CRYPTOGRAPHY AND INFORMATION SECURITY

IT 3203

LECTURE 23

By

Varsha Himthani

Assistant Professor (Selection Grade)

Manipal University Jaipur

Why Key Management And Distribution?

Why Key Management And Distribution?

- ★ Secure encrypted data transmission is needed.
- ★ There is a need for secure key distribution.
- ★ Two keys - Master key and session key.
- ★ Public key certificates and X.509 certificates.
- ★ We need the Public Key Infrastructure (PKI).
- ★ PKI implementations make use of X.509 certificates.

Key Management and Distribution

- ★ Symmetric key distribution using symmetric encryption.
- ★ Symmetric key distribution using asymmetric encryption.

Symmetric Key Distribution with Symmetric Encryption

- ★ Two communicating parties must share the same key.
- ★ Key must be protected from access by others.
- ★ Frequent key changes are desirable.
- ★ Key distribution technique is equally important.
- ★ Various ways a key can be distributed among two parties.

Various Ways of Key Distribution

1. A can select a key and physically deliver it to B.
2. Third party can select the key and deliver it to A and B physically.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If A and B each has an encrypted connection to a third party C, then C can deliver a key on the encrypted links to A and B.

Drawbacks

- ★ In a distributed system, any given host or terminal may need to engage in exchanges with many other hosts and terminals over time.
- ★ Each node needs a number of keys supplied dynamically.
- ★ The problem is especially difficult in a wide-area distributed system.
- ★ The scale of the problem depends on the number of communicating pairs that must be supported.

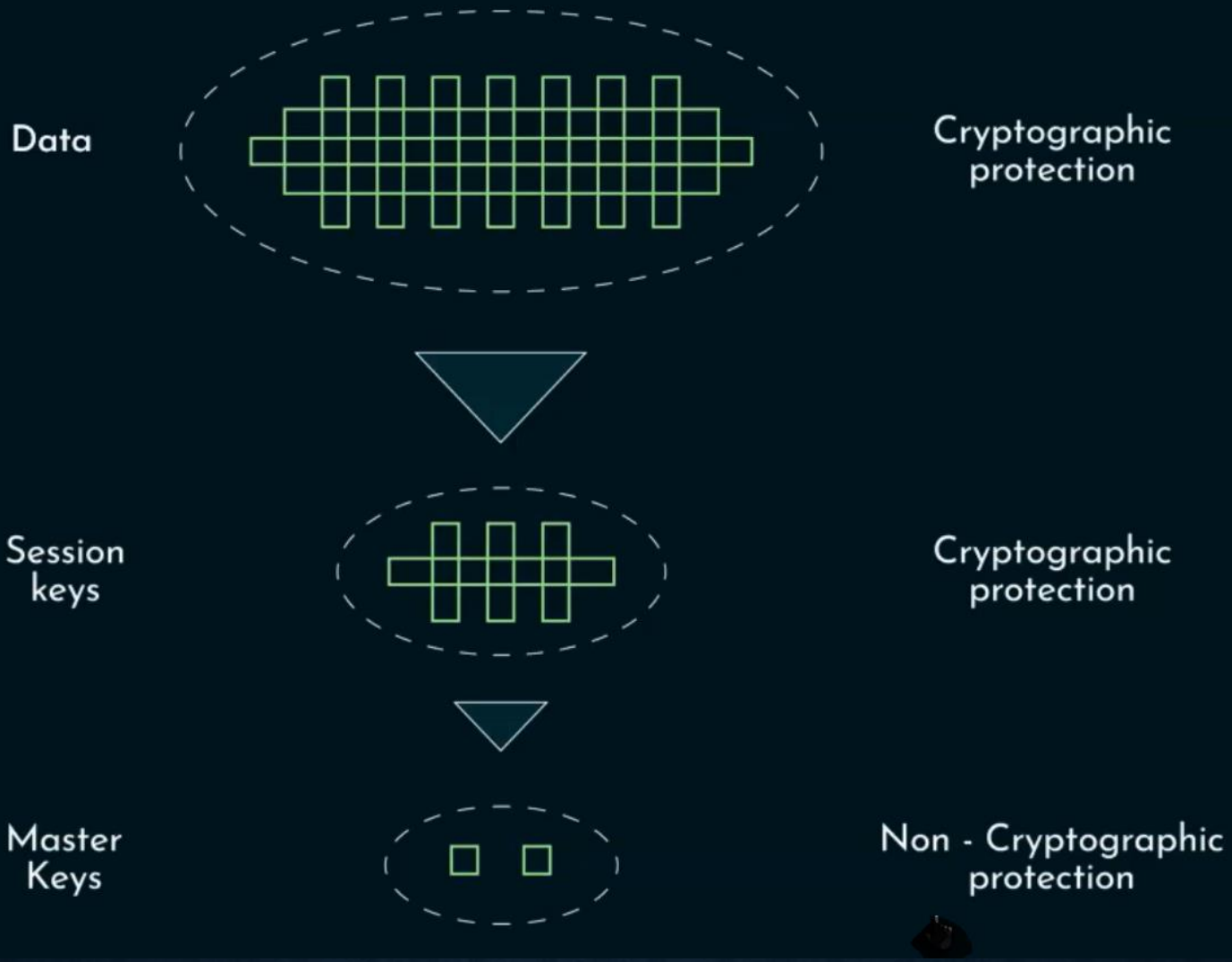
Question: How many number of keys are required, if there are 'N' hosts in symmetric approach?

