

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

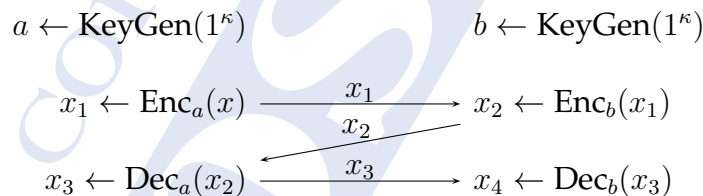
Theorem. *If the Diffie-Hellman key exchange is ROR-POA secure then the Decisional Diffie-Hellman problem is hard.*

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 $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$ with the additional commutativity property that $\text{Dec}_a(\text{Enc}_b(y)) = \text{Enc}_b(\text{Dec}_a(y))$ for any keys a, b , message y .

Consider the following key exchange mechanism:



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 $(\text{KeyGen}, \text{Enc}, \text{Dec})$ 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 $c \leftarrow \text{Enc}_k(m)$ 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 $(\text{KeyGen}, \text{Enc}, \text{Dec})$ is IND-POA (or LOR-CPA) secure, then Π' satisfies your definition.