

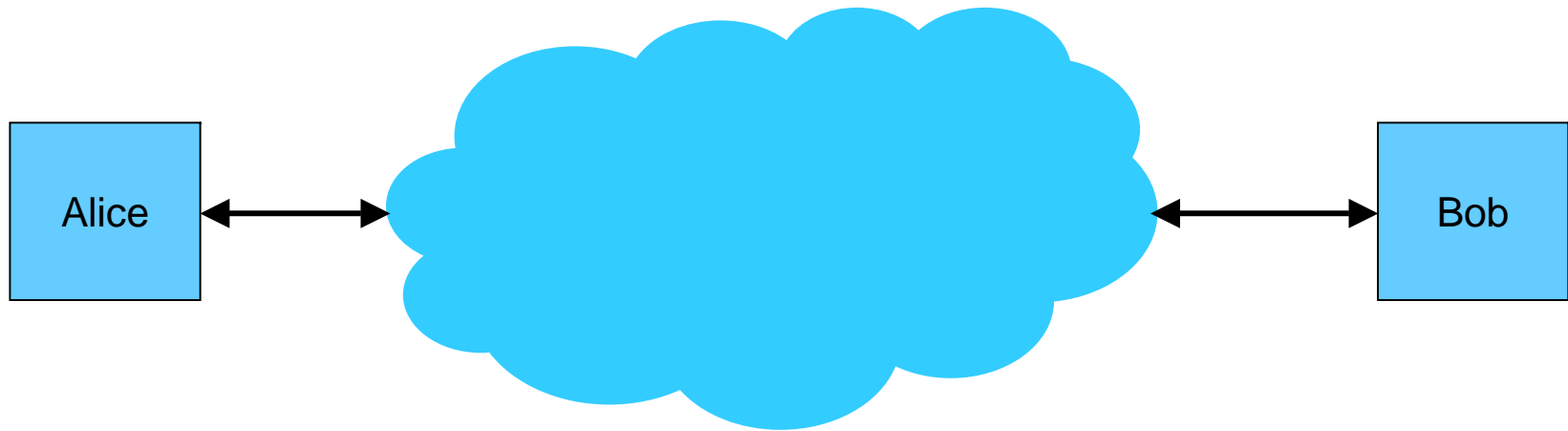
NIS/CpE 691A

Information System Security

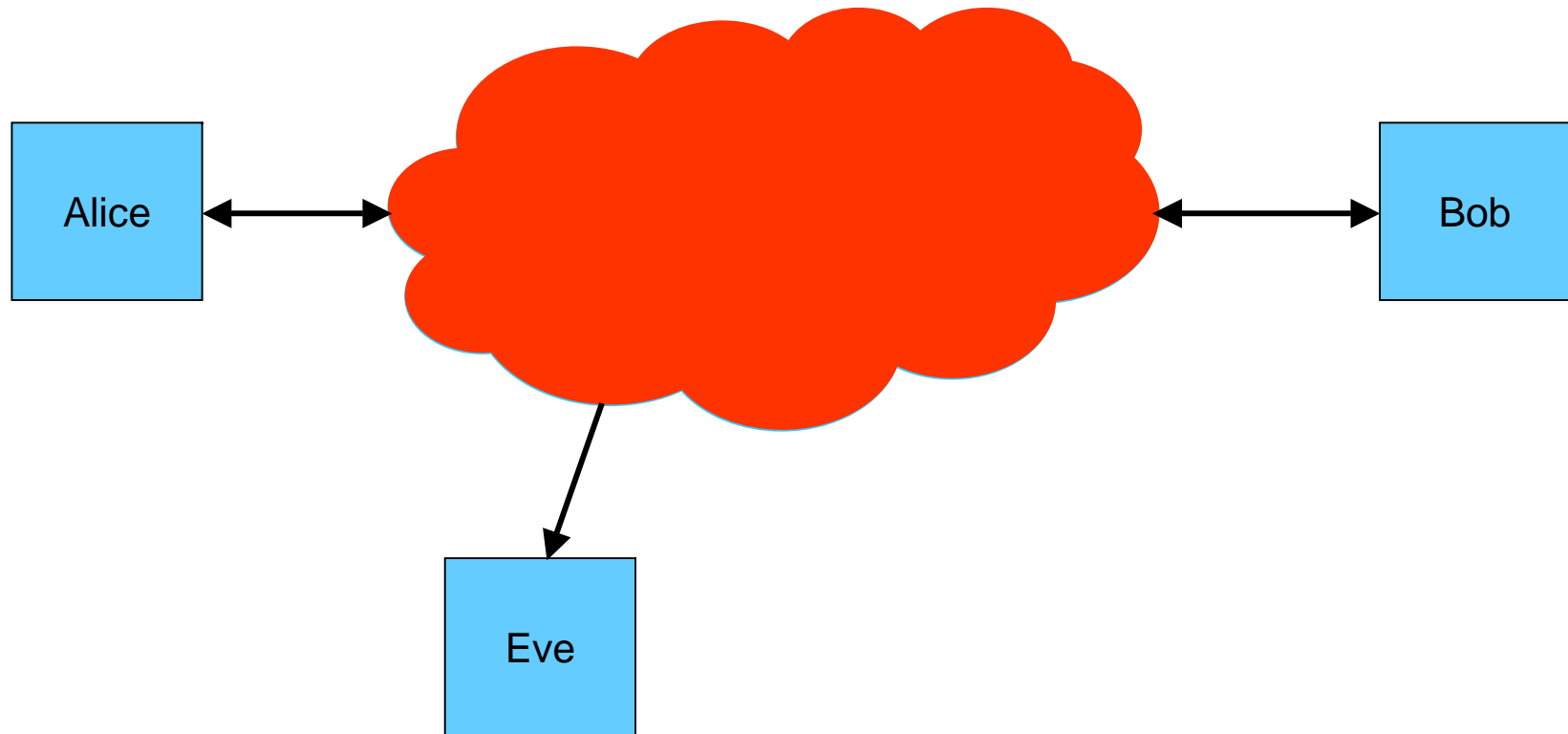
**Stevens Institute of Technology
Spring 2006**

