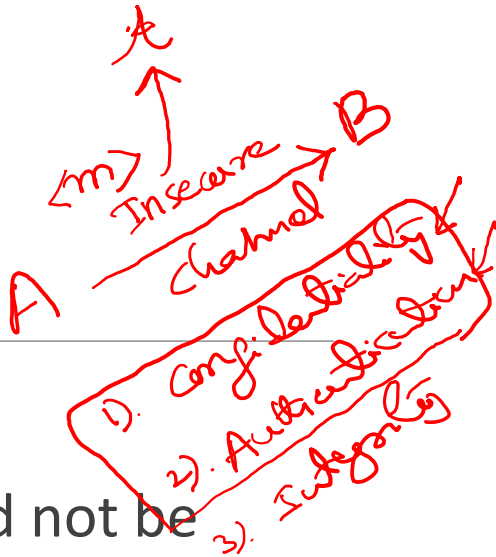
Needham-Schroeder Public-Key Protocol

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

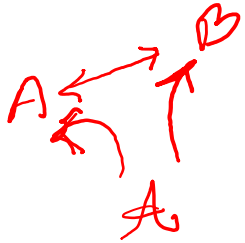
CHITTOOR, INDIA

Building a Secure Channel

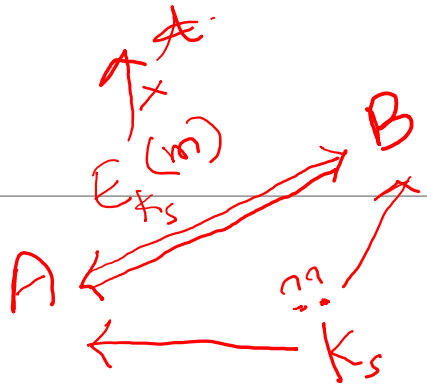


What is a secure channel?

- Messages sent between Alice and Bob should not be
  - eavesdropped by the attacker
  - tampered by the attacker
- Provide assurance on with whom you are talking to



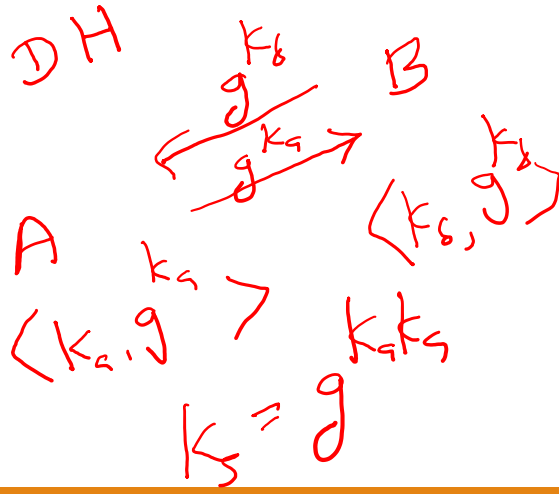
Building a secure channel out of an insecure medium



