Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

5. Exercise sheet
Hand in solutions until Sunday, 8 May 2011, 23:59

Exercise 5.1 (Powers and goals for attackers of encryption schemes).

(10 points)

You have encountered several levels of security:

- Unbreakability (UBK),
- Indistinguishably (IND),
- Non-Malleability (NM);

along with different means for an attacker:

- Key Only Attack (KOA),
- non adaptive Chosen Ciphertext Attack (CCA_1),
- adaptive Chosen Ciphertext Attack (CCA_2).

Pairing an adversarial goal with an attack model defines a security notion, e.g. IND-CCA_2. Note that in the public key scenario a chosen plaintext attack, CPA, is the same as a key only attack, KOA.

Consider the ElGamal encryption scheme with a cyclic group $G = \langle P \rangle$. Assume that the decisional Diffie-Hellman Problem for G (DDH_G) is hard, ie. given $P, A, B, C \in G$ it is hard to decide whether $a \cdot b = c$ where $A = aP$, $B = bP$, $C = cP$.

(i) Decide for each of the 9 security notions whether the scheme is $\boxed{6}$

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

$\boxed{2}$ (ii) What can you say if you assume that DDH_G is easy?

$\boxed{2}$ (iii) What can you say if you assume that the discrete logarithm problem DL_G is easy?

Prove your answer if you can. If not at least argue or cite. Use the connections between the security notions to simplify your arguments.

Exercise 5.2 (Security of public key encryption schemes). (4+2 points)

$\boxed{2}$ (i) What notion of security (of the above mentioned) can be achieved at most by a deterministic encryption scheme. Prove your answer.

$\boxed{2}$ (ii) What notion of security (of the above mentioned) can be achieved at most by a homomorphic encryption scheme. Prove your answer.

$\boxed{+2}$ (iii) Give an example of an IND-CCA$_2$ secure encryption scheme. Describe how it works and state the assumption under which it is proved to be secure.

Exercise 5.3 (Secure ElGamal?). (6 points)

What can you say about IND-CCA$_2$ security of the following modified versions of ElGamal?

$\boxed{2}$ (i) First permute the message M by an arbitrary fixed permutation $\pi\colon G \to G$. Then encrypt $\pi(M)$ with ElGamal.

$\boxed{2}$ (ii) After encrypting the message M with ElGamal, sign the temporary key $T = tP$ with a secure signature scheme sig. Then the output of the new encryption scheme is $(T, M + tA, \text{sig}(T))$.

$\boxed{2}$ (iii) Compute the temporary key $T = tP$ and encrypt the message M with a secure symmetric encryption scheme where tA is used as key.

Remark. *It is self-understood that each claim needs a proof. At least you should argue why it is correct.*