Class 9 – 3/23/06

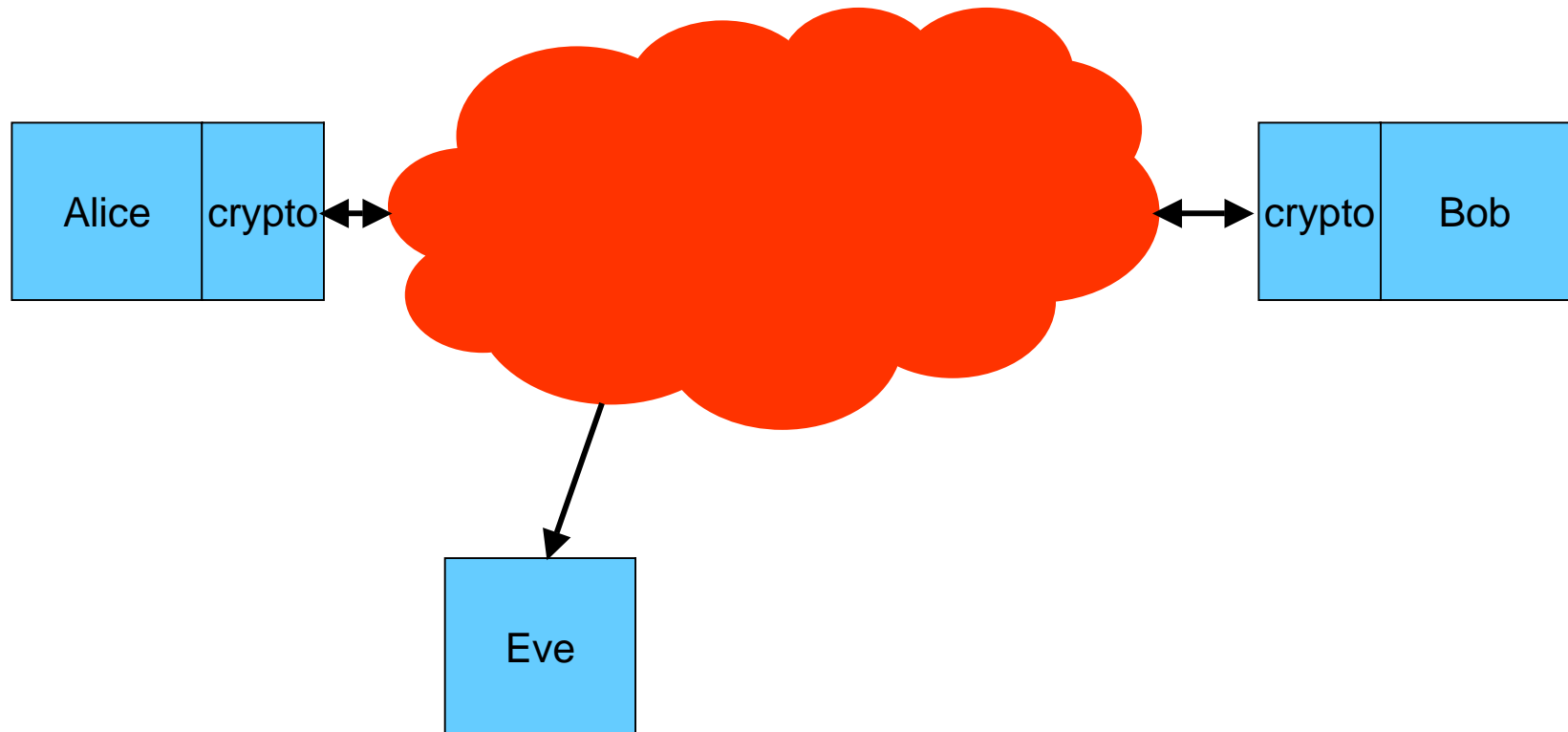
Idealized Networked Communicaitons



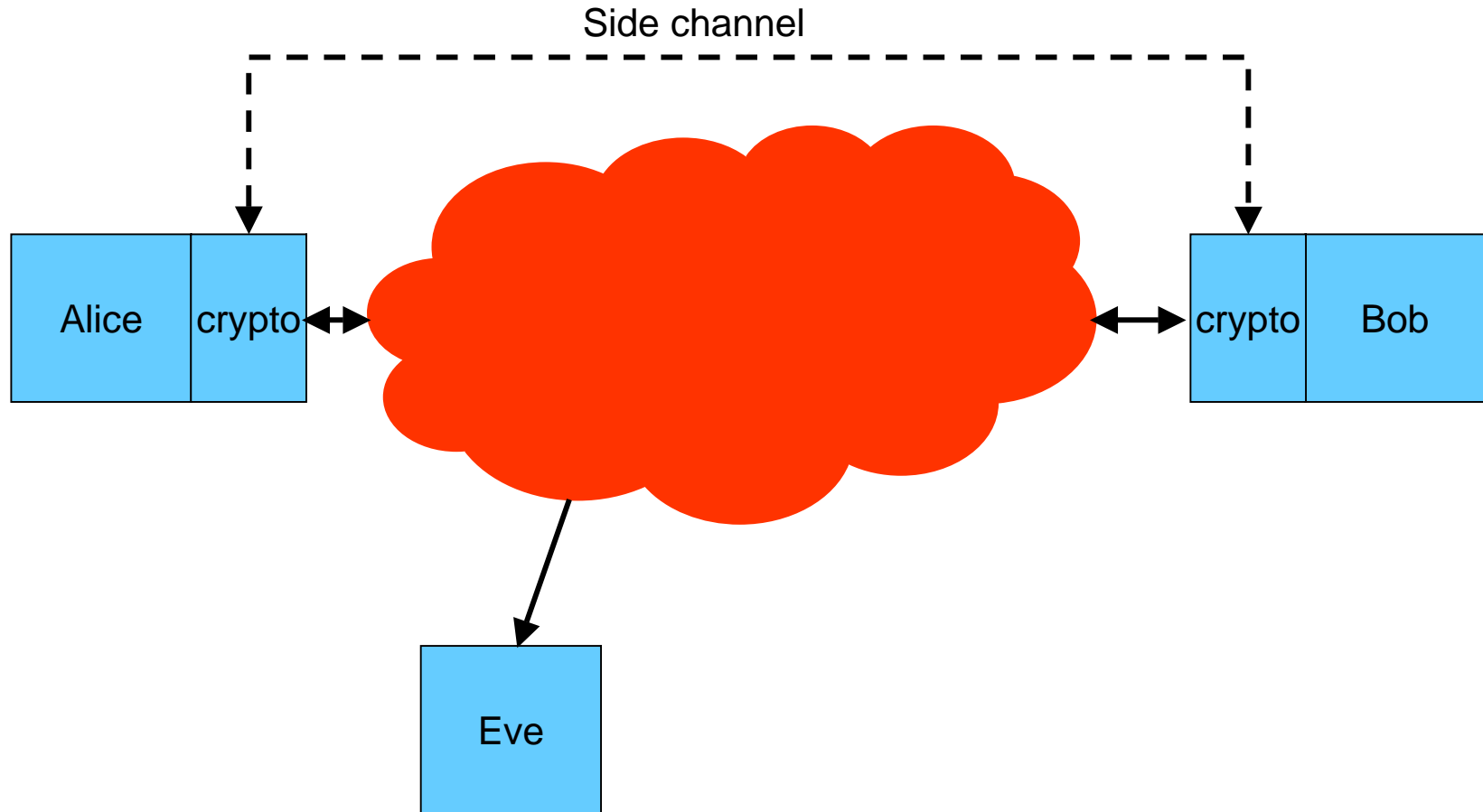
Realistic Networked Communications



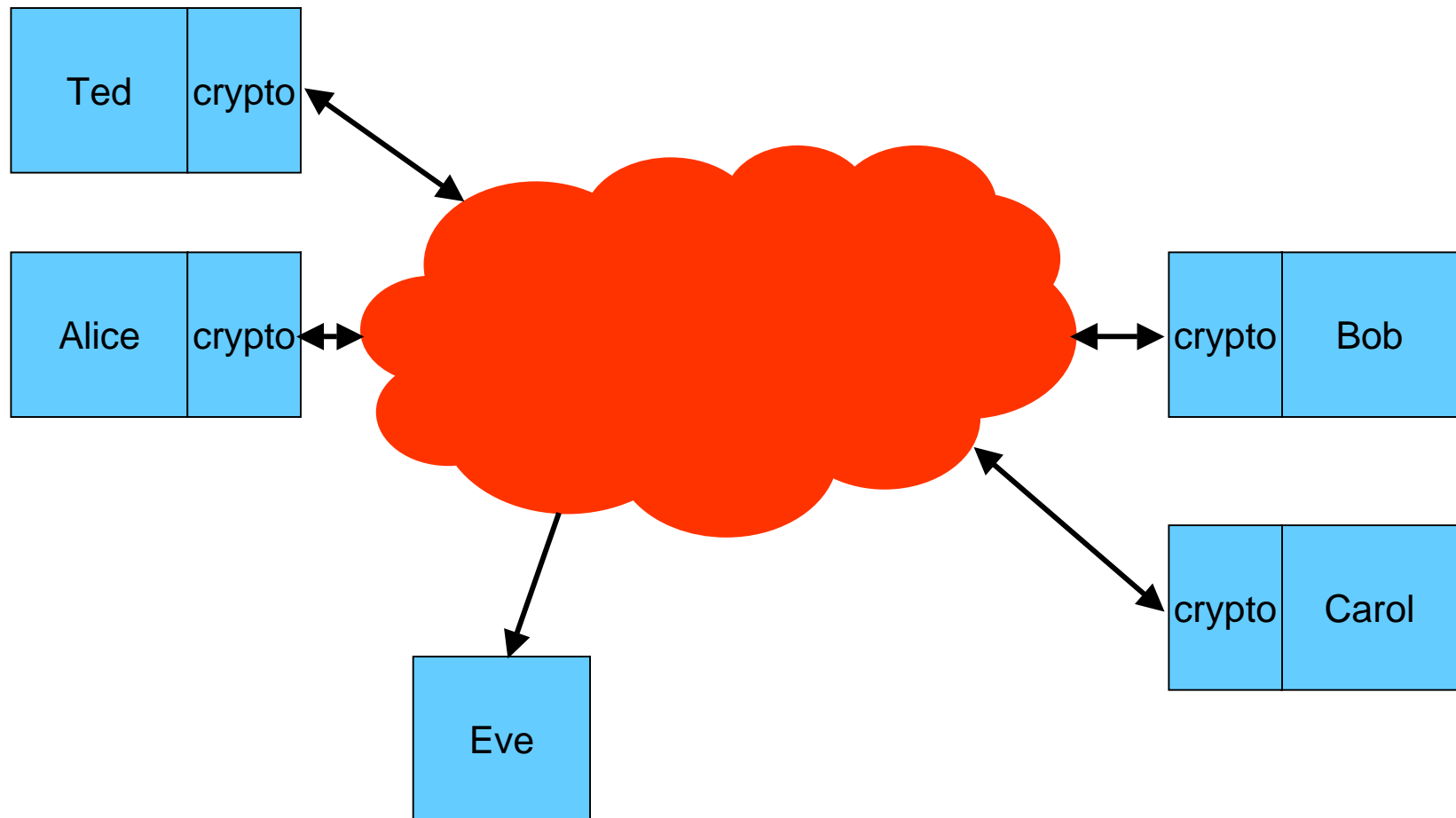
“Secure” Networking



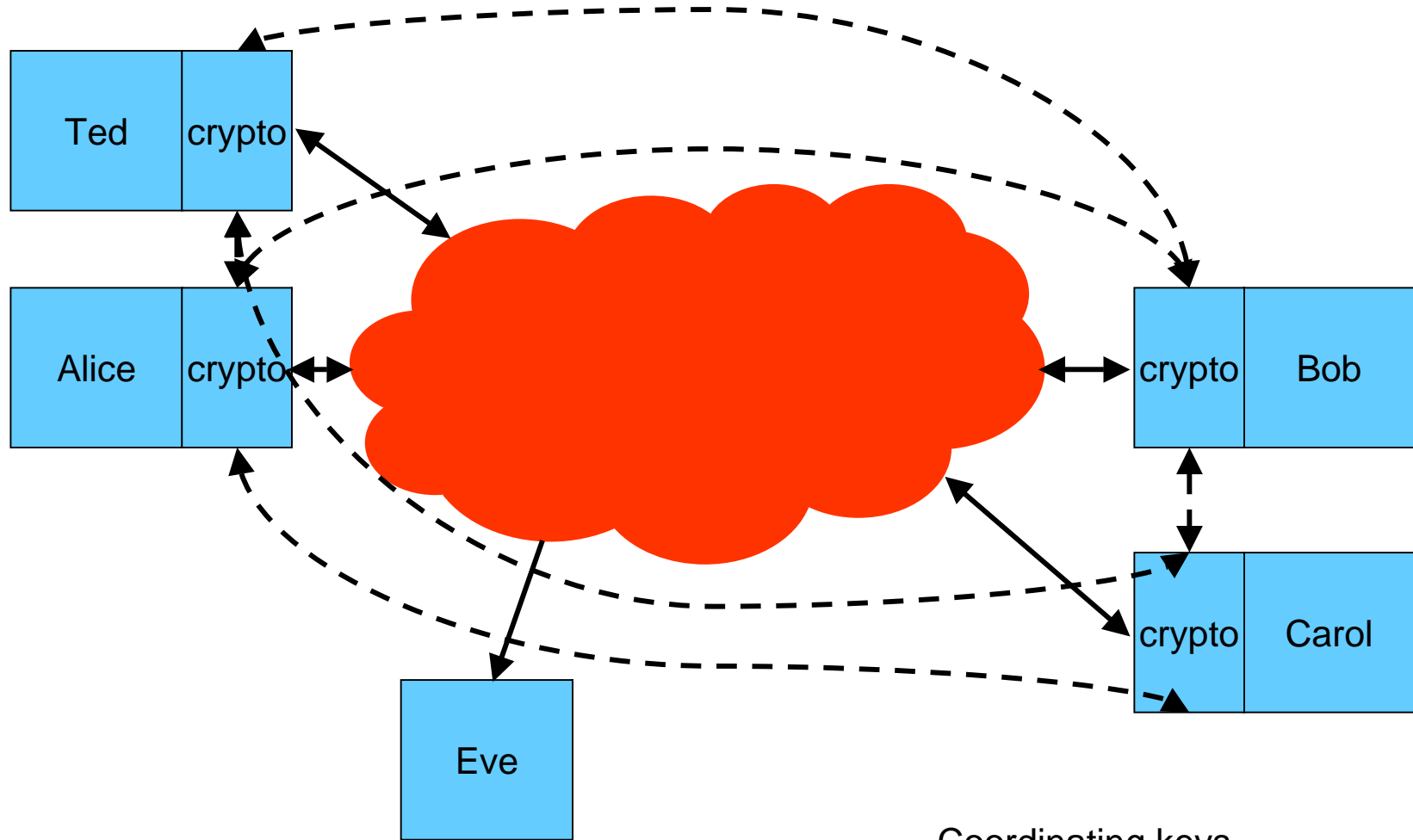
“Secure” Networking



Multistation "Secure" Networking



Multistation "Secure" Networking