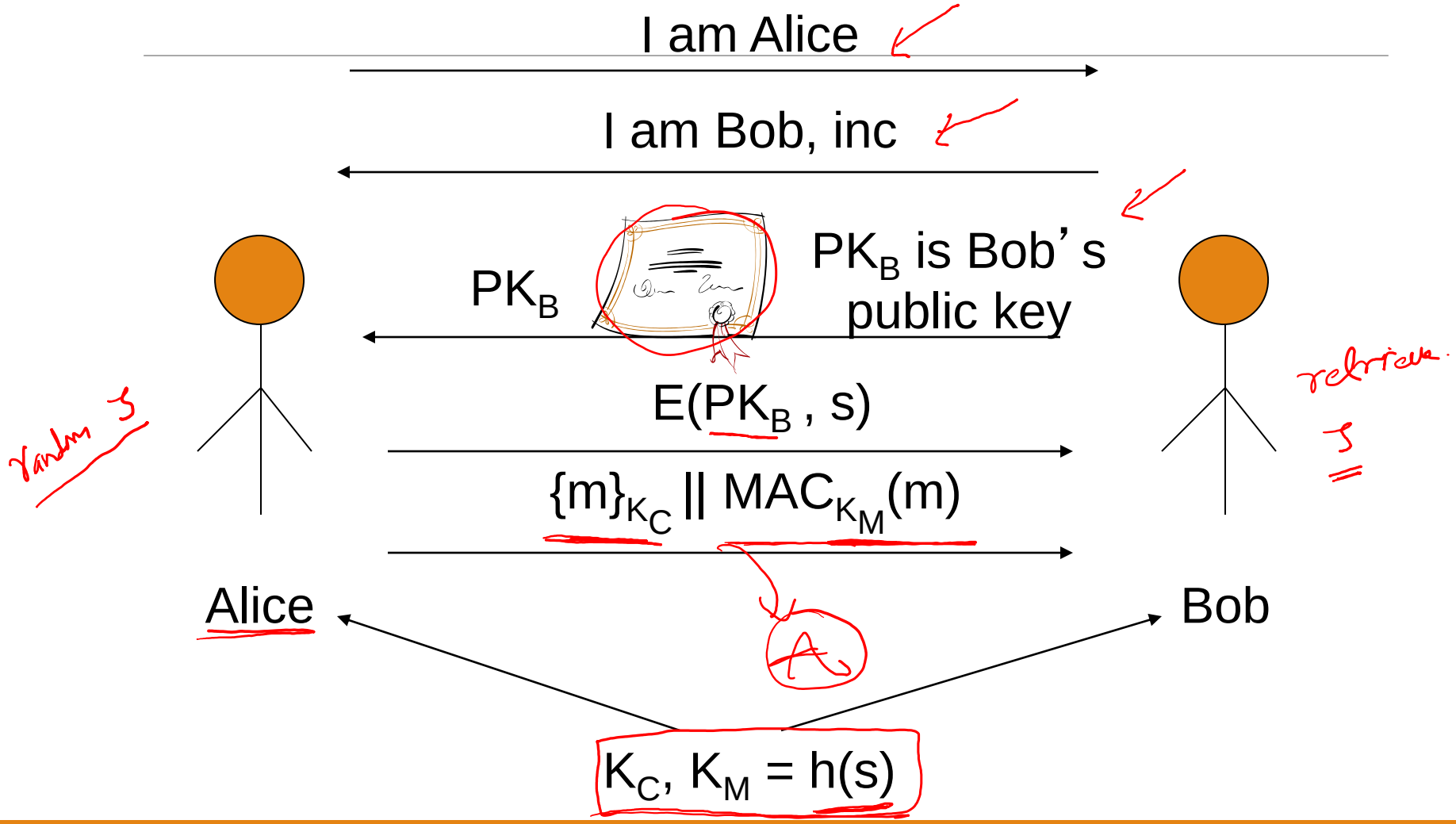
- **Use symmetric cipher**
  - Faster than public-key cipher
  - Encryption ensures confidentiality of communication
  - Authentication and data integrity ensured by applying message authentication code

