a message to B containing an identifier of A(IDa) and a nonce (N_1), which is used to identify this transaction uniquely. {E(PUb,[N1 || IDa])}
- B sends a message to A encrypted with PUa, and containing A's nonce (N1) as well as a new nonce generated by B (N2). Because only B could have decrypted message (1), the presence of N1; in message (2) assures A that the correspondent is B. {E(PUa,[N1 || N2])}
- A returns N2, encrypted using B's public key, to assure B that its correspondent is A.{E(Pub,N2)}
- A selects a secret key K, and sends M=E(PUb E(PRa, Ks)) to B. Encryption of this message with B's public key ensures that only B can read it; encryption with A's private key ensures that only A could have sent it.{E(Pub,E(PRa,Ks))}
- B computes D(PU, D(PR, M)) to recover the secret key,



(1) $E(PU_b, [N_1 \| ID_A])$
(2) $E(PU_a, [N_1 \| N_2])$
Initiator
A
Responder
B
(3) $E(PU_b, N_2)$
(4) $E(PU_b, E(PR_a, K_s))$

THANK YOU