Coordinating keys
becomes an N^2 problem

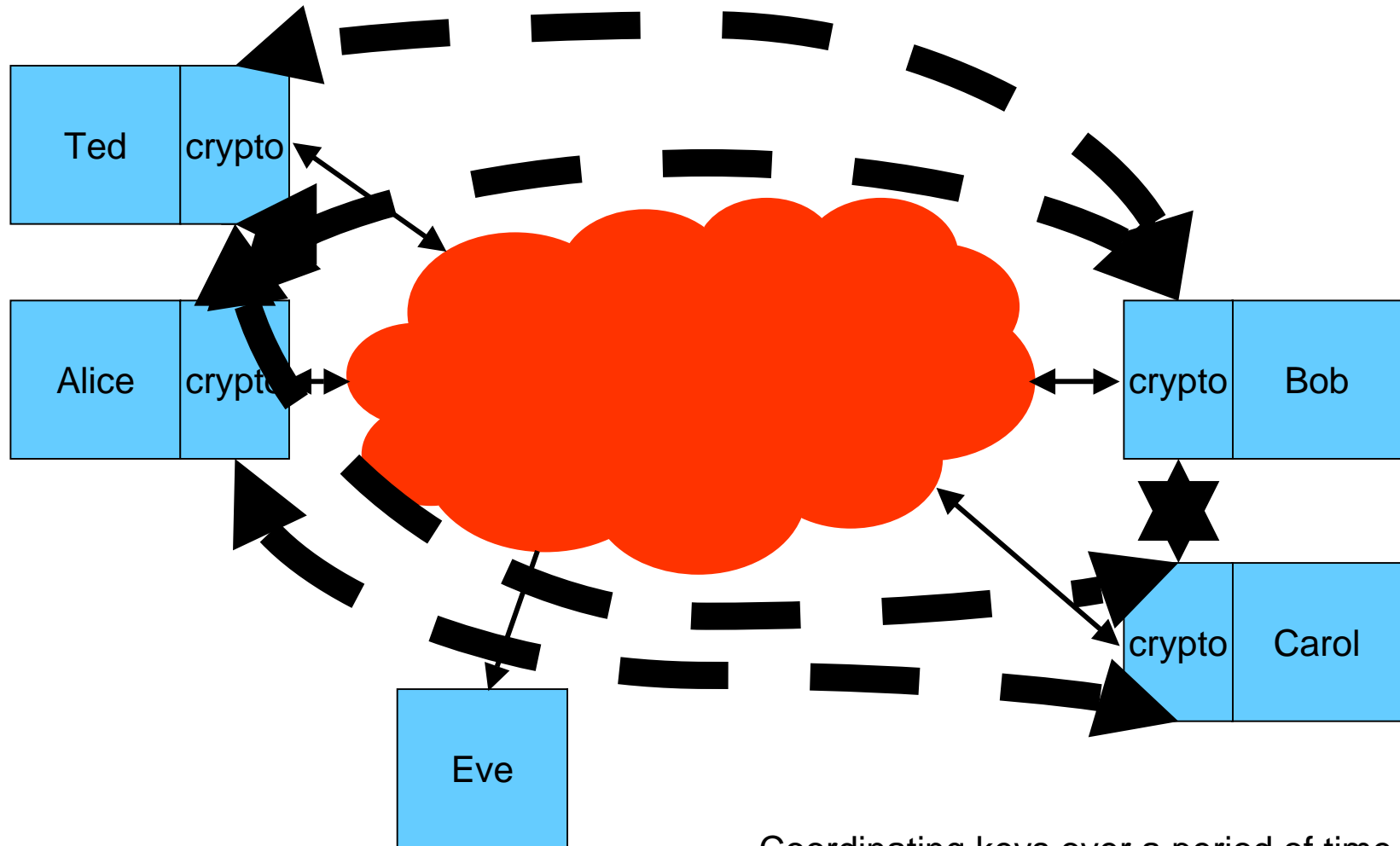
Realities of Encryption

- Keys “wear out”
- Previous keys remain valuable
- Secrets are sometimes compromised

Realities of Encryption

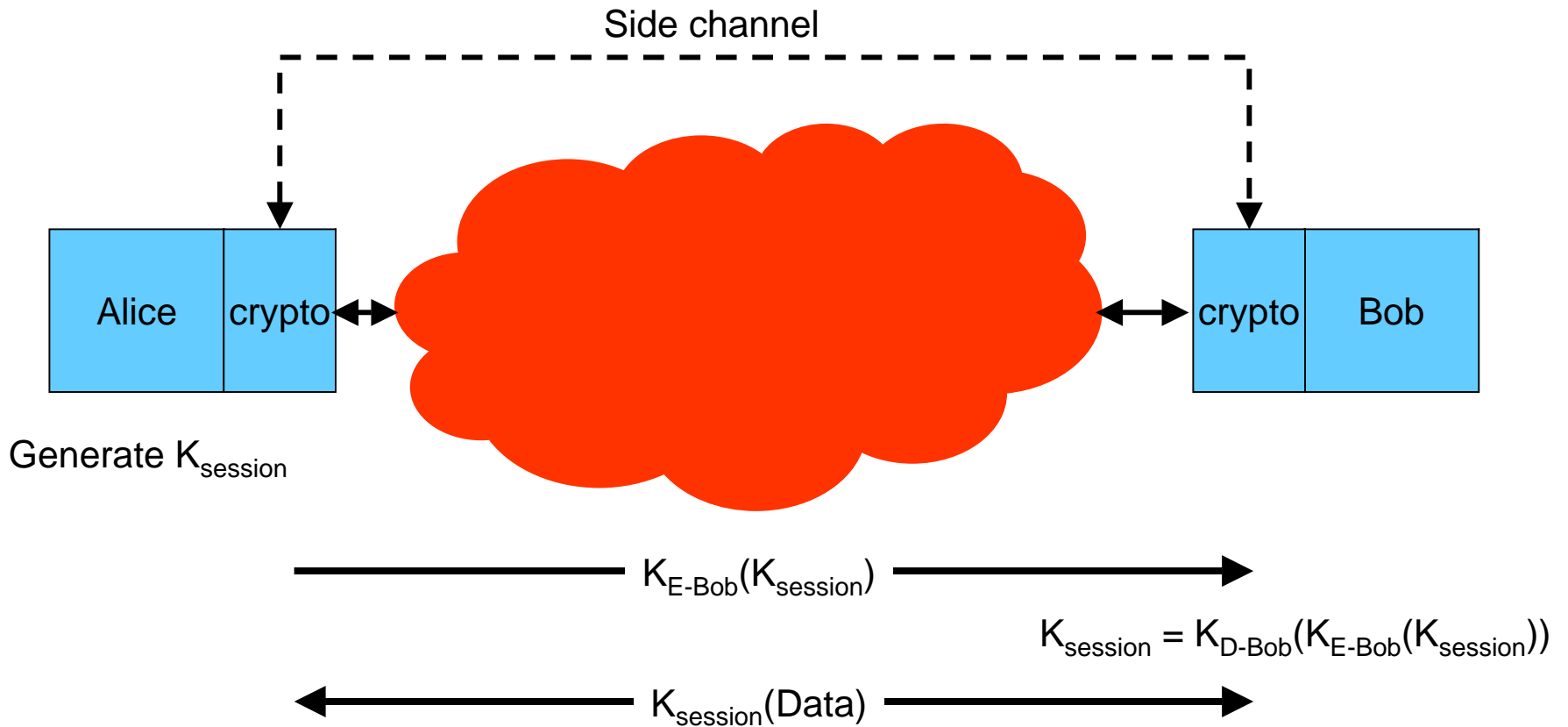
- Keys “wear out”
 - Previous keys remain valuable
 - Secrets are sometimes compromised
- 
- Encryption keys must be updated

