Trusting your friends

In the Yahalom Protocol, s is assumed to be trustworthy, and in particular to create a good cryptographic key k_{ab}.

- a can deduce that the key he receives in message 3 is a good key to share with b;
- a can deduce that b has recently been running the protocol with a;
- b can deduce that the key he receives in message 4 is a good key to share with a;
- b can hence deduce that a sent the second encrypted component of message 4, and that this component was created recently.

Key confirmation

The Yahalom Protocol assures b that a has received the key k_{ab}, but not vice versa.

Authentication using public key cryptography

- If an agent a sees a message encrypted with b's secret key, then he can deduce that b created the message.
- If a sends a message encrypted with b's public key, and which contains a secret value s, and subsequently receives s back, then a can deduce that b decrypted the message.

Needham-Schroeder Public Key Protocol

Msg 1. $a \rightarrow b : \{a, n_a\}_{PK(b)}$

Msg 2. $b \rightarrow a : \{n_a, n_b\}_{PK(a)}$

Msg 3. $a \rightarrow b : \{n_b\}_{PK(b)}$.

The protocol aims to authenticate each agent to the other, and to establish a pair of shared secrets n_a and n_b.