MAC

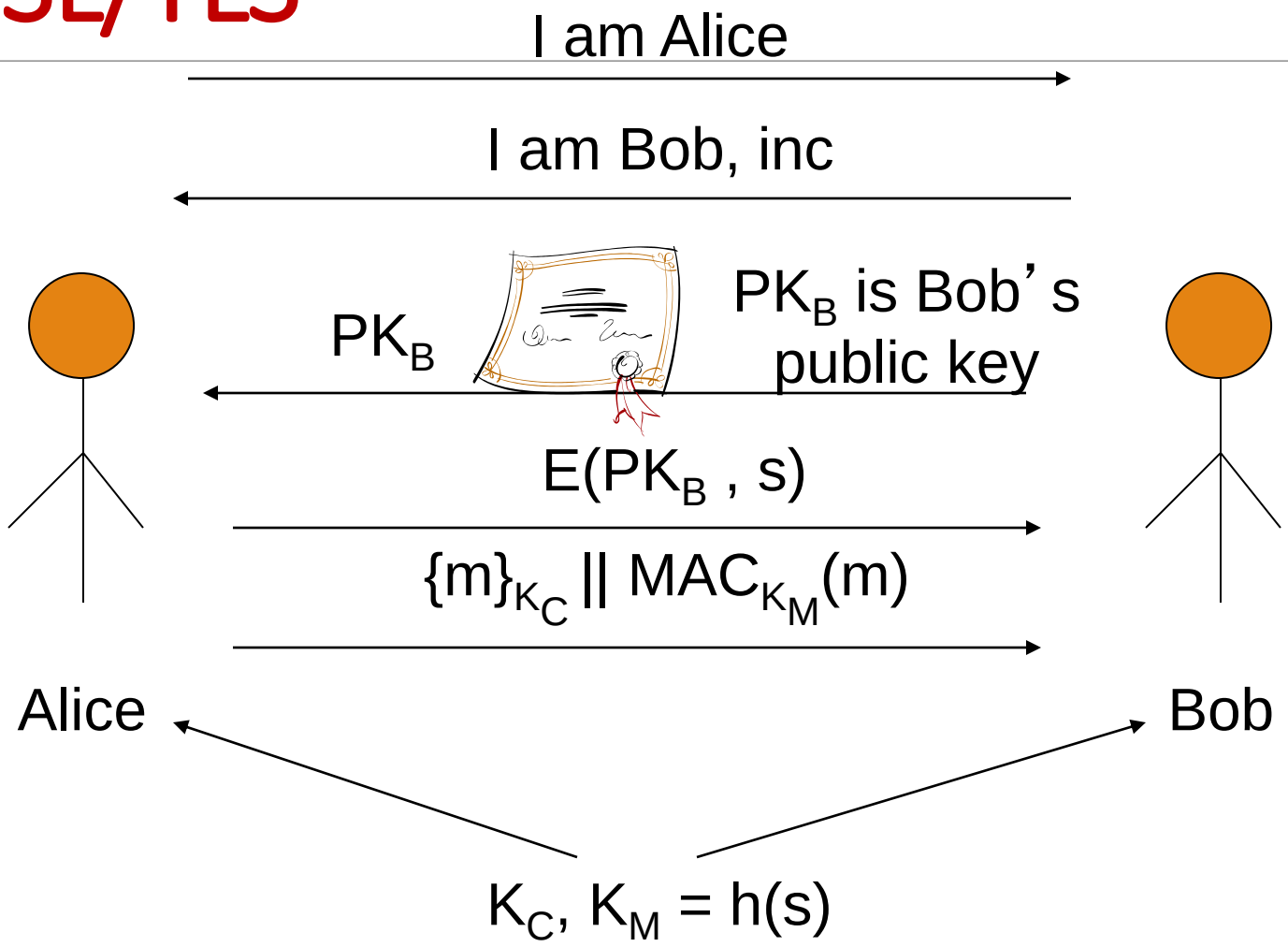
- **Need to establish a shared secret**



Building a secure channel out of an insecure medium



SSL/TLS


I am Alice
I am Bob, inc
PK_B
PK_B is Bob's public key
E(PK_B , s)
{m}_KC || MAC_KM(m)
Alice
Bob
K_C, K_M = h(s)