Multistation "Secure" Networking

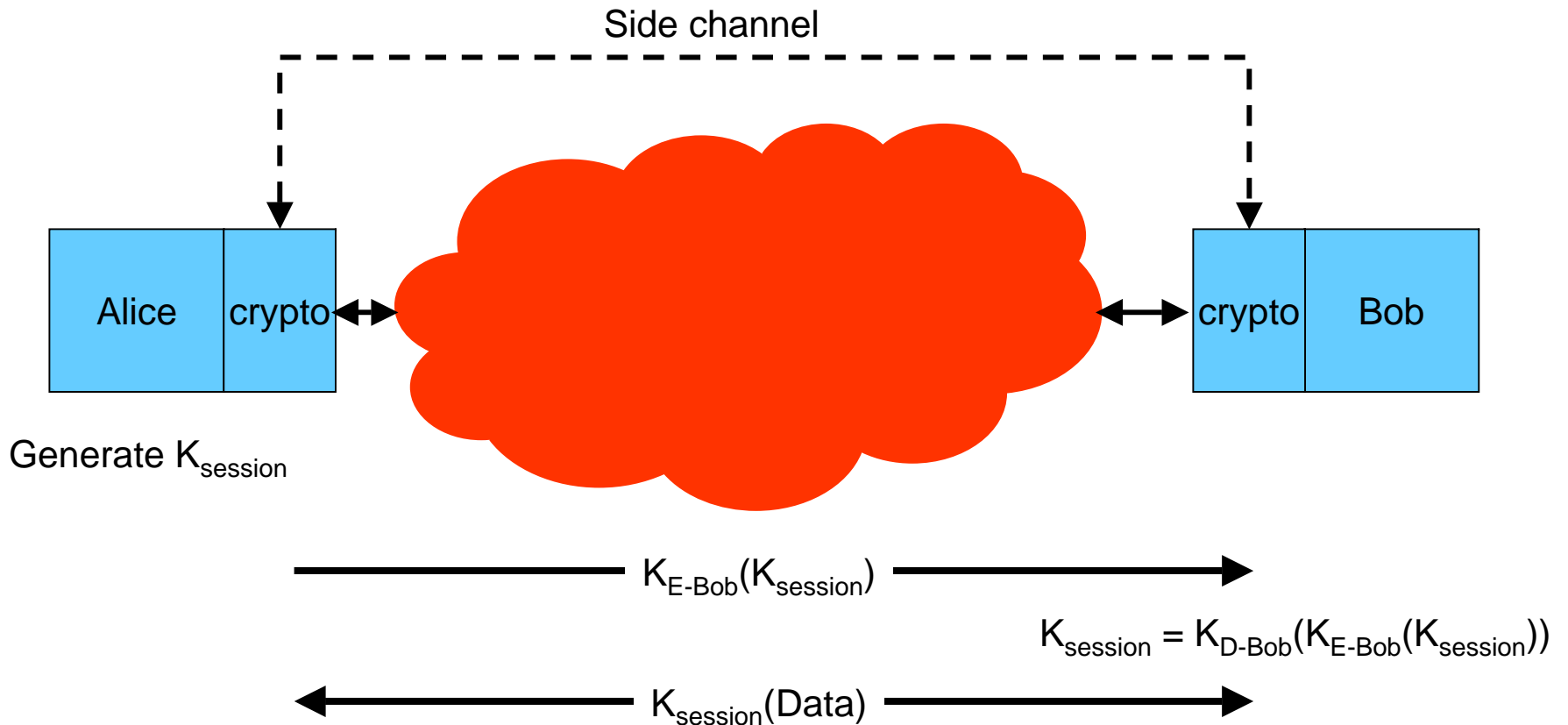


Coordinating keys over a period of time becomes an $(N^2)^T$ problem

Public-Key Cryptosystems to Simplify Key Management

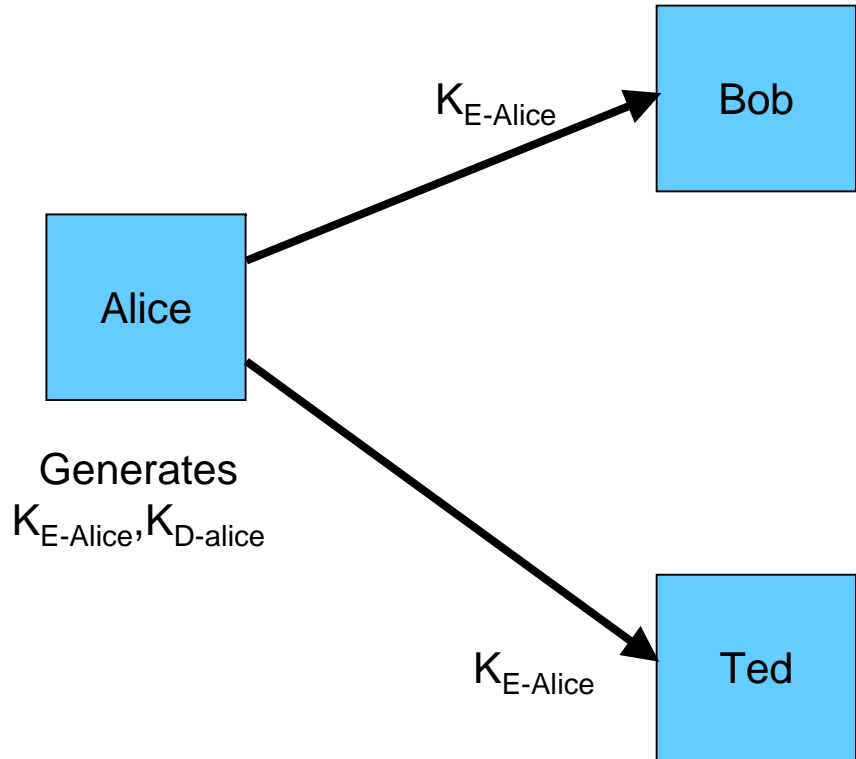


Public-Key Cryptosystems to Simplify Key Management

