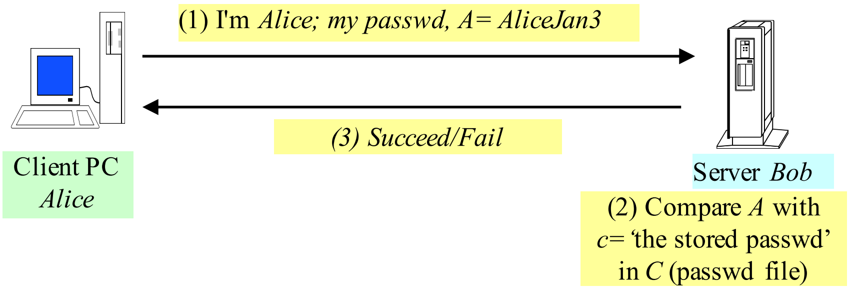
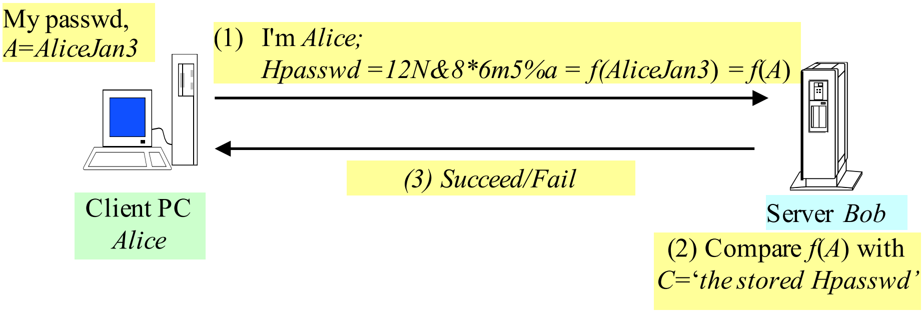
## Exercise Questions for Week 3 – Authentication (this is for week 3)

**E1.1. Identify attacks or security threats the following three protocols/methods are vulnerable to.**

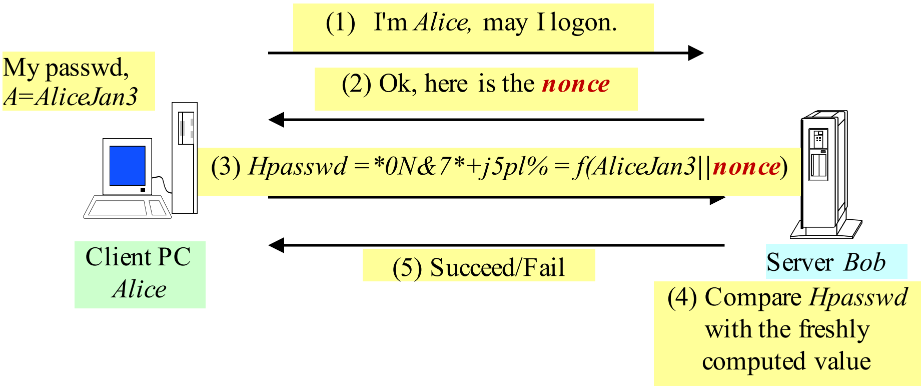
**Protocol 1:**


(1) I'm *Alice; my passwd, A= AliceJan3*
*(3) Succeed/Fail*
Client PC *Alice*
Server *Bob*
(2) Compare *A* with *c*= 'the stored passwd' in *C* (passwd file)

**Protocol 2:**


My passwd, *A=AliceJan3*
(1) I'm *Alice;*
*Hpasswd =12N&8*6m5%a = f(AliceJan3) = f(A)*
*(3) Succeed/Fail*
Client PC *Alice*
Server *Bob*
(2) Compare *f(A)* with *C='the stored Hpasswd'*

**Protocol 3:**


(1) I'm *Alice,* may I logon.
(2) Ok, here is the ***nonce***
My passwd, *A=AliceJan3*
(3) *Hpasswd =*0N&7*+j5pl% = f(AliceJan3||****nonce****)*
(5) Succeed/Fail
Client PC *Alice*
Server *Bob*
(4) Compare *Hpasswd* with the freshly computed value

**E1.2. How many different ways of implementing the challenge-response authentication approach? Provide all the possible implementations.**

**E1.3. (a) With regard to the Kerberos authentication solution, describe the role of the authenticator, and explain why an authenticator is NOT required when a client requests a ticket-granting ticket from an authentication server.**

**(b) Extend the Kerberos 4 protocol to allow a client *C* in a realm *A* to access a server in another realm *B*. Explain why *C* needs to acquire a ticket from the ticket-granting server in *A* and then another ticket from the ticket-granting server in *B.***