Answer: [N x (N-1) / 2]

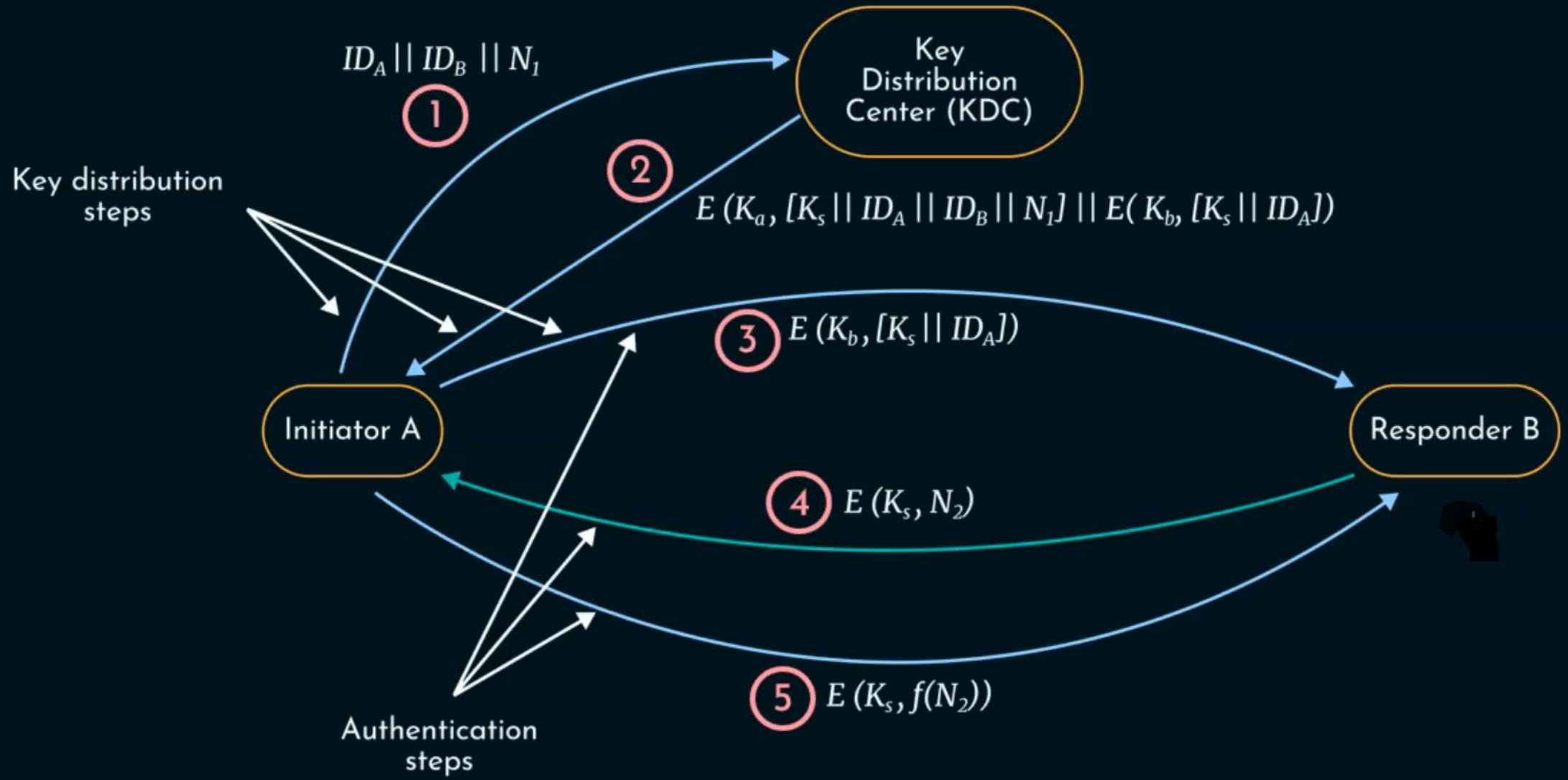
★ A network using node-level encryption with 1000 nodes would conceivably need to distribute as many as half a million keys.

