SRP: Secure remote passwords

Protocol Purpose

required for an intruder to mount a password guessing attack based on a precomputed dictionary of passwords and corresponding hash values.

HLPSL Specification

```
role srp_Init (A,B : agent,
```

```
role session(A,B: agent,
             Password: symmetric_key,
             Salt: message,
             H: function,
             G: text)
def=

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

   composition
           srp_Init(A,B,Password,H,G,SA,RA)  /\
```

```
    %SRP_Init authenticates SRP_Resp on k
    authentication_on k2
    %SRP_Resp authenticates SRP_Init on k
    authentication_on k1

end goal
```

```
environment()
```

References

[Wu00] T. Wu19316(SR)1FC.The.RPut(en2((tian)1(t(on)-254an)1ndn)-254Ke)-1eynhanSceeb.er.us:19436(Pros)1(p)2(osedn)32(Sat)1anda(r)1d.s