The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

6. Assignment

(Due: Monday, 21 May 2012, 13^{00})

Exercise 6.1. Security notions (4 points)

You have encountered several levels of security.

- Unbreakability,
- One-wayness,
- Indistinguishability (IND),
- Non-Malleability,

along with different means for an attacker

- Key-Only Attack,
- Non-adaptively Chosen Ciphertext Attack,
- Chosen Ciphertext Attack (CCA2).

Pairing an adversarial goal with an attack model defines a *security notion*, e.g. IND-CCA2.

Consider the RSA encryption scheme. Assume that Factoring is hard and decide for each of the 12 security notions whether the scheme is

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

What can you say, if you assume that Factoring is easy? Use the connections between the security notions to simplify your argument.

Exercise 6.2 (Coin flip protocol)**.** Consider the following protocol for two parties A and B to flip a fair coin.

1. A trusted party T publishes her public key pk (for a randomized asymmetric encryption scheme).
2. A chooses a random bit b_A, encrypts it using pk, and announces the ciphertext c_A to B and T.
3. B acts symmetrically and announces a ciphertext $c_B \neq c_A$.
4. T decrypts both c_A and c_B, and the parties XOR the results to obtain the value of the coin.

(i) (2 points) Argue that if B follows the protocol honestly, the final value of the coin is uniformly distributed, even if A is dishonest.

(ii) (3 points) Assume the parties use ElGamal encryption (where the bit b is encoded as the group element g^b). Show how a dishonest B can bias the coin to take the value 0; in fact, to any distribution he likes.

(iii) (4 points) Suggest what type of encryption scheme would be appropriate to use here. Define an appropriate notion of security and prove that your suggestion achieves this definition.

Exercise 6.3 (Diffie-Hellmann and ElGamal)**.** Given a group $G = \langle g \rangle$, you are to reduce the Diffie-Hellman Problem (DH) to deciphering ElGamal encryptions with key only. The idea is to use the inputs $A = g^a$ and $B = g^b$ to DH in the ElGamal encryption system. Choose $y \xleftarrow{\$} G$, and submit (y, A) to the attacker $\mathcal{A}$.

(i) (3 points) If $\mathcal{A}$ correctly returns the decipherment x, how do you determine g^{ab} from it?

(ii) (3 points) State the reduction in detail, and show that the distribution of the submissions to $\mathcal{A}$ equals the distribution of ElGamal encryptions.

(iii) (2 points) Letting $\tau_{\mathcal{A}}$ and $\sigma_{\mathcal{A}}$ denote the running time and success probability of $\mathcal{A}$, derive bounds on the corrsponding quantities for the reduction.

(iv) (1 points) Conclude that if DH is hard, then ElGamal encryptions are secure against deciphering with key only.