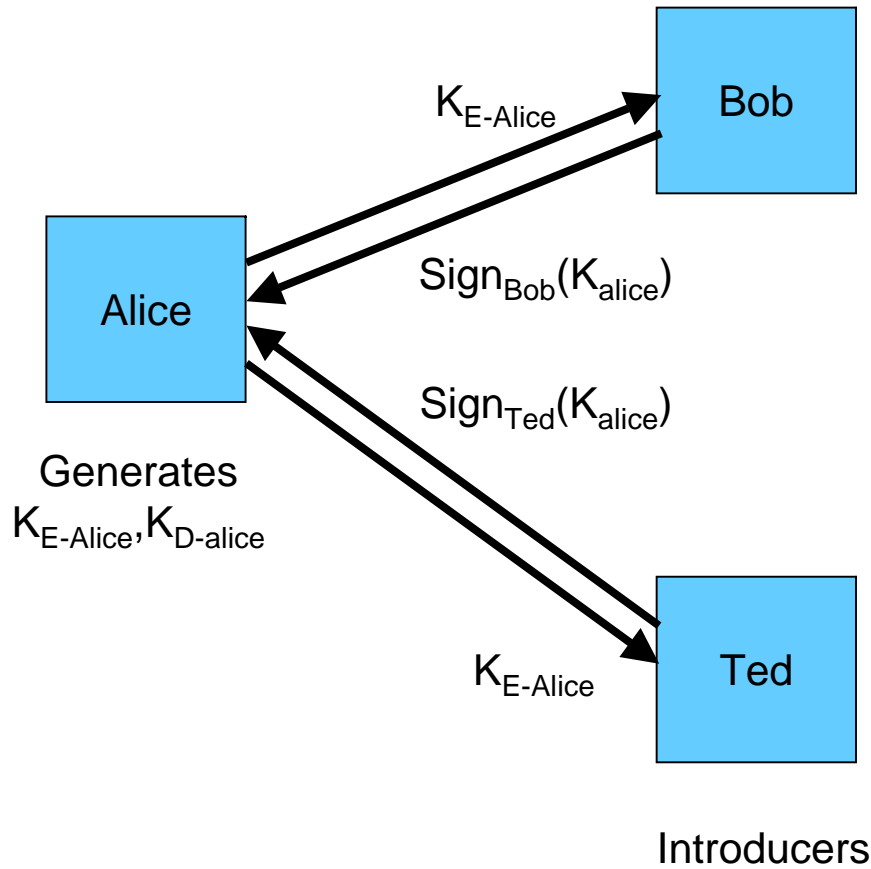


All stations must store copies of all K_E – updating is still a problem

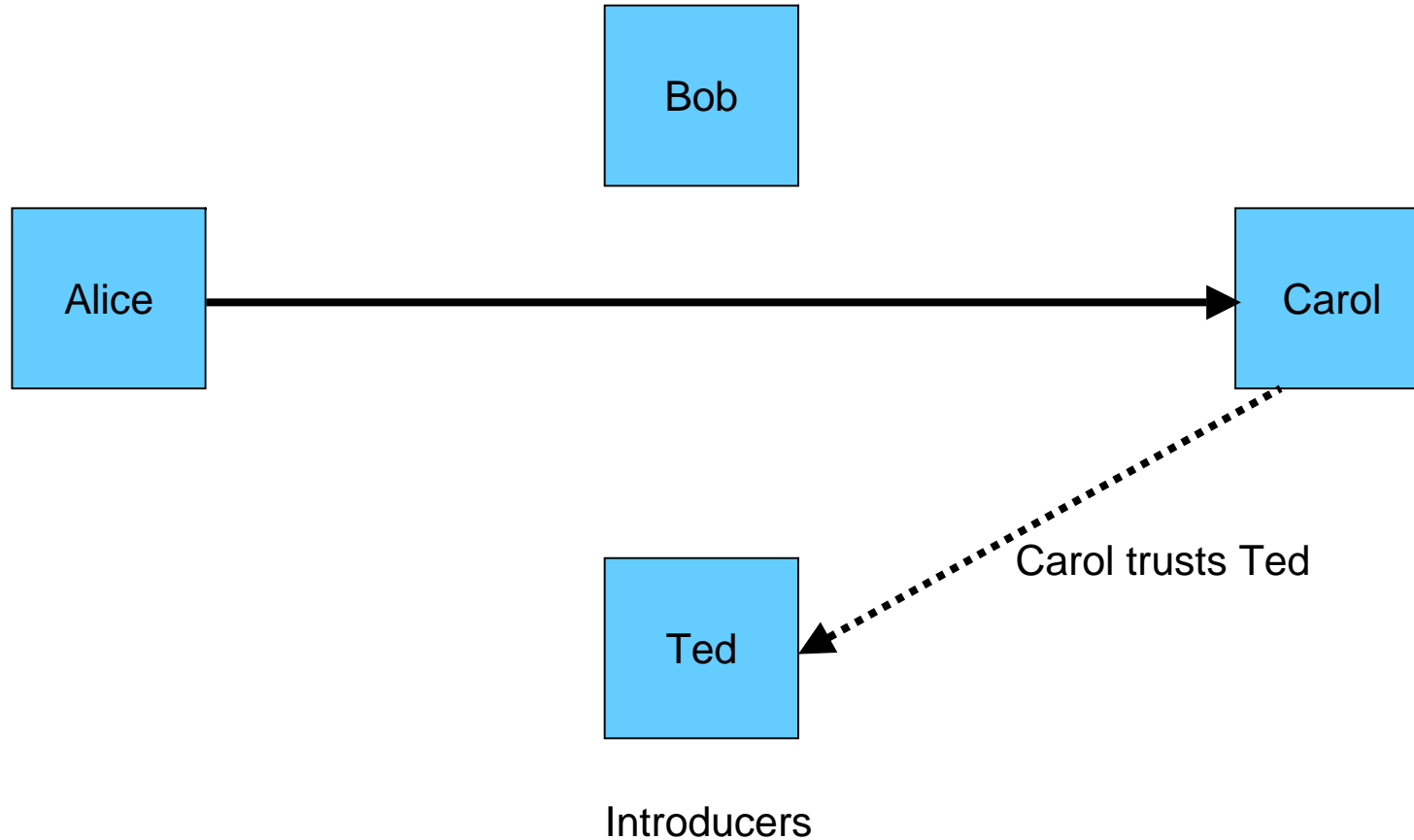
PGP for Key Management



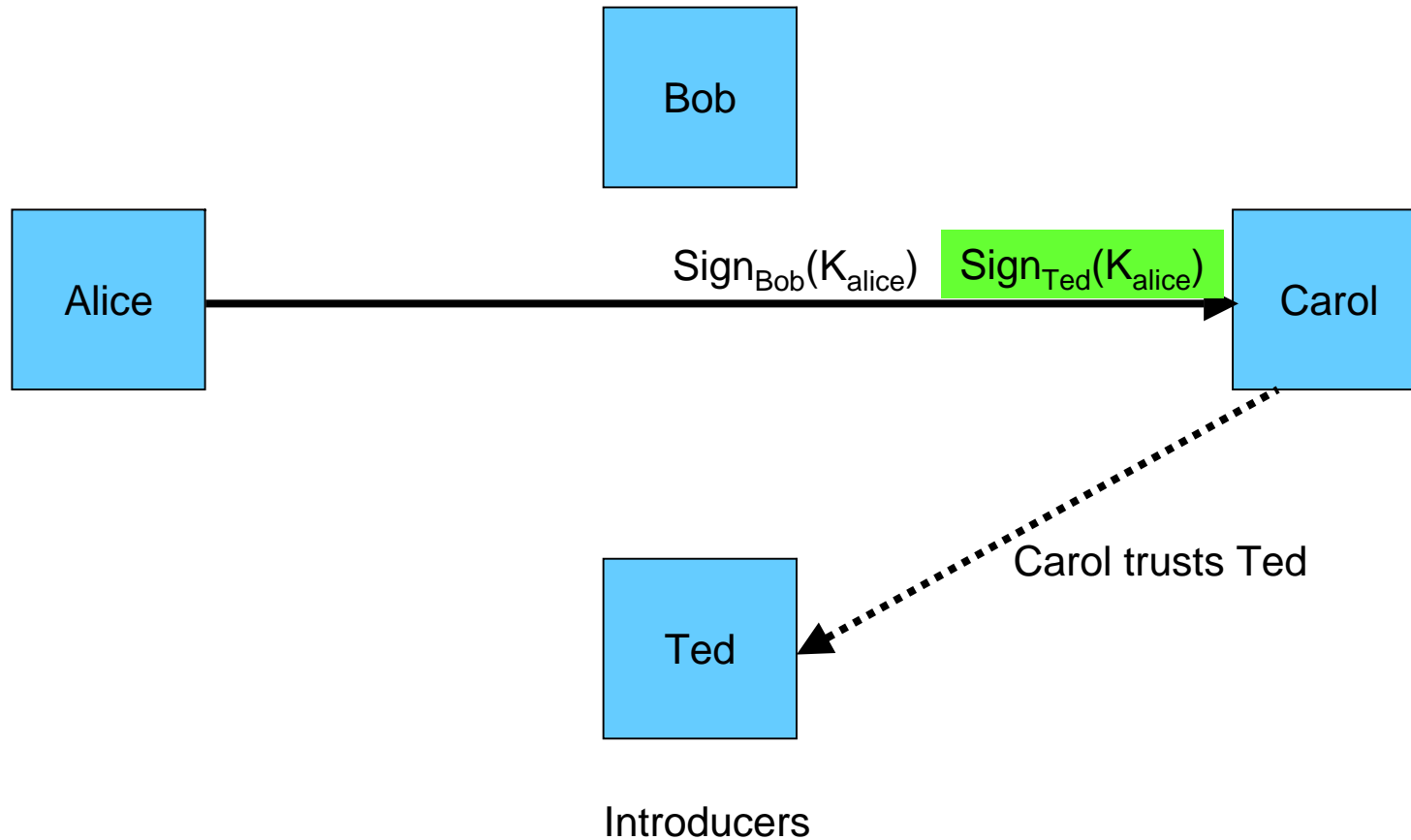
PGP for Key Management



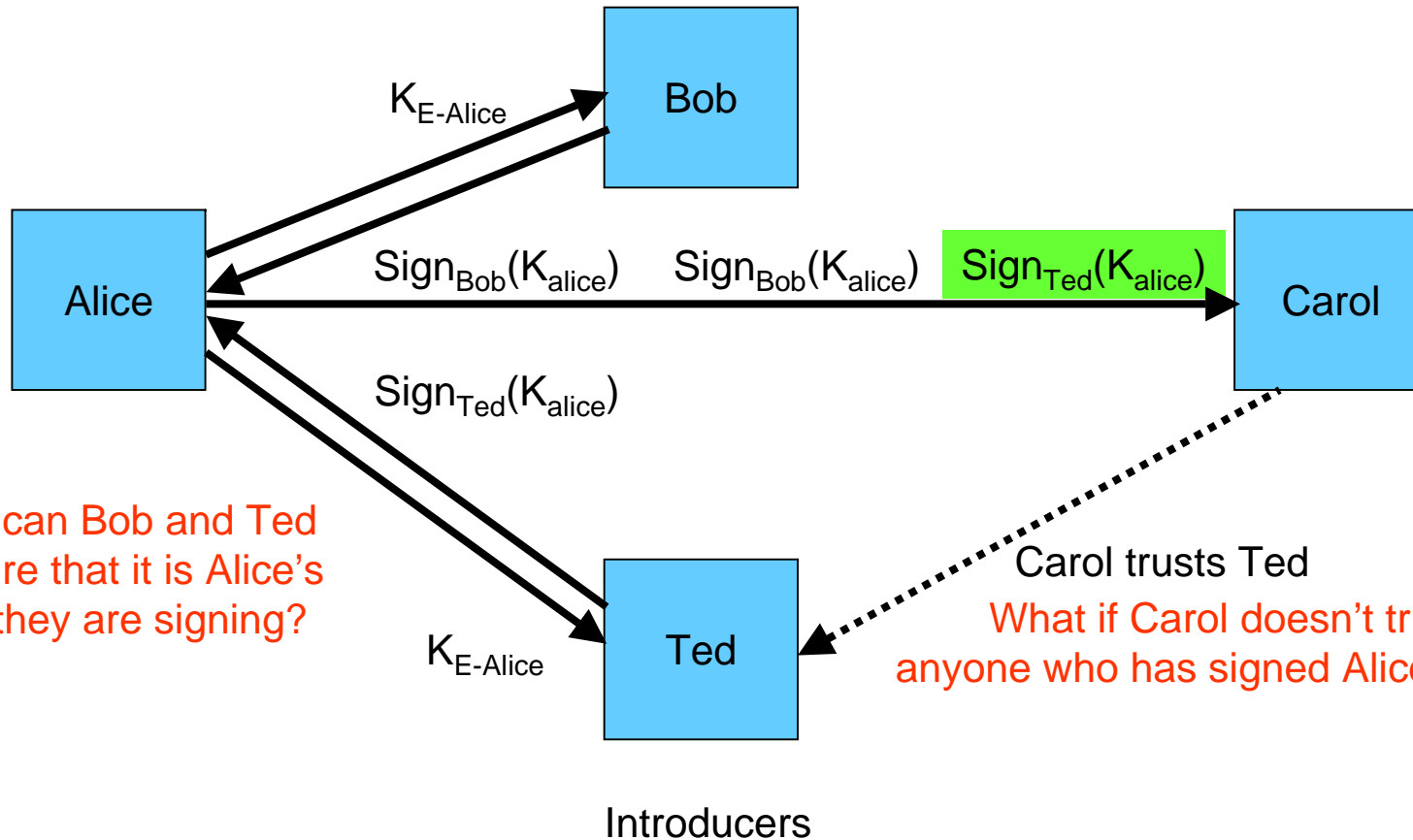