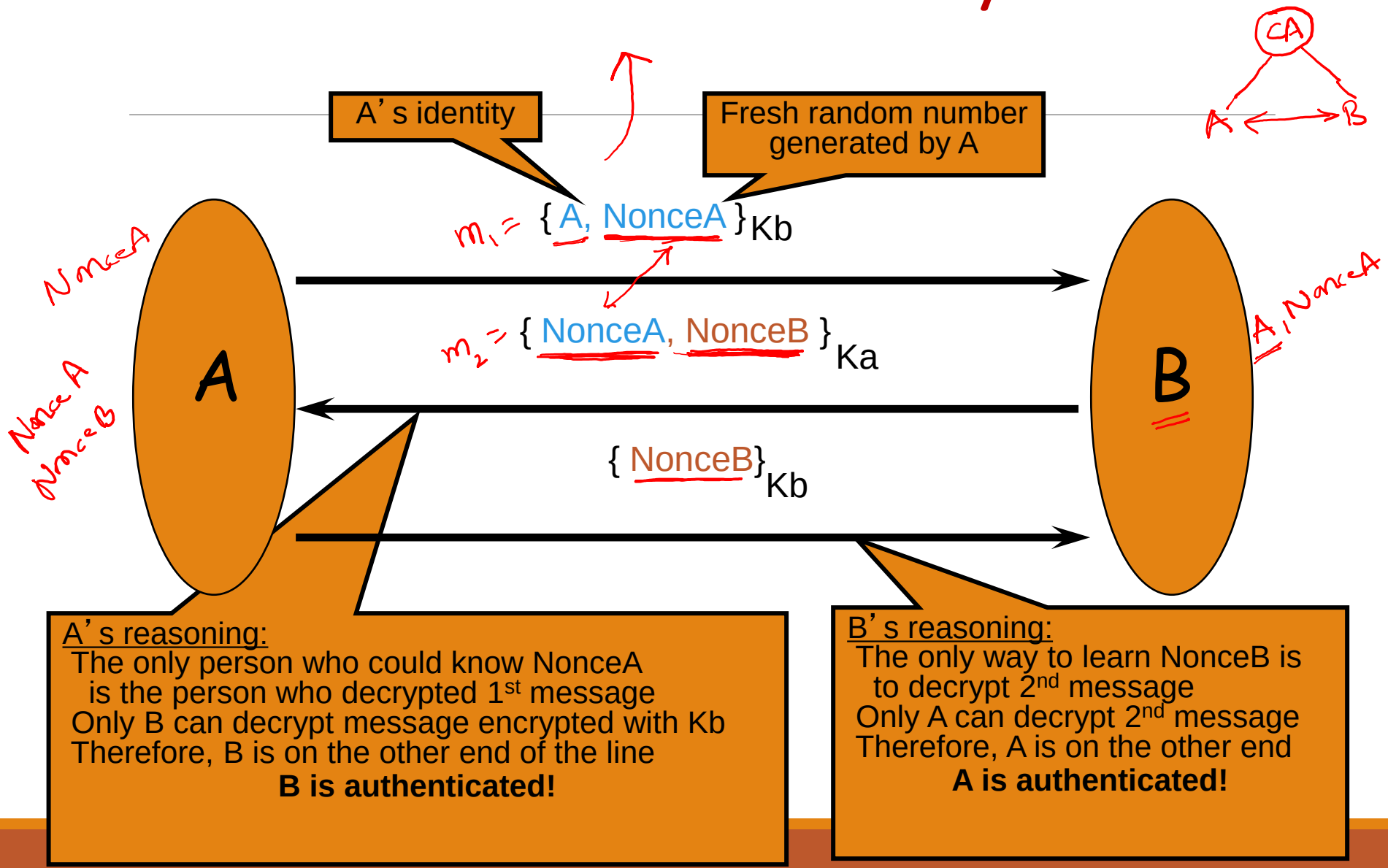
Needham-Schroeder

- Appeared in a 1979 paper
- Goal: Authentication in a network of workstations
- In 1995, Gavin Lowe discovered an attack.