★ If that same network supported 10,000 applications, then as many as 50 million keys may be required for application-level encryption.

The use of key hierarchy

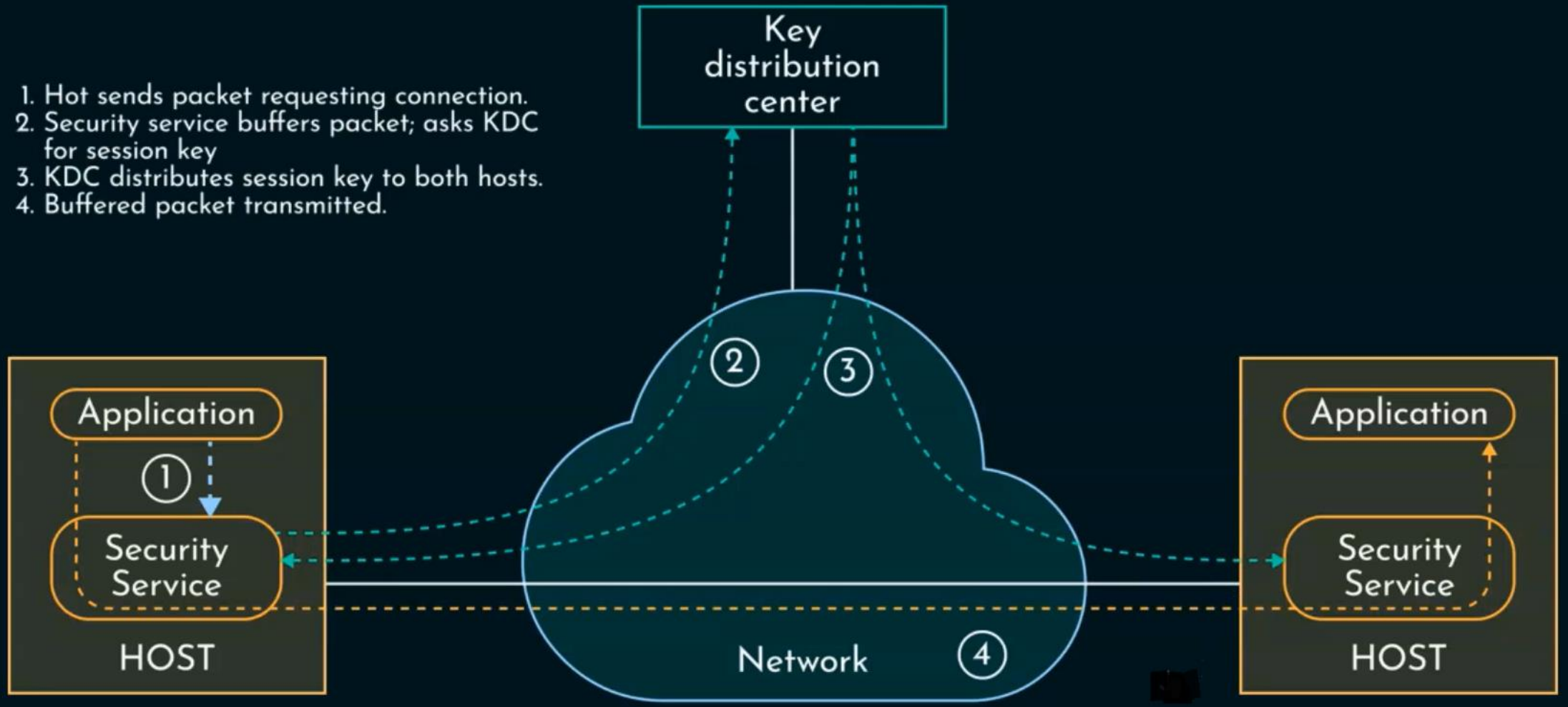


A Key Distribution Scenario

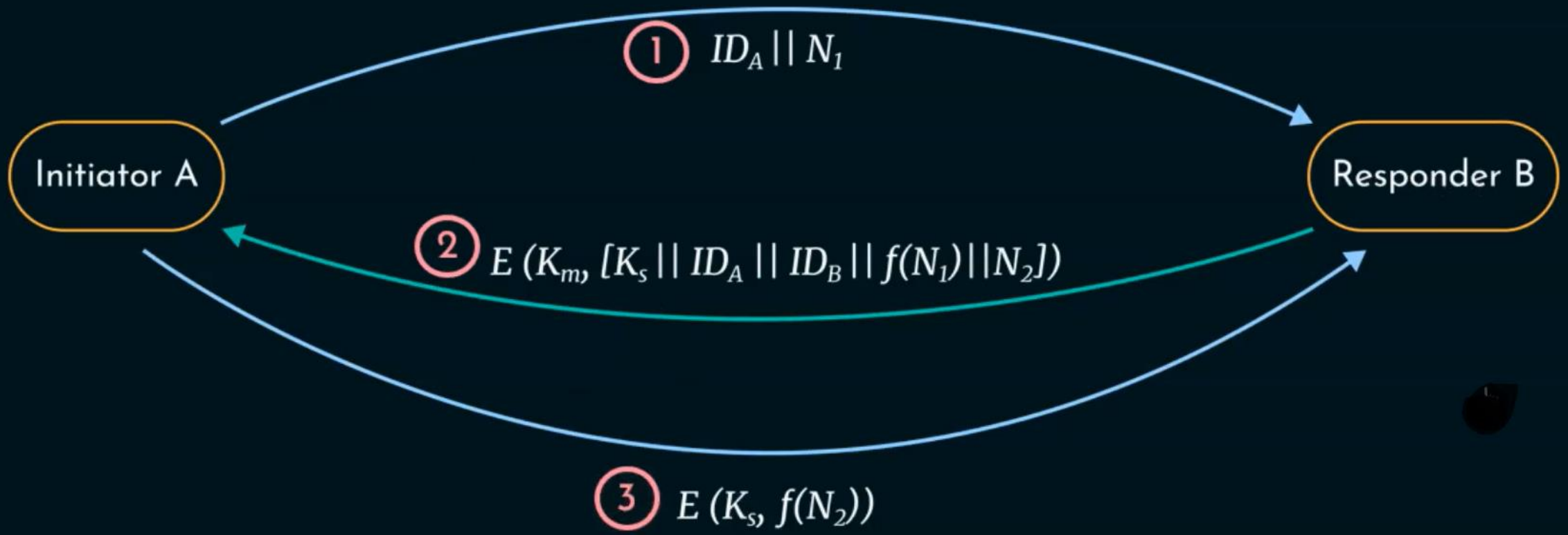


Automatic Key Distribution For Connection Oriented Protocol

1. Hot sends packet requesting connection.
2. Security service buffers packet; asks KDC for session key
3. KDC distributes session key to both hosts.
4. Buffered packet transmitted.



