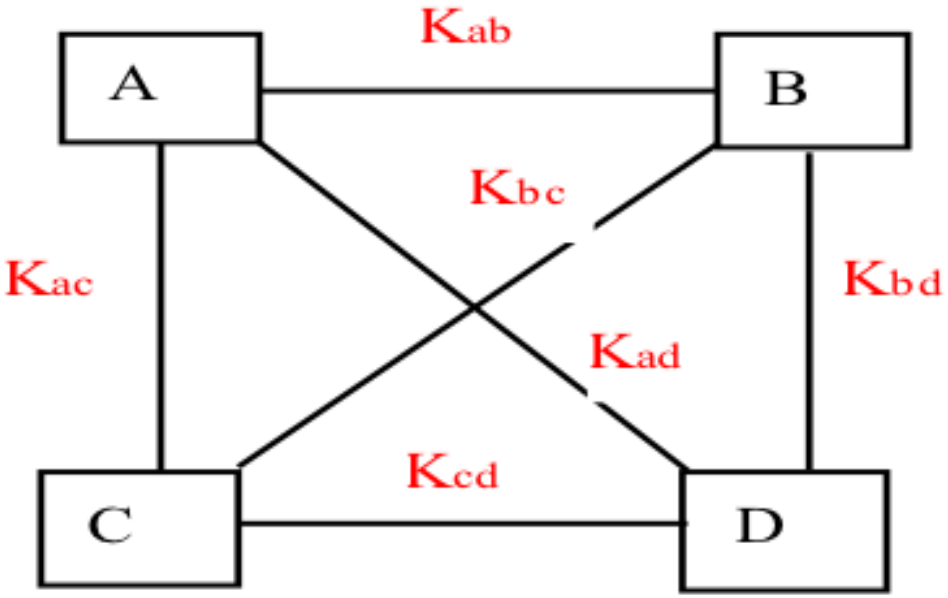
Symmetric Key Distribution without using PKC

- Symmetric key distribution using symmetric key encryption - Needham-Schroeder Protocol.
- This protocol is widely used in single sign on (SSO) solutions, e.g. window domain authentication, Kerberos.

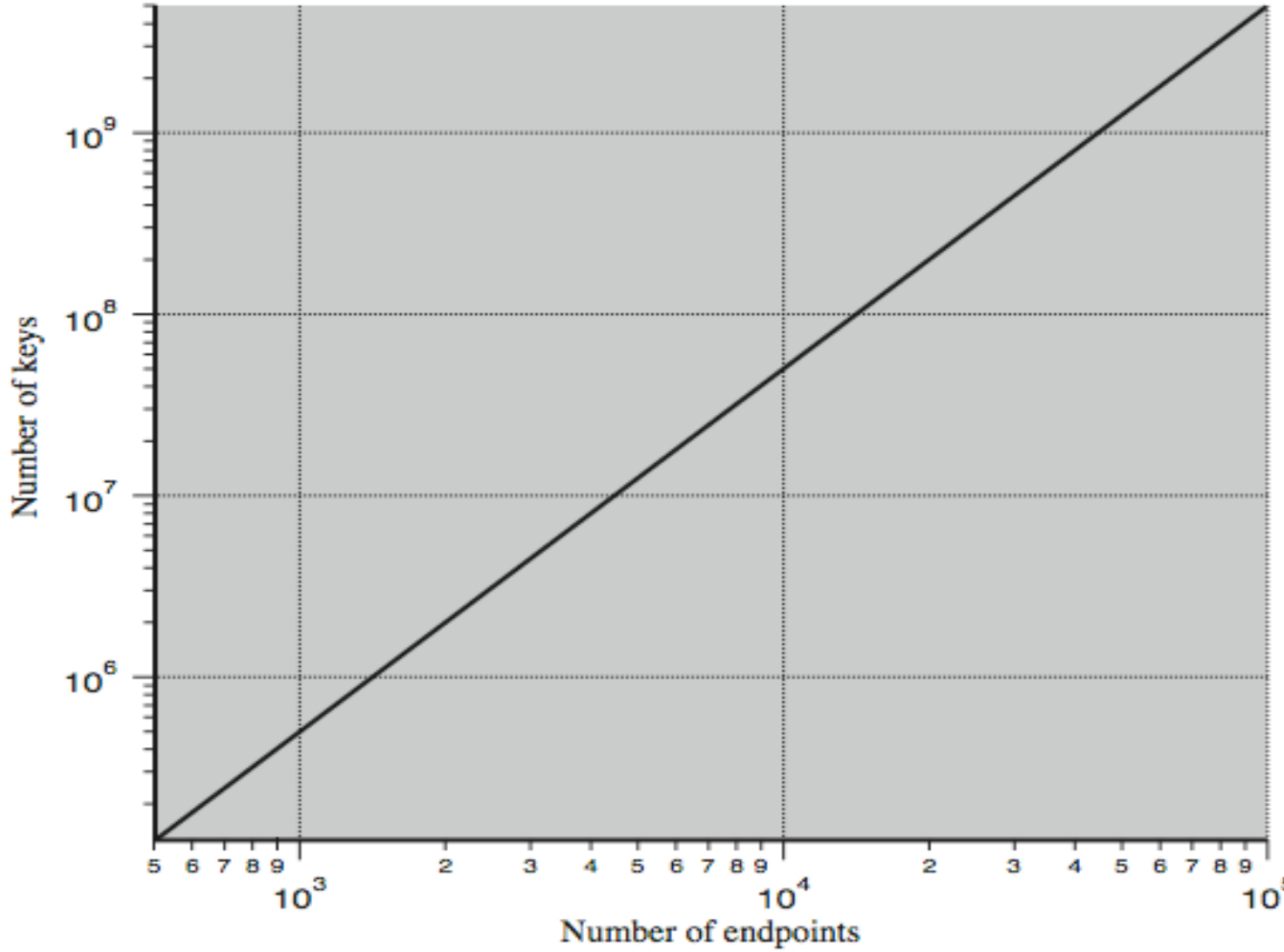
Distribution without using PKC – Approach-One

