CRAM-MD5 Challenge-Response Authentication Mechanism

Protocol Purpose

CRAM-MD5 is intended to provide an authentication extension to IMAP4 that neither transfers passwords in cleartext nor requires significant security infrastructure in order to function. To this

```
end role
```

```
role session(A, S: agent,
             K, F: function)
def=

  local SK: message,
        SNDA, SNDS, RCVA, RCVS: channel (dy)

  init SK = K(A.S)

  composition
       client(A,S,SK,F,SNDA,RCVA)
    /\ server(S,K,F,SNDS,RCVS)

end role
```

```
role environment()
def=

 const a, s : agent,
       k, f : function,
       auth : protocol_id

 intruder_knowledge = {a,s,i,f}

 composition
```

```
%secrecy_of SK
```