Advanced cryptography: Cloud & More, winter 2013/14

MICHAEL NÜSKEN

7. Exercise sheet
Hand in solutions until Sunday, 5 January 2014, 23:59

Exercise 7.1 (IND-CCA security). (8+4 points)

(i) Prove: RSA encryption is not IND-CCA secure. 4

Hint: Use the fact that RSA encryption is deterministic.

(ii) Derive a general rule like: an encryption scheme which ... is not IND-CCA secure. +2

(iii) Prove: ElGamal encryption is not IND-CCA secure. 4

(iv) Derive a general rule like: an encryption scheme which ... is not IND-CCA secure. +2

Exercise 7.2 (ElGamal IND-KOA secure). (16+4 points)

Let $G = \langle g \rangle$ be a cyclic group. In this exercise we prove that ElGamal is IND-KOA secure (or IND-CPA secure, which is the same) if the decisional Diffie–Hellman problem (DDH) is hard in the underlying group G.

Warning: DDH is *not* hard in $\mathbb{Z}_p^\times = \langle g \rangle$. +4

To avoid this, you may use a group $\langle g \rangle \subseteq \mathbb{Z}_p^\times$ with $\ell = \mathrm{ord}(g)$ an odd prime. Well, or an elliptic curve.

Let $\mathcal{A}$ be an IND-KOA attacker of ElGamal. That is $\mathcal{A}$ is called with a key A; interacts with a challenger $\mathcal{C}$ by sending two messages $x_1, x_2 \in G$ and receiving a challenge $(B, E) \in G^2$ (if the challenger is fair this is an encryption $(B, x_i \cdot K)$ of x_i for $i \in \{0, 1\}$ with $B = g^b$ and $K = A^b$); and finally outputs $j \in \{0, 1\}$. We call $\mathcal{A}$ successful (under a fair challenger) if $i = j$.

(i) Give an algorithm that calls $\mathcal{A}$ and solves the DDH in G. That is an algorithm with input $A = g^a$, $B = g^b$, and $C \in G$ and output TRUE if $C = g^{ab}$ and FALSE otherwise. 4

Hint: The algorithm should call $\mathcal{A}$ with a certain input, simulate the challenger (receive x_1, x_2 from $\mathcal{A}$ and send back a challenge), and output TRUE or FALSE depending on the output of $\mathcal{A}$.

4 (ii) Prove that your algorithm returns TRUE on input $A = g^a$, $B = g^b$, $C = g^{ab} \in G$ if $\mathcal{A}$ is successful.

4 (iii) Prove that your algorithm returns FALSE on input $A = g^a$, $B = g^b$, $C \neq g^{ab} \in G$ with probability $1/2$.

Hint: Choose the challenge randomly.

2 (iv) Assume $\mathcal{A}$ succeeds with probability p. What is the success probability of your algorithm if for an input $A = g^a$, $B = g^b$, C, in half of all cases $C = g^{ab}$ holds?

2 (v) Put everything together: Assume that DDH is hard in G and conclude that ElGamal is IND-KOA secure.

Exercise 7.3. (4+4 points)

4+4 How can we make ElGamal encryption IND-CCA secure?

Hint: Prevent the attacker from using the decryption oracle for homomorphically modified ciphertexts.

Exercise 7.4 (Key exchange security). (12+14 points)

6+2 (i) Is the Diffie Hellman key exchange secure wrt. to the tentative security model from the course?

6+2 (ii) Does the model exclude Man-in-the-middle attacks?

+10 (iii) Modify the model so that it excludes the Man-in-the-middle.