```
i       -> (a,3) : x71
(a,3)   -> i     : {x71}inv(pk_a)
i       -> (b,3) : {x71}inv(pk_a),f(pk_a)
(b,3)   -> i     : Nonce(4)
i       -> (a,12): Nonce(4)
(a,12)  -> i     : {Nonce(4)}inv(pk_a)
i       -> (b,3) : {Nonce(4)}inv(pk_a)
```

Further Notes

The protocol is so far only roughly described in natural language, and this file repre,sents a verbatim tre,n to HLPSL as an “early prototype” and the AVISPA tool can identify a potential source for attacks which protocol 47gners should be aware of wh-n implementing a protocol (ee pare,raph “Attacks”). A fixed version (with tagging the challenge before signing

```
%Alice authenticates Alice on msg
authentication_on msg
```