

# 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

SOLUTION:

The reflection attack is as follow:

1. A to E: Hi I'm Alice
- 1\*: E to A: Hi I'm Bob
- 2\*: A to E:  $R_a$
- 2 : E to A:  $R_a$
- 3 : A to E:  $E(K, R_a), R_a'$
- 3\*: E to A:  $E(K, R_a), R_a'$
- 4 : A to E( $K, R_a'$ )
- 4 : E to A( $K, R_a'$ )

At this point A thinks that she's talking to B while she's actually talking to E.

### Problem 2.

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

SOLUTION:

Suppose the same random  $r$  is re-used to sign  $M_1$  and  $M_2$  so that  $(K, C_1)$  is the signature of  $M_1$  and  $(K, C_2)$  is the signature of  $M_2$ .

We have two equations and two unknown ( $x$  and  $r$ ):

$$\begin{aligned}C_1 * r &= M_1 - K * x \\C_2 * r &= M_2 - K * x\end{aligned}$$

### 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.

SOLUTION:

If Eve records the last part of message 2 and uses it as message one in a subsequent session (either with A or B), she will get back  $K_s$  in clear and will be able to decrypt all the messages that used  $K_s$ .

### Problem 4.

Order of operation is DSS. Let  $p = 11$ ,  $q = 5$ ,  $g = 3$  and  $k = 3$ . Show that:

$$(g^k \bmod p) \bmod q \neq (g^k \bmod q) \bmod p$$

SOLUTION:

$$3^3 \bmod p \bmod q = 27 \bmod 11 \bmod 5 = 5 \bmod 5 = 0$$

$$3^3 \bmod q \bmod p = 27 \bmod 5 \bmod 11 = 2 \bmod 11 = 2$$

### Problem 5.

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

SOLUTION

If the signature can be verified, it means that the received message was actually the one signed by the owner of the signing key, i.e., it has not been altered during transmission.

Data integrity provides assurance of non manipulation of the data, but it doesn't prevent an attacker to forge a message with a valid integrity check.

**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"><li>1. get a copy of Bob’s certificate</li><li>2. using CA’s public key verify the signature on Bob’s certificate</li><li>3. check for expiration</li><li>4. check for revocation</li><li>5. extract and use Bob’s public key</li></ol>	<ol style="list-style-type: none"><li>1. get a copy of Bob’s certificate</li><li>2. check for expiration</li><li>3. using CA’s public key verify the signature on Bob’s certificate</li><li>4. check for revocation</li><li>5. extract and use Bob’s public key</li></ol>

SOLUTION:

Protocol 2 is better because it avoids verifying the signature if the contract has expired. In resource constrained devices, like PDAs or smartphones, difficult computations like signature verification might take a long time.

**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?

SOLUTION:

The date on a message doesn’t imply that the message was actually signed on that date. Because messages were received before expiration/revocation of the certificates, both message are not trustworthy.

**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.

SOLUTION:

See page 385 for a discussion about good lists versus bad lists. Typically, negative lists would have fewer entries than that of a positive list. However, in certain scenarios, this might not be the case. Also, a positive list gives explicit information about a certificate valid status while a negative list only gives implicit. This might be preferable at times.