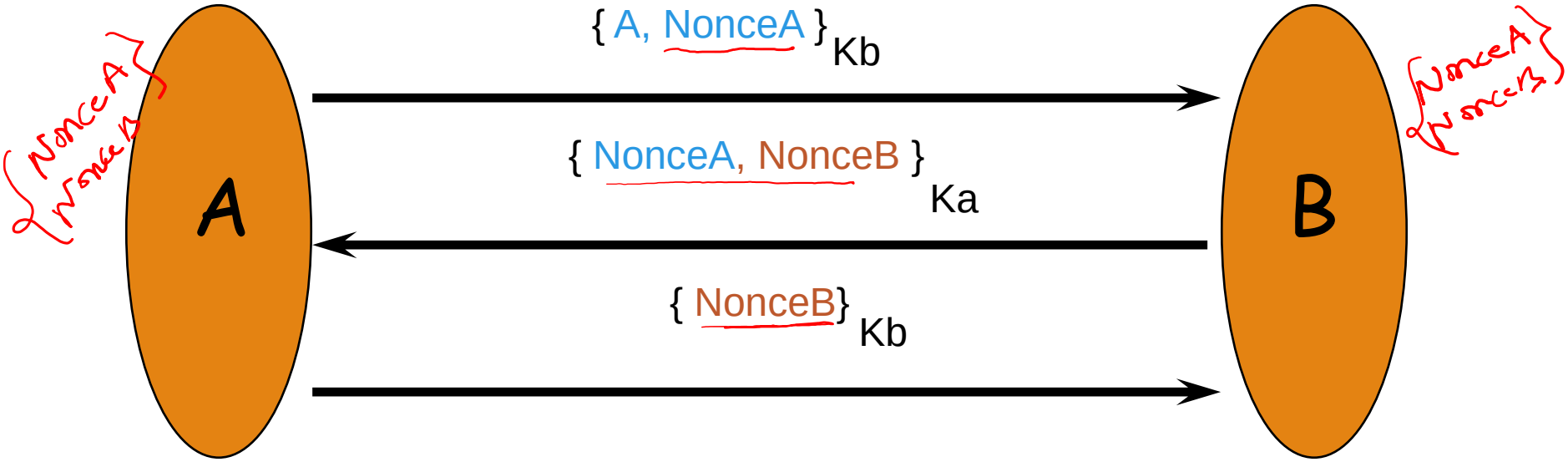
Public-key cryptography

- Every agent A has a key pair Ka, Ka^{-1}
- Any one who knows public key Ka and can encrypt messages to A (use $\{m\}_{Ka}$ notation)
- Only A knows secret key Ka^{-1}, therefore, only A can decrypt messages encrypted with Ka

