Cryptology I (spring 2014) Prof. Dr. Dominique Unruh

Exercise Sheet 7

Out: May 22, 2014 Due: May 29, 2014

This is the last homework. Notice that the time for this homework is only one week.

Problem 1: Symbolic cryptography

In the following, we will investigate protocols that use both symmetric and asymmetric encryption (in the symbolic model). We model messages as follows: A, B are names of participants (known to everyone). pk_A, pk_B are the public keys of A, B (known to everyone). A ciphertext encrypted with public key pk_X is written $penc(pk_X, m)$. We use symbols K_i for symmetric keys, and we write $senc(K, m)$ for the symmetric encryption of m using K. We use R_i for random values (nonces). We write $\hat{R}_i$ and $\hat{K}_i$ for additional random values/keys belonging to the adversary. We write (x, y) for pairs.

(a) Write down the deduction rules that model the capabilities of the adversary (i.e., those that do not depend on the protocol). You may assume that no party is corrupted (that is, all public keys belong to honest participants and the adversary cannot decrypt messages encrypted with one of these public keys).

(b) Consider the following protocol:

- Alice and Bob share a random value R_1. Alice has a secret value R_0 that he wishes to send to Bob.
- Alice picks a symmetric key K_1 and sends $penc(pk_B, (K_1, R_1))$ to Bob.
- After checking that the message from Alice contains the right value R_1, Bob picks a key K_2 and sends $senc(K_1, K_2)$ to Alice.
- Alice sends $senc(K_2, R_0)$ to Bob.

Write down the deduction rules corresponding to this protocol. (Assume that only a single instance each of Alice and of Bob runs, and that the network between Alice and Bob is insecure in the sense that the adversary can intercept and replace messages.)

(c) Write down a grammar M that describes the terms the adversary can deduce. That is, if $\vdash t$, the t should match M. (Here $\vdash$ is the deduction relation corresponding to the deduction rules you wrote down in (a) and (b).)

For each rule, explain (shortly) why all terms in the conclusion of the rule match M if all terms in the preconditions of the rule match M.

(d) Show that the protocol is secure, i.e., that $\nvdash R_0$.

(e) **[Bonus question]** Consider the following variation of the protocol from (b):

- Alice has a secret value R_0 that he wishes to send to Bob.
- Alice picks a symmetric key K_1 and sends $penc(pk_B, K_1)$ to Bob.
- Bob picks a key K_2 and sends $senc(K_1, K_2)$ to Alice.
- Alice sends $senc(K_2, R_0)$ to Bob.

(The only difference is that now the shared random value R_1 is not included in the first message from Alice.)

Write down the deduction rules corresponding to this protocol (analogous to (b)).

(f) **[Bonus question]** Show that for the deduction rules from (a) and (e), we have $\vdash R_0$ (i.e., the protocol is insecure). Write down the derivation tree of $\vdash R_0$.[1]

Hint: If you do not see the solution, you can try to produce a grammar of terms as in (c). This will help you to see why R_0 can be deduced.

(g) **[Bonus question]** Explain why the attack found in (f) does not work if Bob answers to each message only once. (I.e., when getting several messages of the form $penc(pk_B, K)$ for some K, he responds only to the first one.) Explain why it is difficult to prove the security in this case using the methods we discussed.

[1]The package `mathpartir` is useful for writing deduction rules and derivation trees in LaTeX. `http://cristal.inria.fr/~remy/latex/`