Academic Year: 2023-2024.

Semester : VI Subject : CSS

## NEEDHAM - SCHROEDER AUTHENTICATION PROTOCOL:

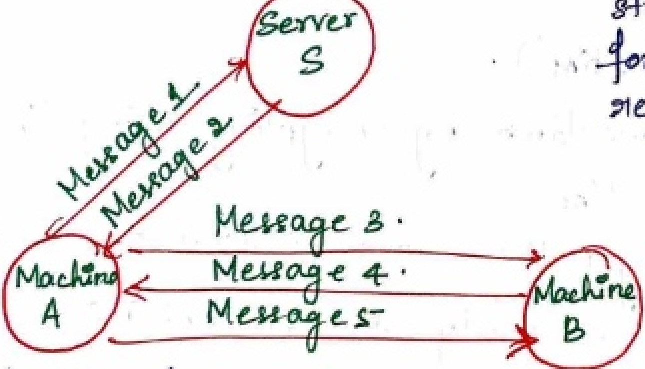
It uses a communication protocol to secure an unsecure communication.

There are 2 types:

* NS protocol with symmetric key.
* NS protocol with asymmetric key.

### (1) NS protocol with symmetric key.

Nonce → Randomly generated string which is valid only for sometime to prevent replay attack.



A → Machine A. B → Machine B.

$K_{AS}$ → Symmetric key known only to A n S.

$K_{BS}$ → Symmetric key known only to B n S.

$N_A$ and $N_B$ → Nonce generated by A and B.

$K_{AB}$ → Symmetric key (or) Session key used for communication between A and B.

**Message 1:** $A \rightarrow S : \{A, B, N_A\}$.

A identifies herself and B to S, telling the server she wants to communicate with B. by sharing $N_A$.

**Message 2:**

$S \rightarrow A : \{N_A, K_{AB}, \underbrace{B\{K_{AB}, A\}_{KBS}}_{\text{key to } B}\}_{KAS}$.

Semester : VI Subject : CSS Academic Year: 2023 2024

* S sends $K_{AB}$ to A and also encypted ~~$K_{AB}$ with~~ key to B.
* All are encypted using $K_{AS}$.
* A will decypt using $K_{AS}$ and get $K_{AB}$ for her and send encypted key to B.

Message3: A → B : $\{K_{AB}, A\}K_{BS}$.

B will decypt using $K_{BS}$ and get $K_{AB}$.

Now both A and B got $K_{AB}$.

Message4:

B → A : $\{N_B\}K_{AB}$.

*B will encypt his nonce value using $K_{AB}$ and send it to B.

*B proves himself to A.

*A decypt $N_B$ using $K_{AB}$ which she has received.

Message5:

A → B : $\{N_B+1\}_{KAB}$.

This step is peformed to prove herself to AB. She has veified B and she communicates that she holds the same key.

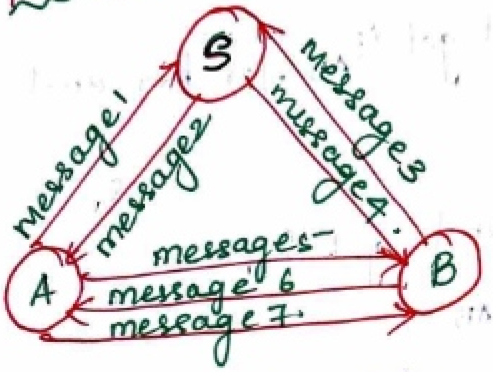
NS protocol with asymmetric key.

$K_{PA}$ → Public key of A . (A, S)

$K_{PB}$ → Public key of B . (B, S)

$K_{SS}$ →. $\underbrace{\text{Server secret key}}_{}$.

Known by S, A, B.



Message 1 : A → S : A, B.

A wants to communicate with B. So A will request B's public key from S.

Message 2 : S → A : $\{K_{PB}, B\}_{KSS}$.

→ Server sends the public key of B by encyption using KSS.

→ A will decrypt using KSS and receive $K_{PB}$.

message 3 : B → S : B, A.

B request A's public key from the server.

message 4 : S → B : $\{K_{PA}, A\}_{KSS}$.

→ Server sends the public key of A by encypting using KSS.

→ B will decypt using KSS and receive $K_{PA}$.

message 5 : A → B : $\{N_A, A\}_{KPB}$.

A encypts his naunce using public key of B.

B decypts and receives $N_A$.

Semester : VI Subject : CSS Academic Year: 2023-2024.

message 6 : $B \rightarrow A : \{N_A, N_B\}_{K_{PA}}$.

B encypts $N_A$ and $N_B$ using $K_{PA}$ and sends to A.

A decypts ~~and~~ using his own private key and receives.

$N_A, N_B$.

Ih this step B has proved himself to A.

message 7 : $A \rightarrow B : \{N_B\}_{K_{PB}}$.

In this step A proves himself to B, by sending $N_B$ to B.