Needham-Schroeder Public-Key Protocol



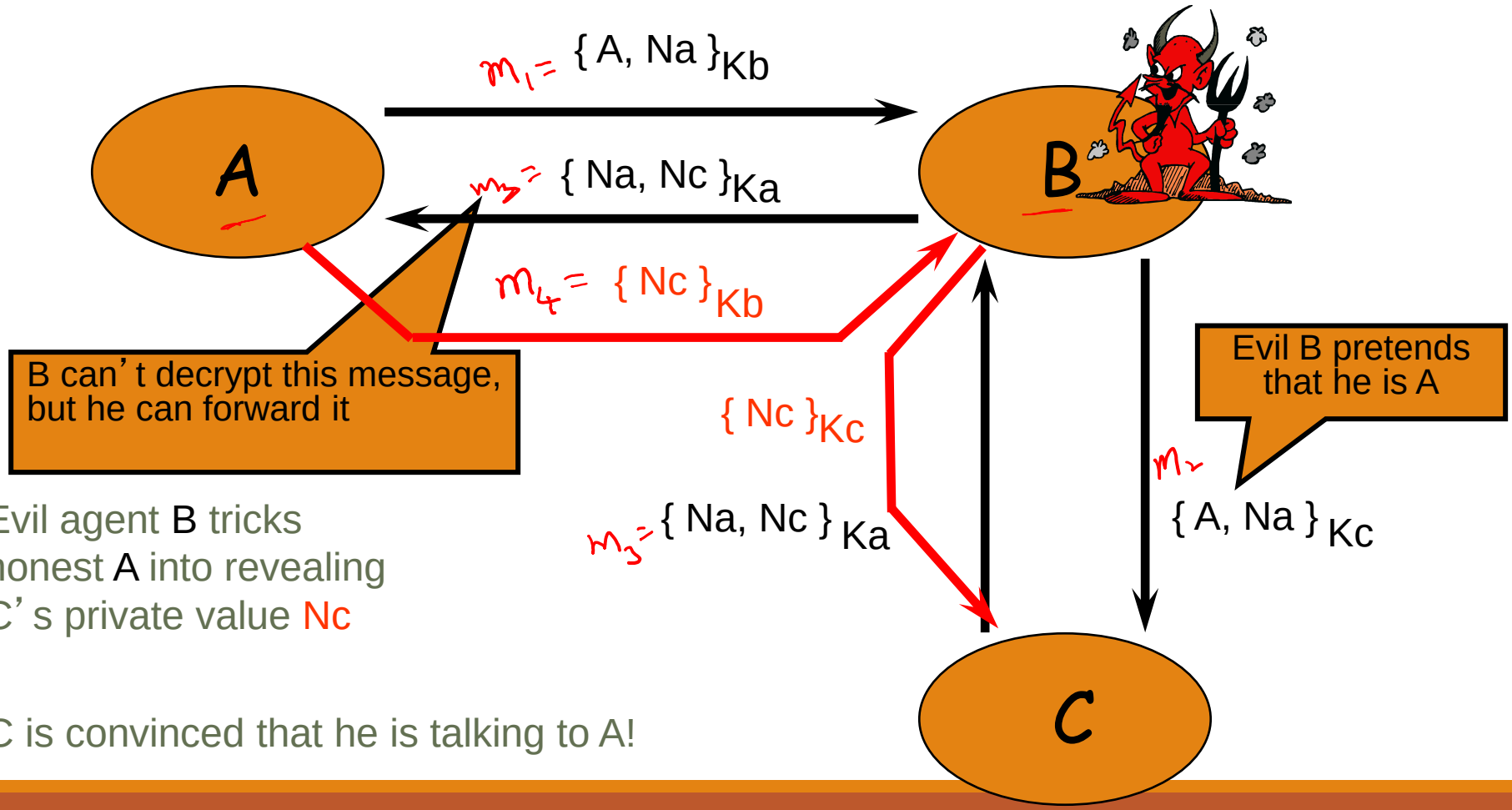
What Does This Protocol Achieve?



- Protocol aims to provide both authentication and secrecy
- After this the exchange, only A and B know NonceA and NonceB
- NonceA and NonceB can be used to derive a shared key

Anomaly in Needham-Schroeder

[published by Lowe]



