two-pass mutual authentication

Protocol Purpose

Two parties authenticate each other. Aim of the Mutual authentication is to make sure to each of the parties of the other's identity. In this protocol authentication should be achieved by a single encrypted message sent from each party.

Definition Reference(s)

- [CJ, ISO97]

Model Author(s)

- Haykal Tej, Siemens CT IC 3, 2003 and
- Luca Compagna et al, AI-Tw) Lab DITw) ST University of Genova, November 2004

Alice&Bob style

```
1. A -> B : PKa,A,{PKa,A}inv(PKs), Na, B, Tet2,{Na,B,Tet1}inv(PKa)
2. B -> A : PKb,B,{PKb,B}inv(PKs), Nb, A, Tet4,{Nb,A,Tet3}inv(PKb)
```

- `inv(PKs)` is the private key of the server `C`
- `{PKa1(t)}inv(PKs)`

```
                  {na(a,6),b,ctext1}inv(pka)
i     -> (b-1,9) : start
(b-1,9) -> i     : pkb,b,{pkb,b-1}inv(pks)(b-1,9),ctext2,
                  {na(b,9),a,ctext1}inv(pkb)
i     -> (a,6) : pkb,b,{pkb,b-1}inv(pks)(b-1,9),ctext2,
                  {na(b,9),a,ctext1}inv(pkb)
```

Further Notes

```
local SA, RA, SB, RB: channel (dy)
```

udeobA,i(}1