PGP for Key Management



PGP for Key Management



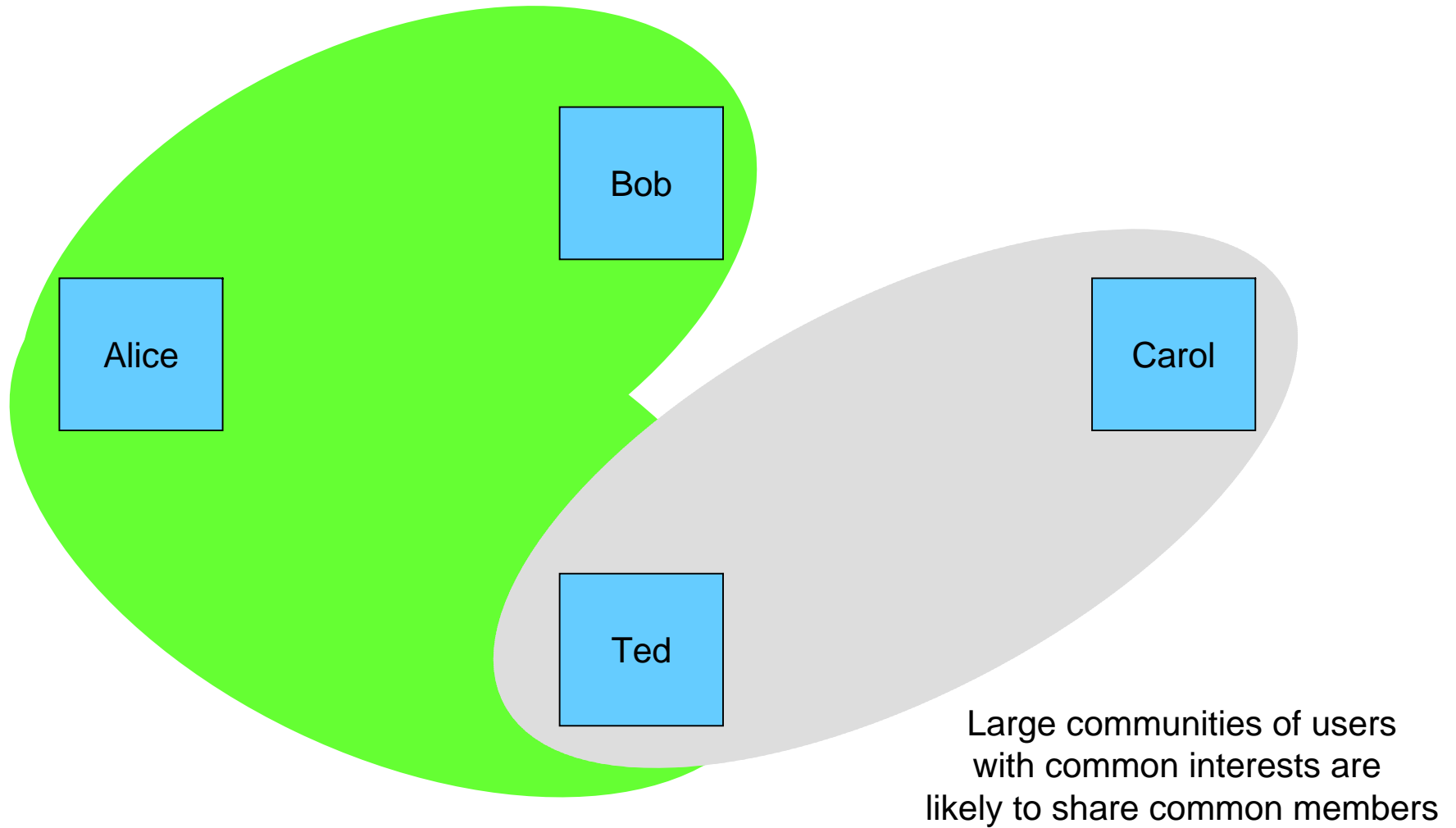
PGP for Key Management



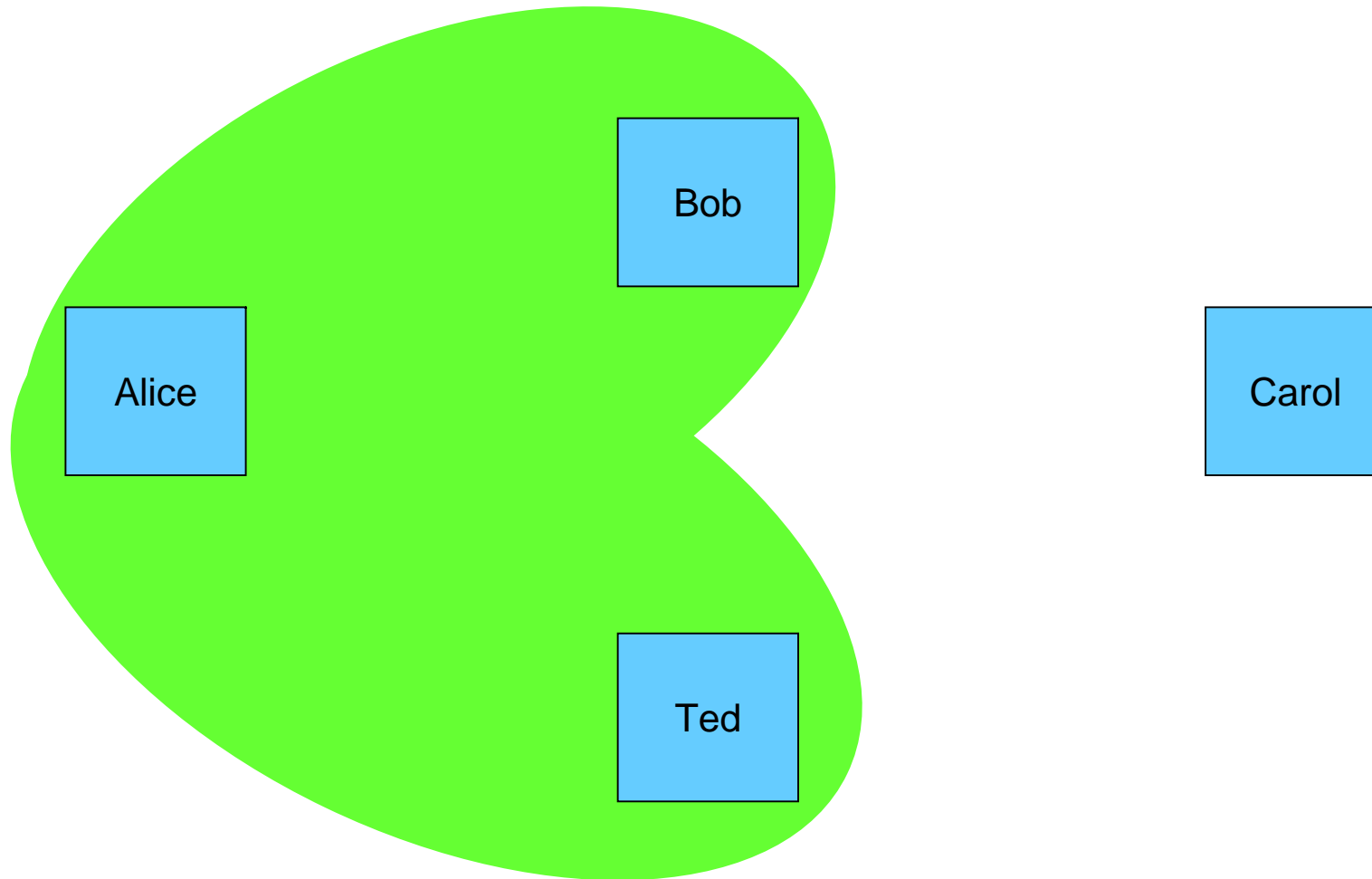
How can Bob and Ted be sure that it is Alice's key they are signing?

Carol trusts Ted
What if Carol doesn't trust anyone who has signed Alice's key?