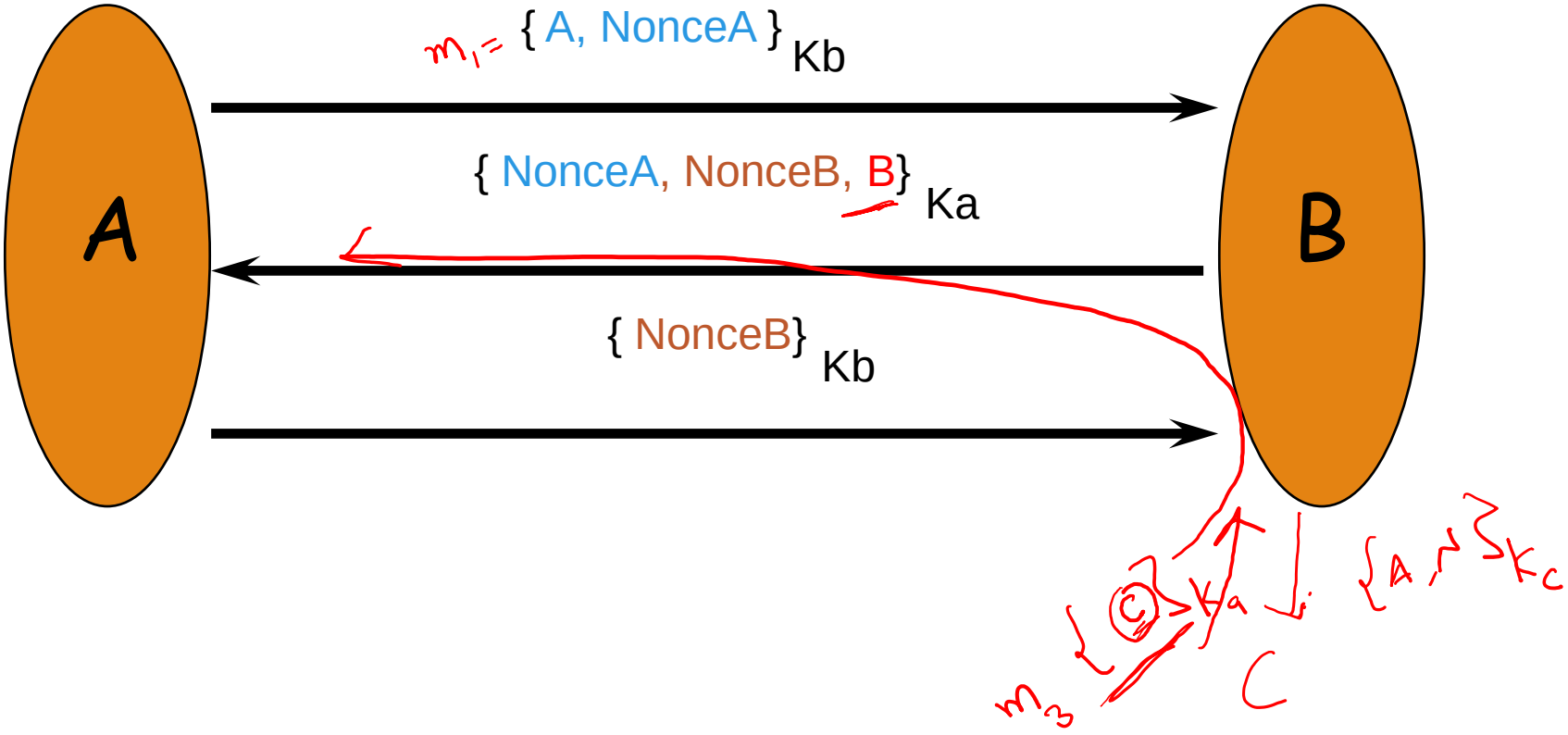
Evil agent B tricks honest A into revealing C's private value Nc

C is convinced that he is talking to A!

