

ICS 134

Homework 3

Due at NOON, Friday, March 16.
Submission by email to the TA: plaintext or PDF only.

Problem 1.

Consider the following authentication protocol where Alice and Bob share K .

1. $A \rightarrow B$: Hi Bob, it's Alice
2. $B \rightarrow A$: R_b
3. $A \rightarrow B$: $E(K, R_b), R_a$
4. $B \rightarrow A$: $E(K, R_a)$

Is a reflection attack possible? Explain your answer

Problem 2.

Explain what happens (if anything) when the signer (using DSA) re-used the same random number.

Problem 3.

This protocol is supposed to let A and B (who already share a long-term key K) agree on a new session key K_s and to perform mutual authentication. Assume that K_s and N_a are of the same length and are always chosen at random.

1. $A \rightarrow B$: $E(K, N_a)$
2. $B \rightarrow A$: $N_a, E(K, K_s)$
3. $A \rightarrow B$: $E(K, K_s, N_a)$

Find possible problem(s) or attack(s) in this protocol and modify the protocol to avoid them.

Problem 4.

Order of operation is DSS. Let $p = 11$, $q = 5$, $g = 3$ and $k = 3$. Show that:
 $(g^k \bmod p) \bmod q \not\equiv (g^k \bmod q) \bmod p$

Problem 5.

Explain why sender authentication implies data integrity. Explain why data integrity does not imply sender authentication.

Problem 6.

Suppose Alice wants to use Bob’s public key in order to encrypt data for him (and/or to check his signatures). She can use one of the following protocols. Which is better? Why?

Protocol 1	Protocol 2
<ol style="list-style-type: none">1. get a copy of Bob’s certificate2. using CA’s public key verify the signature on Bob’s certificate3. check for expiration4. check for revocation5. extract and use Bob’s public key	<ol style="list-style-type: none">1. get a copy of Bob’s certificate2. check for expiration3. using CA’s public key verify the signature on Bob’s certificate4. check for revocation5. extract and use Bob’s public key

Problem 7.

Suppose you have two PK certificates from Alice and Bob. Today (03/09/2007) you get a signed message from Alice dated 7/8/2006 and a signed message from Bob dated 10/12/2006. Alice PK certificate expired on 1/1/2007 while Bob certificate was revoked on the same day. Can you trust the message from Alice? Can you trust the message from Bob?

Problem 8.

A CRL is sometimes described as “negative” or “black” list since only revoked certificates are listed. A “positive” or “white” list would consist contain only good (not revoked) certificates. Can you think of any incentive for wanting to use a “positive” list instead of a “negative” list? Otherwise, describe why a “positive” list would not provide any benefits over a “negative” list.