Shamir-Rivest-Adleman Three Pass Protocol

Author(s): A. Shamir, R. Rivest, L. Adleman

Summary: The following protocol, described in [CJ97], allows two principals to exchange a secret message without sharing any initial secret.

Protocol specification (in common syntax)

```
A, B :    principal
Ka, Kb :  symkey
M :       fresh number

1.    A  ->  B  :    {M}Ka
2.    B  ->  A  :    {{M}Ka}Kb
3.    A  ->  B  :    {M}Kb
```

Description of the protocol rules

This protocol assumes that encryption is commutative, *i.e.*

$$\{\{x\}y\}z = \{\{x\}z\}y.$$

The initiator `A` encrypts his message `M` by his secret key `Ka`, then `B` encrypts the message he received by his secret key `Kb`. Since {{M}Ka}Kb = {{M}Kb}Ka, the agent `A` can decr ypt it and send {M}Kb to `B`. Then, using `Kb`, `B` can retrieve `M`.

Citations

[CJ97] John Clark and Jeremy Jacob. A survey of authentication protocol literature : Version 1.0., November 1997.