Lessons of Needham-Schroeder

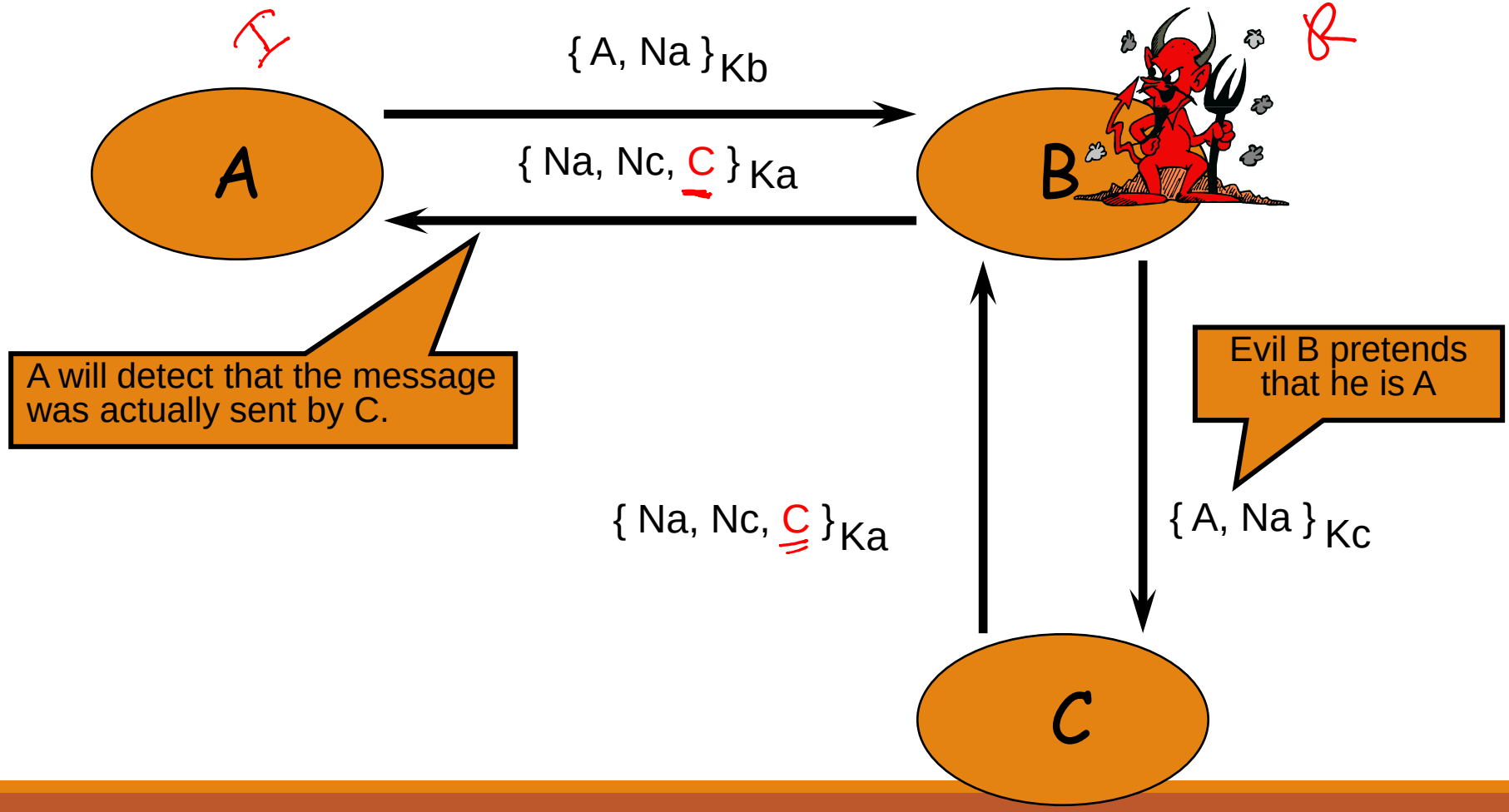
- **Classic man-in-the-middle attack**
- **Exploits participants' reasoning to fool them**
  - A is correct that B must have decrypted $\{A,Na\}_{Kb}$ message, but this does not mean that message $\{Na,Nb\}_{Ka}$ came from B
  - The attack has nothing to do with cryptography!
- **It is important to realize limitations of attacks**
  - The attack requires that A willingly talk to adversary
  - In the original setting, each workstation is assumed to be well-behaved, and the protocol is correct!

Fixing Needham-Schroeder's protocol



The attack no longer works

[published by Lowe]



References

- Lowe G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In International Workshop on Tools and Algorithms for the Construction and Analysis of Systems 1996 Mar 27 (pp. 147-166). Springer, Berlin, Heidelberg.