- *Approach One*: Given *n* users (parties/nodes) to communicate with each other, the system needs $n(n-1)/2$ keys.
- As *n* increases, the number of keys becomes untenable for everyone.
- The n^2 problem!



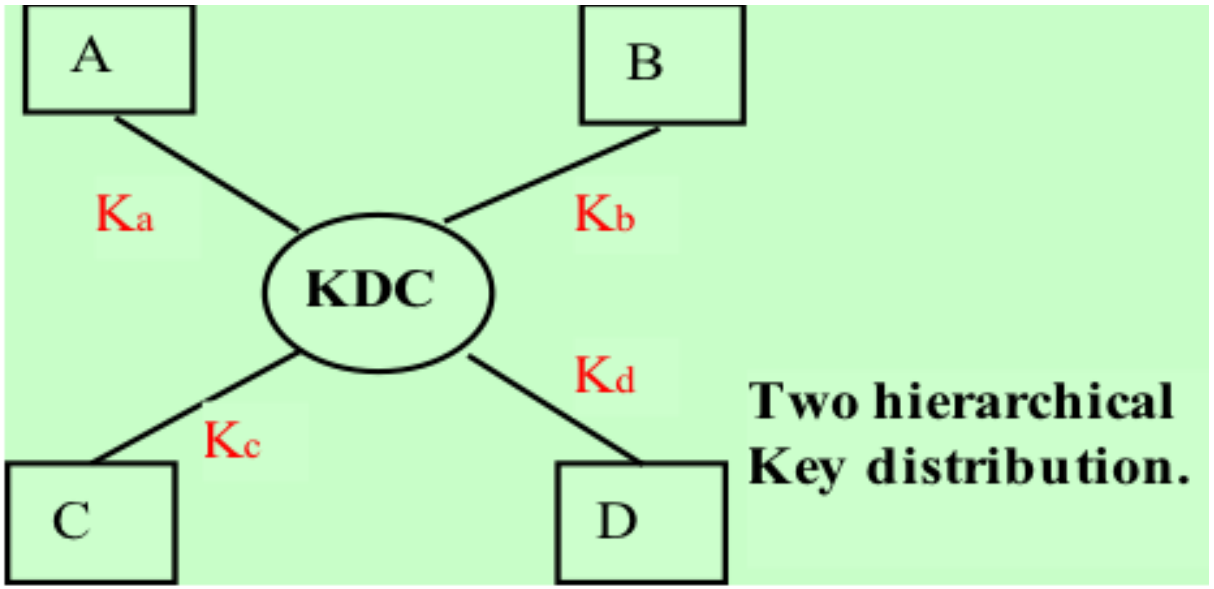
One hierarchical Key distribution.