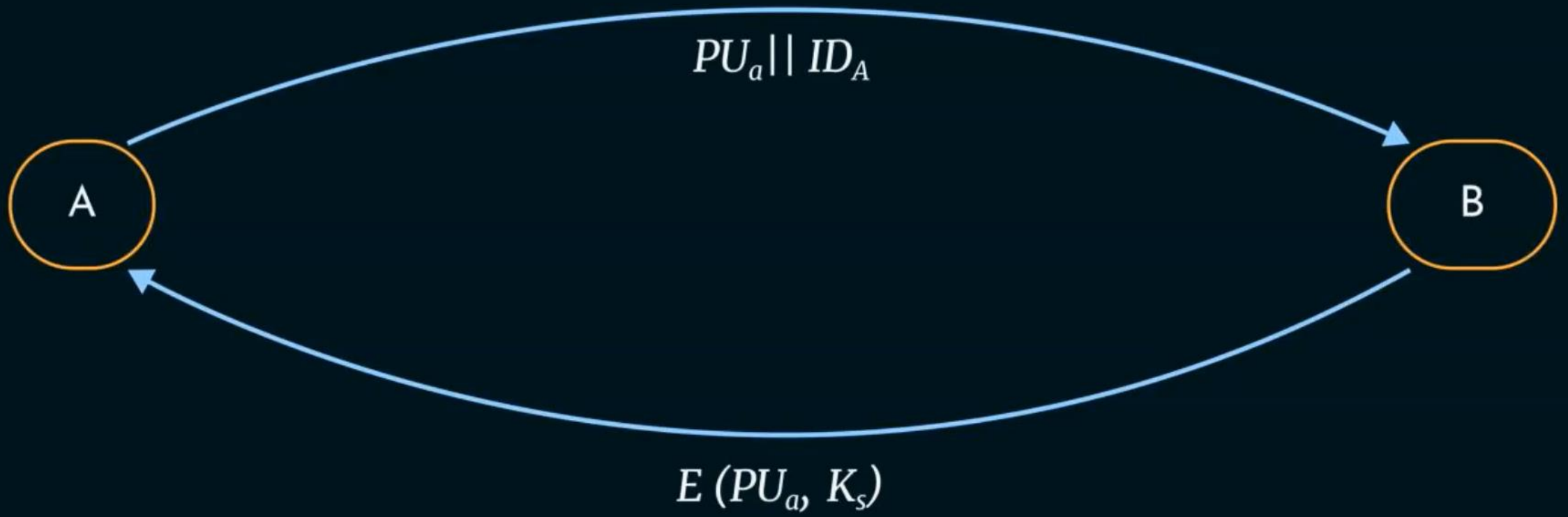
Decentralized Key Control



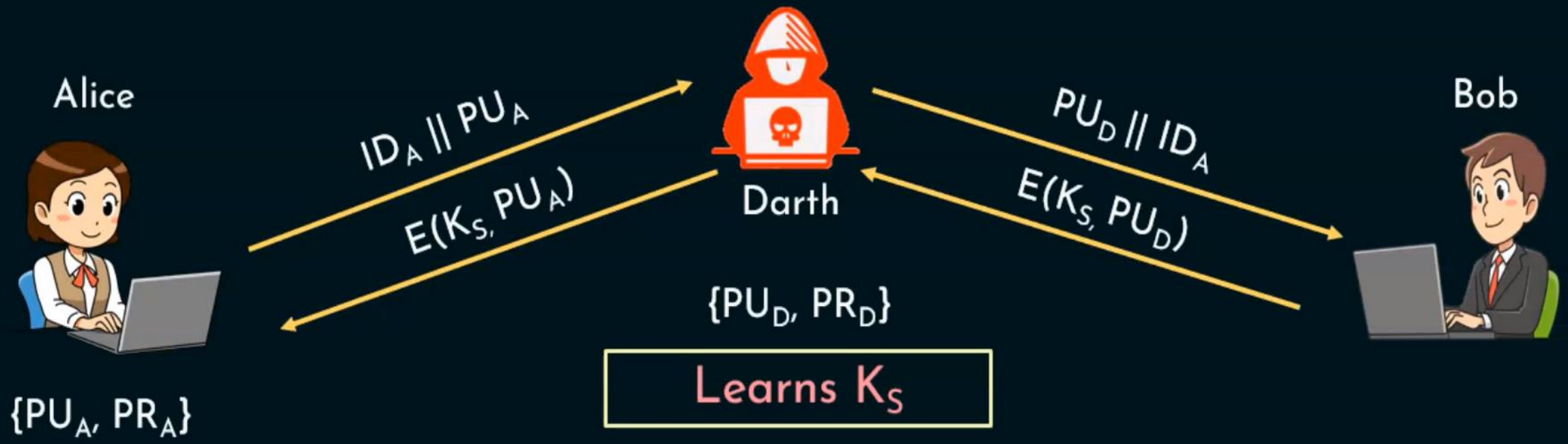
Symmetric Key Distribution with Asymmetric Encryption

- ★ Using public-key cryptosystem, we can encrypt secret keys for distribution.
- ★ It is a simple protocol.
- ★ No keys exists before the start of the communication and none exist after the completion of the communication.
- ★ Communication is secure from eavesdropping but insecure against man-in-the-middle attack.

Simple Use of Public-Key Encryption to Establish a Session Key



Man-in-the-middle attack



Secret Key Distribution with Confidentiality and Authentication

Thank you