Cryptography, winter 2015/16

MICHAEL NÜSKEN, SIMON SCHNEIDER

9. Exercise sheet
Hand in solutions until Saturday, 16 January 2016, 12:00

Exercise 9.1 (DH security). (6 points)

Prove: 6

Theorem. *If the Diffie-Hellman key exchange is ROR-POA secure then the Decisional Diffie-Hellman problem is hard.*

Exercise 9.2 (Another key exchange). (6+10 points)

Let's try to realize `https://www.youtube.com/watch?v=U62S8SchxX4`.

Assume that you have an encryption scheme $\Pi = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ with the additional commutativity property that $\mathrm{Dec}_a(\mathrm{Enc}_b(y)) = \mathrm{Enc}_b(\mathrm{Dec}_a(y))$ for any keys a, b, message y.

Consider the following key exchange mechanism:

$$
\begin{array}{lcl}
a \leftarrow \mathrm{KeyGen}(1^\kappa) & & b \leftarrow \mathrm{KeyGen}(1^\kappa) \\
x_1 \leftarrow \mathrm{Enc}_a(x) & \xrightarrow{x_1} & x_2 \leftarrow \mathrm{Enc}_b(x_1) \\
x_3 \leftarrow \mathrm{Dec}_a(x_2) & \xleftarrow{x_2} & \\
 & \xrightarrow{x_3} & x_4 \leftarrow \mathrm{Dec}_b(x_3)
\end{array}
$$

We want to discuss whether this is a secure key exchange, whether it is ROR-POA secure, ...

(i) The One-Time Pad has the desired commutativity property. Show that the derived key exchange is insecure. 4

(ii) What about AES-CTR? Can we use that, do we have correctness? Is the derived key exchange secure? 2

(iii) Can you find an encryption scheme for which that key exchange is ROR-POA secure under suitable assumption on the security of the encryption scheme? +10

Exercise 9.3 (Key exchange plus data transport). (4+8 points)

4+8

Let Π be a key-exchange protocol, and $(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ be a private-key encryption scheme. Consider the following interactive protocol Π' for encrypting a message: first, the sender and receiver run Π to generate a shared key k. Next, the sender computes $c \leftarrow \mathrm{Enc}_k(m)$ and sends c to the other party, who decrypts and recovers m using k.

(i) Formulate a definition for IND-POA (or LOR-CPA) security appropriate for this interactive setting.

(ii) Prove that if Π is ROR-POA secure and $(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ is IND-POA (or LOR-CPA) secure, then Π' satisfies your definition.