Homework Assignment # 12

Due Date: Never

This homework will not be graded. It is nevertheless recommended as preparation for the final exam, as the material treated in the last lecture is relevant for the exam.

1. We reconsider problem 6 (a) from homework #8 which dealt with the Diffie-Hellman key exchange protocol. Assume now that Oscar runs an active man-in-the-middle attack against the key exchange given in the problem. He uses the value $o = 16$. Compute the key pairs K_{AO} and K_{BO} (i) the way Oscar computes them, and (ii) the way Alice and Bob compute them.

2. Assume Oscar attempts to use an active (substitution) attack against the Diffie-Hellman key exchange with certificates in the following ways:

   (a) Alice wants to communicate with Bob. When Alice obtains C(B) from Bob, Oscar replaces it with (a valid!) C(O). How will this forgery be detected?

   (b) Same scenario. Oscar tries now to replace only Bob's public key b_B with his own public key b_O. How will this forgery be detected?

3. One major problem in certificate systems in practice is the establishment of a user identity. Describe in detail how Oscar can cause mischief if he manages to trick a CA in believing that he is Alice. What kind of information will the certificate then contain? Show how an authenticated Diffie-Hellman key exchange between Bob and Oscar will then look.

4. It seems as though Oscar could easily run a man-in-the-middle attack if a party requests a certificate. Assume a certificate is requested by Alice by sending the ID and the public key to the CA. *Who* will easily detect if Oscar replaces the public key of Alice in the certificate request by his own one?

5. Another problem in certificate systems is the authenticated distribution of the CA's public key which is needed for certificate verification. Assume Oscar has full control over all of Bob's communications, that is, he can alter all messages to and from Bob. Oscar replaces now the CA's public key with his own one (note that Bob has no means to authenticate the key that he receives, so he thinks that he received the CA public key.)

   (a) (Certificate issuing) Bob requests a certificate by sending a request containing (1) Bob's ID $ID(B)$ and (2) Bob's public key b_B from the CA. Describe exactly what Oscar has to do so that Bob doesn't find out that he has the wrong public CA key.

   (b) (Protocol execution) Describe what Oscar has to do to establish a session key with Bob using the authenticated Diffie-Hellman key exchange, such that Bob thinks he is executing the protocol with Alice.