PGP for Key Management

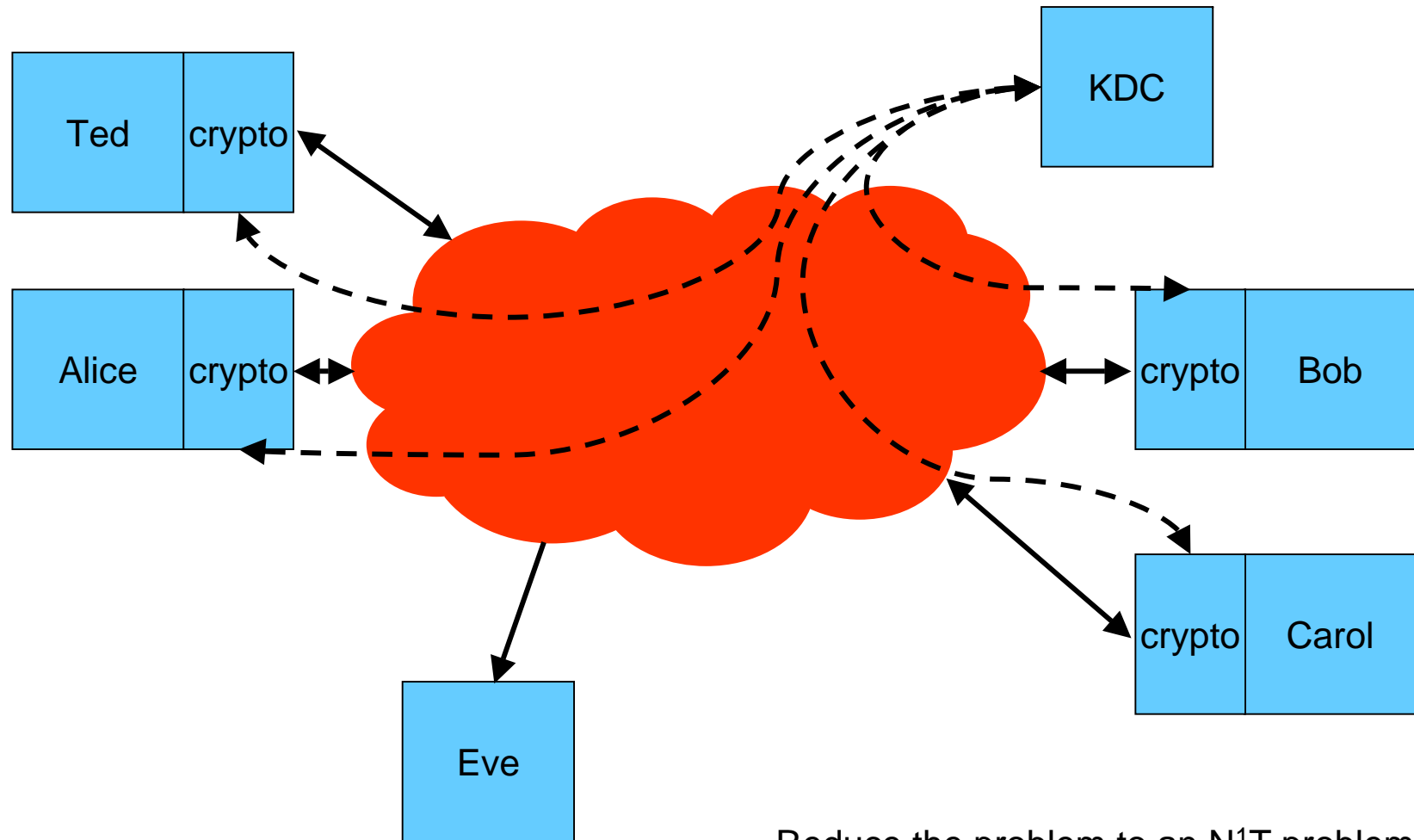


PGP for Key Management



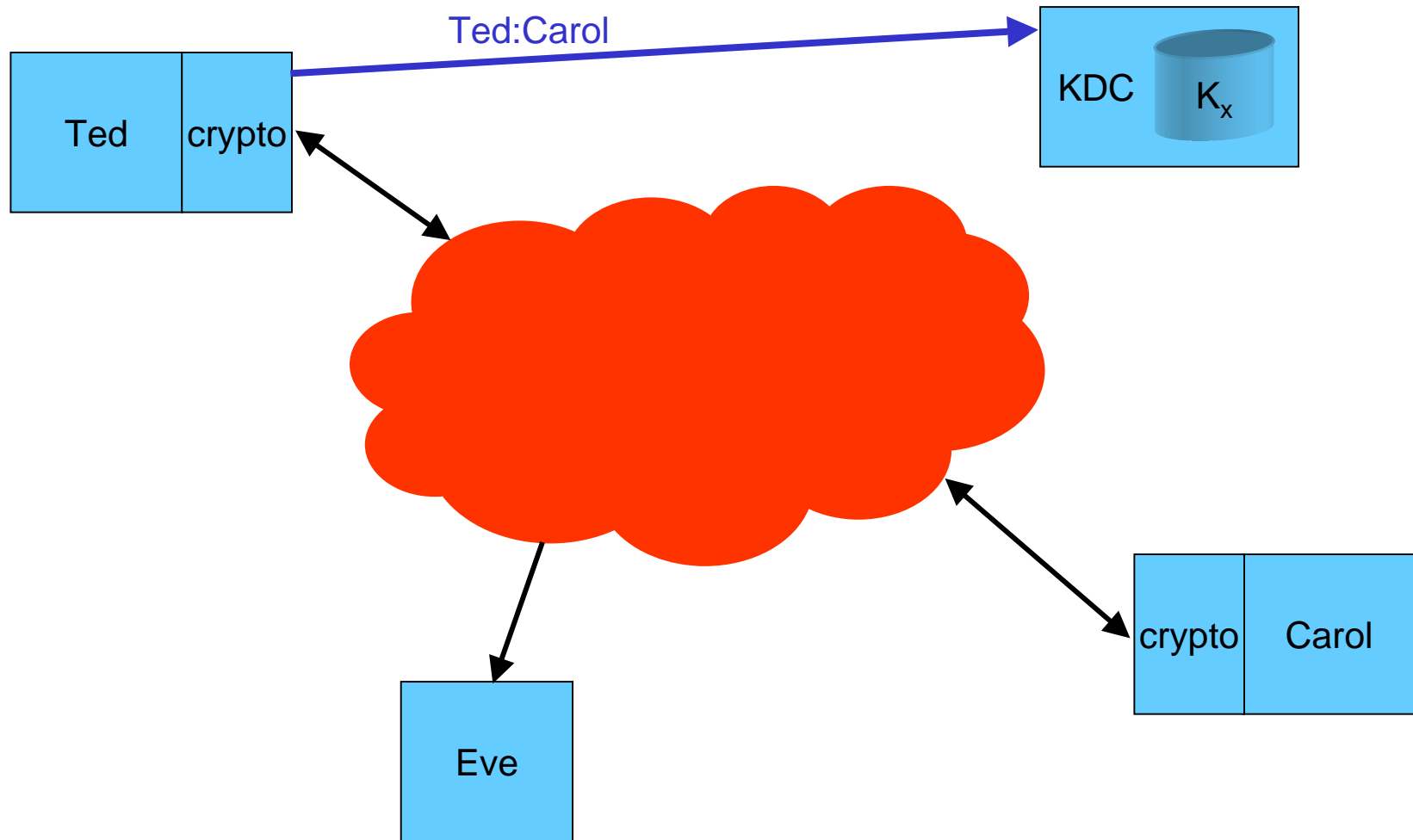
For Bob and Ted to vouch for Alice, they will need to exchange keys using a secure side channel

Key Management with a Key Distribution Center

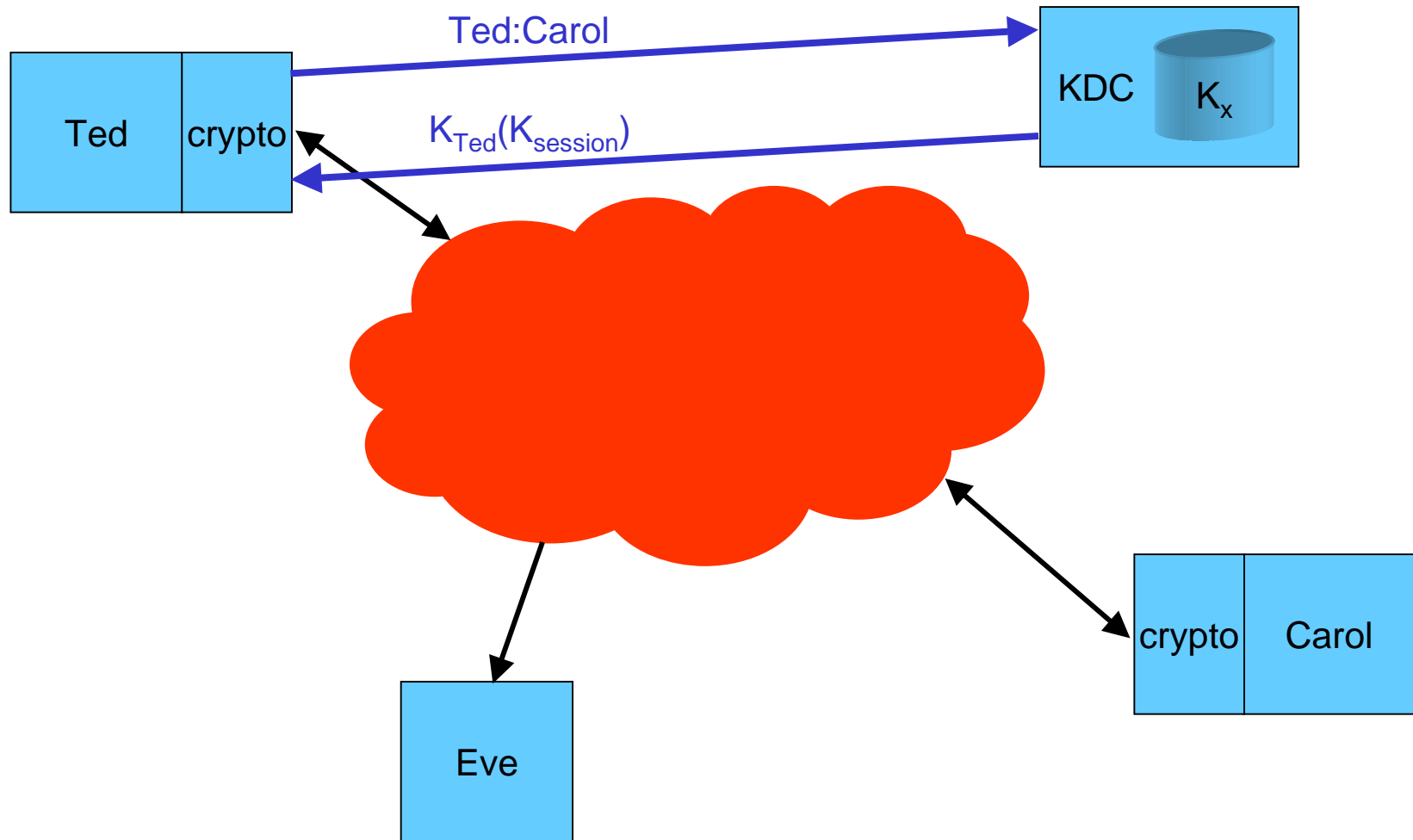


Reduce the problem to an N^1T problem
One trusted party to all communications

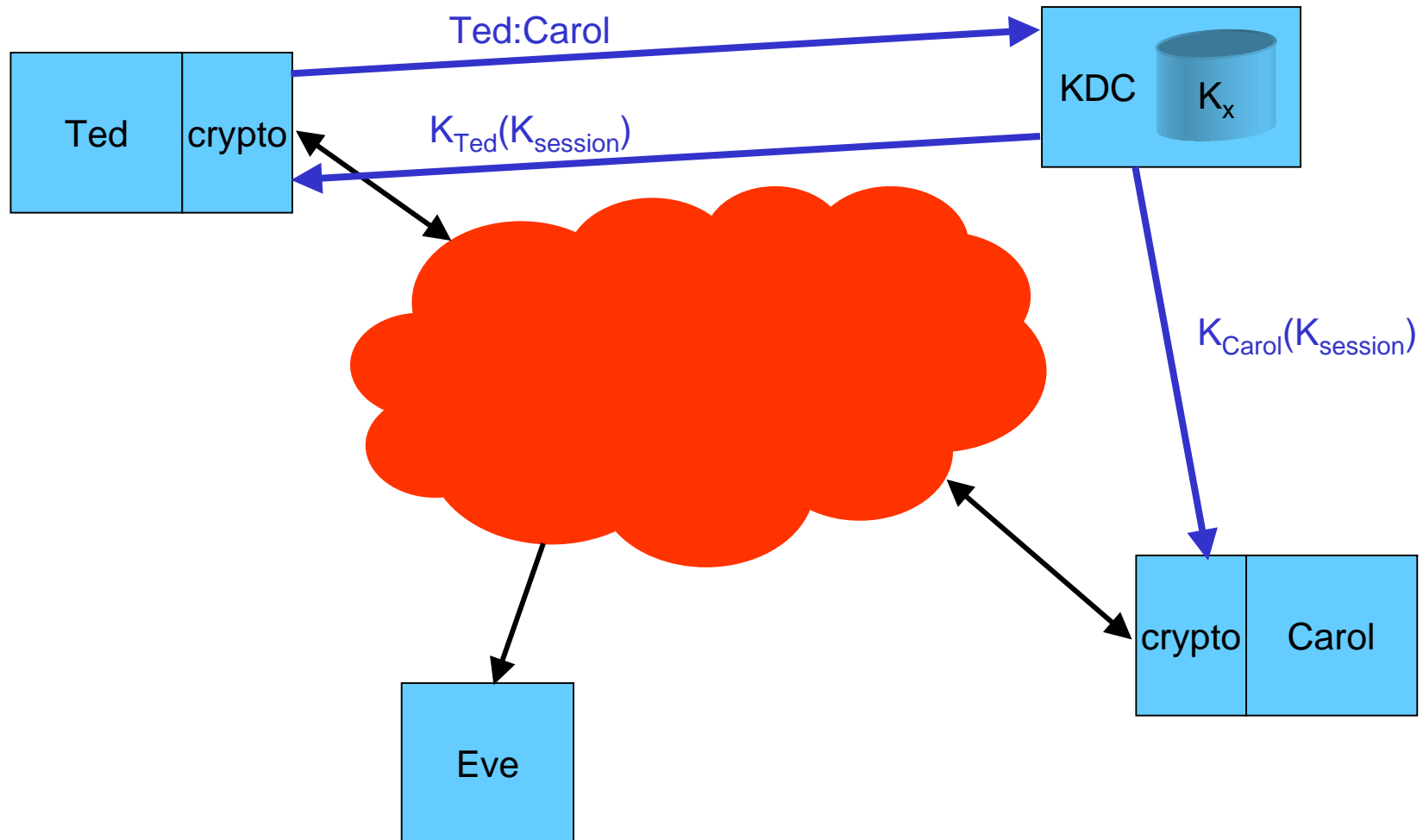
Key Management with a Key Distribution Center