Distribution without using PKC - Scalability problem



Distribution without using PKC – Approach-Two

- *Approach Two:* use a key distribution centre (*KDC*) or security server.
  - A key hierarchy, e.g. two hierarchical approach - *master keys* (*long-term keys*) and *session keys* (*valid just for one session*).



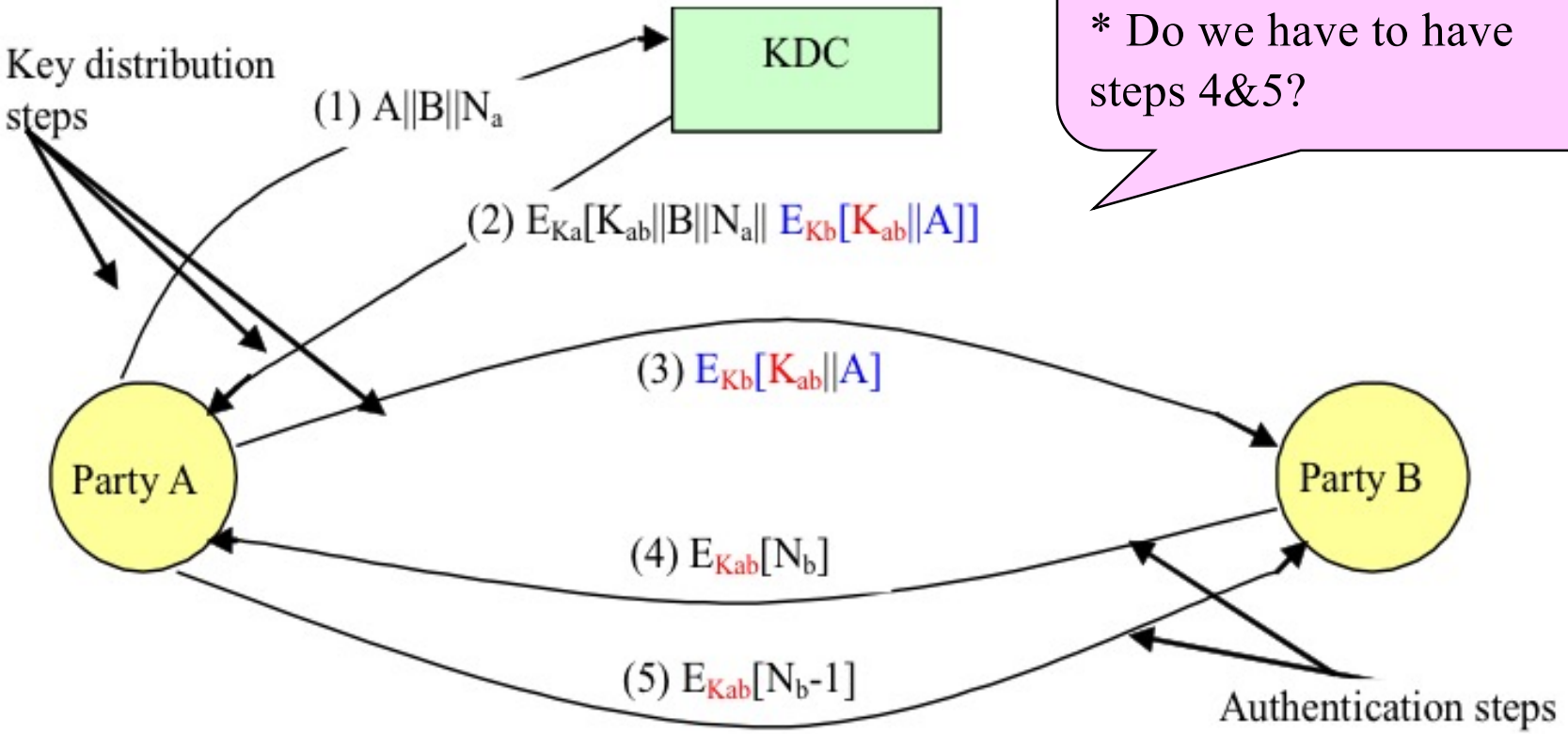
Distribution without using PKC – Approach-Two

- A unique master key, shared between a pair of user/*KDC*, is for session key distribution.
- A session key is to secure a particular session.
- Benefit of using Approach Two
  - Reduces the scale of the problem - reduces the n^2 problem to an n problem, thus making the system more scalable.
- But:
  - The need to trust the intermediaries - KDC.
    - KDC has enough information to impersonate anyone to anyone. If it is compromised, all the resources in the system are vulnerable.
  - KDC is a single point of failure.
  - KDC may be a performance bottleneck.

