Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

4. Exercise sheet
Hand in solutions until Monday, 6 May 2013, 10:00

Exercise 4.1 (Repetition: Security notions). (12 points)
Recall the following notions from your Cryptography lecture (or read Chapter 7 in Stinson (2006) or Chapter 10 in Bellare & Goldwasser (2008)): There are several levels of security

- Unbreakability (UB or UBK),
- Universal Unforgeability (UUF; also called selective unforgeability),
- Existential Unforgeability (EUF);

along with different means for an attacker:

- Key-Only Attack (KOA),
- Known Signature Attack (KSA),
- Chosen Message Attack (CMA).

Pairing an adversarial goal with an attack model defines a security notion, e.g. EUF-CMA.

(i) Give a short description of each security level and each attack. Does security in one notion imply security in some other notions? Picture the implications in a suitable way.

(ii) Consider the ElGamal signature scheme with a cyclic group $G$. Assume that the discrete logarithm problem for $G$ (DL$_G$) is hard, i.e. it is hard to compute $a$ from $g^a$ where $g$ is a generator of $G$. Decide for each of the 9 security notions whether the scheme is

- secure,
- not secure, or
- the answer is unknown.

Give for each claim a short hint or quote.

(iii) What can you say, if you assume that DL$_G$ is easy?
Exercise 4.2 (ElGamal encryption is IND-KOA secure if . . .). (18 points)

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

(i) Describe the ElGamal encryption scheme (in your words).

Let $A$ be an IND-KOA attacker of ElGamal. That is $A$ is called with a key $A$; interacts with a challenger $C$ 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 $A$ successful (under a fair challenger) if $i = j$.

(ii) Give an algorithm that calls $A$ 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.

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

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

(iv) 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.

(v) Assume $A$ 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?

(vi) Assume that DDH is hard in $G$ and conclude that ElGamal is IND-KOA secure.

References