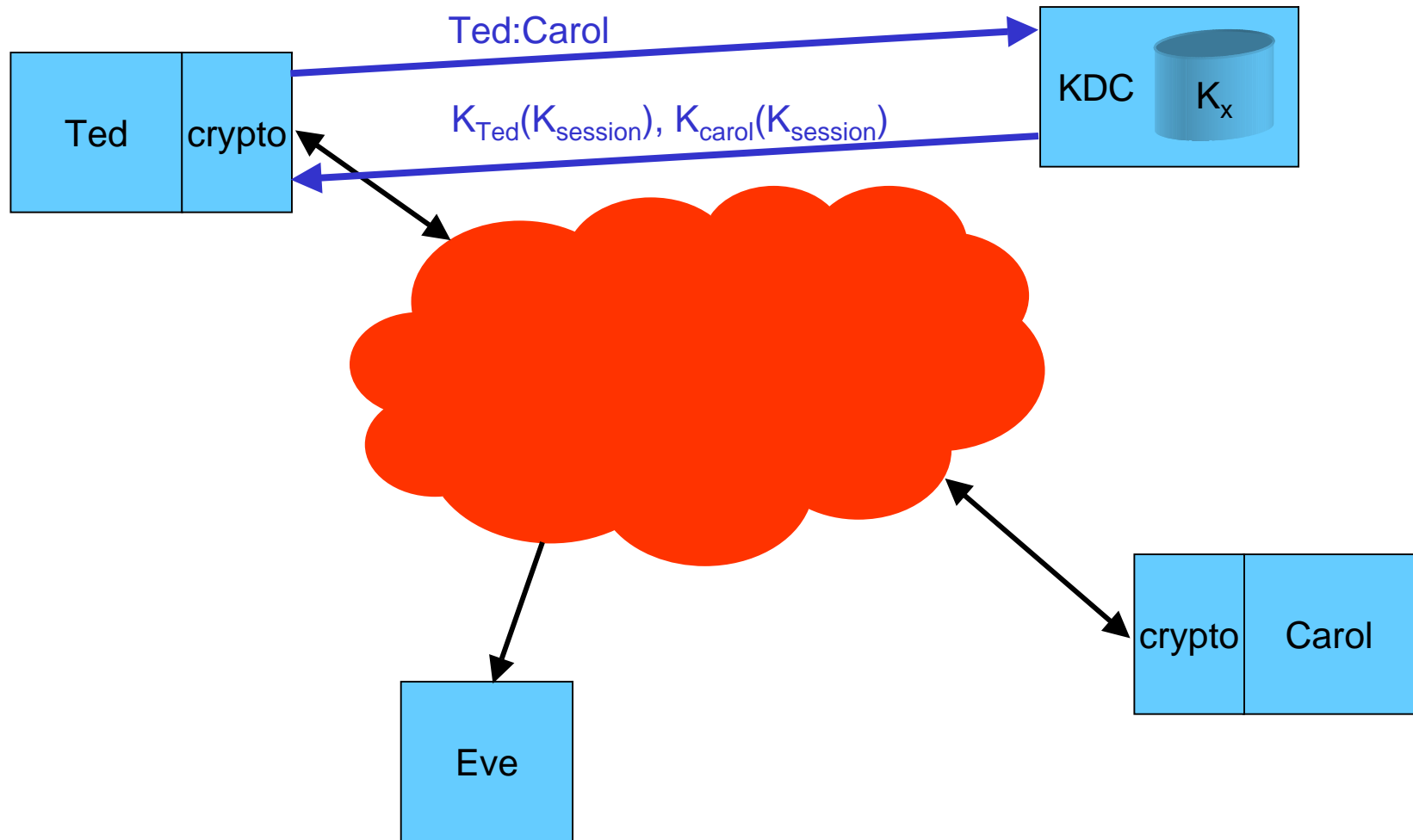
Key Management with a Key Distribution Center



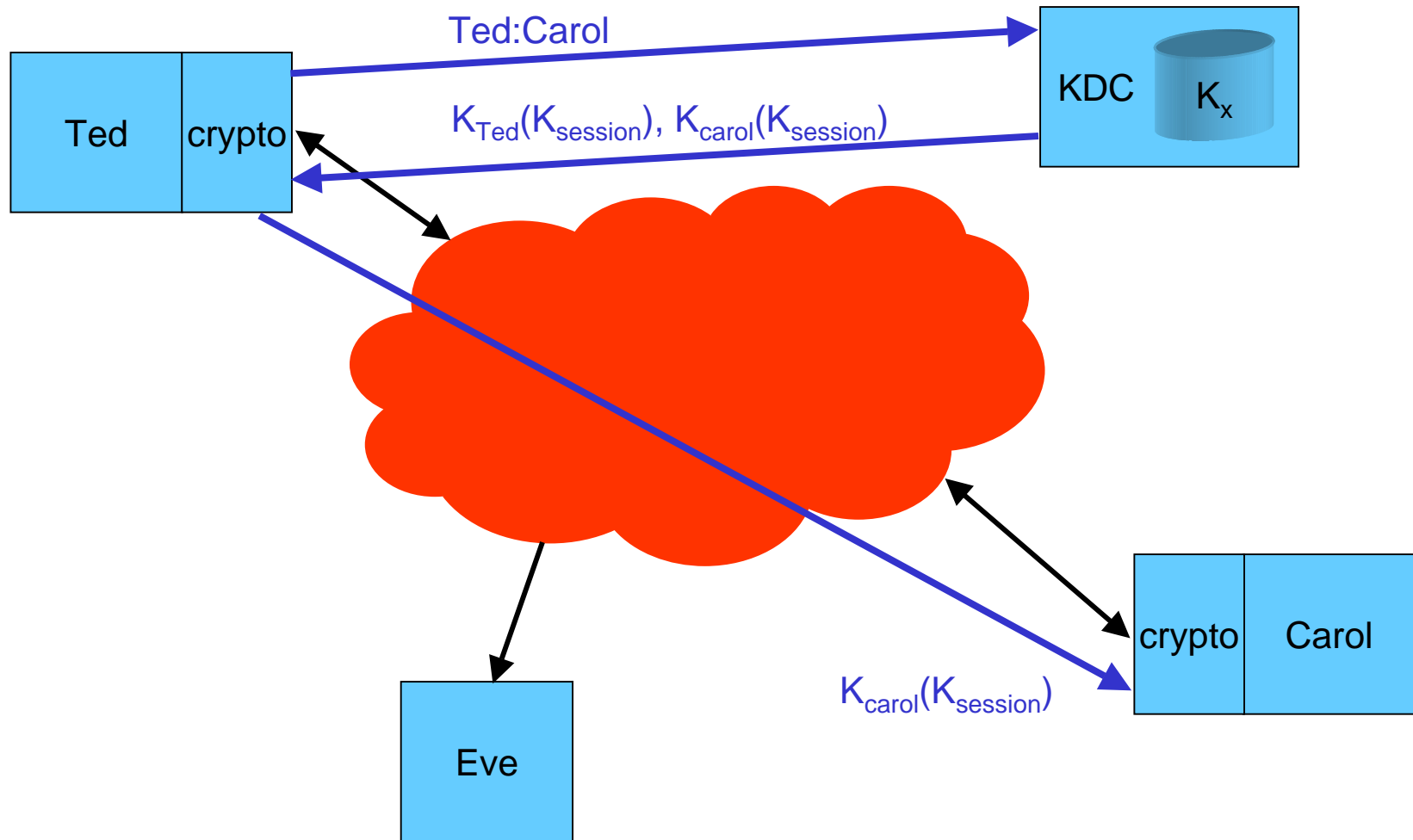
Key Management with a Key Distribution Center



Key Management with a Key Distribution Center



Key Management with a Key Distribution Center



Fundamental Security Considerations for Key Management

- Someone, somewhere in the network must be trustworthy
- At some level, communications security must be built on a shared secret
- The frequency and number of protocol exchanges must be optimized
- The key management protocol correctness must be verified

Fundamental Security Considerations for Key Management

- Someone, somewhere in the network must be trustworthy
 - It might as well be the KDC
- At some level, communications security must be built on a shared secret
 - A secret-key cryptosystem is one simple way to provide this function
- The frequency and number of protocol exchanges must be optimized
 - Some exchanges can be combined (e.g., the KDC can send both party's keys to the requestor)
- The key management protocol correctness must be verified
 - This is the hardest part – under any circumstances, is it possible for the eavesdropper to obtain any information that might give them an advantage in attacking the protocol?
 - Assume the attacker has copies of all previous messages and key exchanges.