Distribution without using PKC - Needham-Schroeder Protocol

- The Needham-Schroeder is a key distribution protocol.
- It uses Approach-Two. That is:
  - both parties, *A* and *B*, shares a secret key with the KDC, K_a and K_b ;
  - *A* and *B* wishes to establish a secure communication channel, i.e. establish a shared one-time session key K_{ab}, for use between *A* and *B* in this session.
- N_a, N_b are nonces (random challenges), generated by *A* and *B* respectively, to keep messages fresh.

Distribution without using PKC - Needham-Schroeder Protocol



*Is the nested encryption in (2) necessary?
* Do we have to have steps 4&5?

Distribution without using PKC - Needham-Schroeder Protocol

(1) A sends a request to *KDC* for a session key to establish a secure channel with *B*.

(2) KDC generate a random number K_{ab}, and replies with the response containing

- session key K_{ab}.
- original request enables A matching the response with the request.
- an item (the session key and A's identity) which only *B* can view.

(3) A forwards the item to *B*.

At this point, the session key is securely delivered to A and B, and they may begin secure communication.

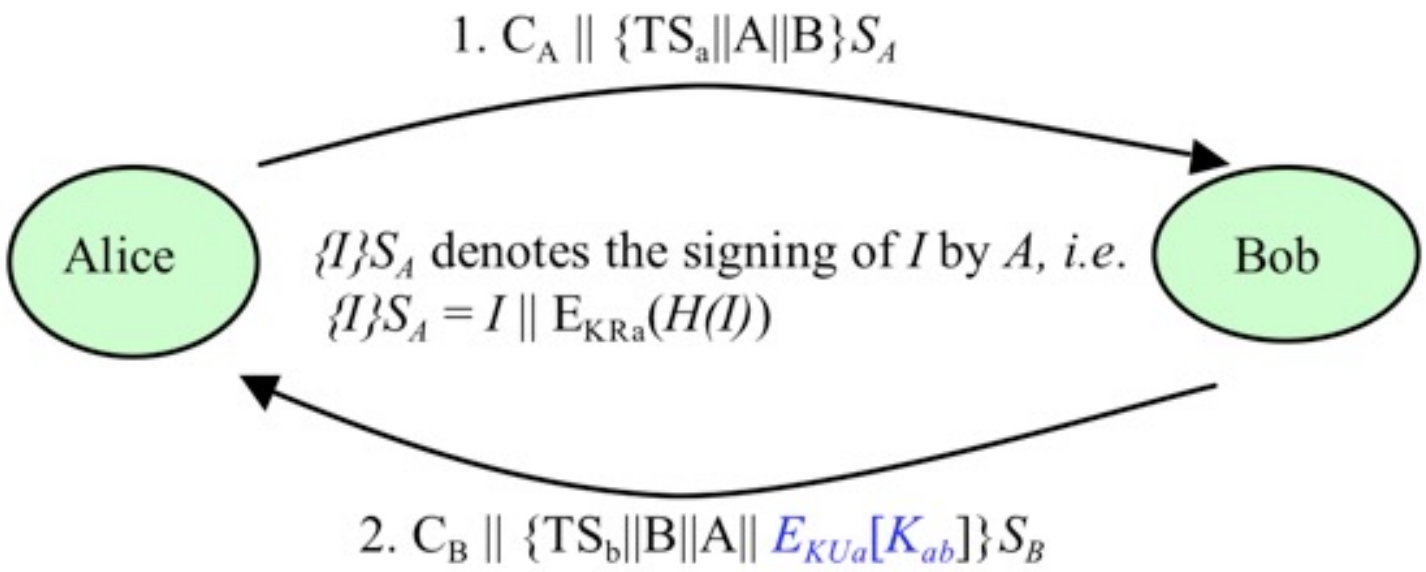
(4) B sends a nonce N_b to *A* encrypted using the new session key.

(5) A responds with N_b-1.

Steps (4) & (5) assure B that the message received in (3) was not a replay, i.e. to authenticate A.

Symmetric Key Distribution using PKC – Two passes

- Secret key distribution with mutual authentication using public key cipher + timestamps. C_A and C_B are, respectively, Alice's and Bob's certificates.



Symmetric Key Distribution using PKC - Three passes

- Symmetrical key distribution with mutual authentication using public key cipher + nonces (random numbers).
- In both of these two protocols, entity authentication is done by using digital signatures.