Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

4. Exercise sheet
Hand in solutions until Sunday, 1 May 2011, 23:59

Exercise 4.1 (Amplification – or: A little bit better than guessing is enough).
(8+4 points)

For a fixed encryption scheme consider an probabilistic algorithm $\mathcal{A}$ that computes the least significant bit of the plaintext x for a given ciphertext y. Think, for example, of the RSA encryption scheme. Assume the success probability of $\mathcal{A}$ is slightly better than guessing, ie.

$$p = \text{prob}(\mathcal{A}(y) = \text{bit}_0(x)) > \frac{1}{2},$$

where $\text{bit}_0(x)$ denotes the least significant bit of x, ie. $\text{bit}_0(x) := x \,\text{rem}\, 2$. Consider a new algorithm $\mathcal{B}$ which calls $\mathcal{A}$ m times and outputs the majority of the outputs of $\mathcal{A}$ — returning failure in the event of a draw.

(i) Prove that $\boxed{4}$

$$\text{prob}(\mathcal{B}(y) = \text{bit}_0(x)) > \sum_{m/2 < i \leq m} \binom{m}{i} p^i (1-p)^{m-i}$$

and give a simple — but still useful — lower bound for the sum. (Hint: Chernoff)

(ii) How many repetitions m do you need for $p = 0.6, 0.7, 0.8$ in order to guarantee $\text{prob}(\mathcal{B}(y) = \text{bit}_0(x)) > 0.9$? $\boxed{4}$

(iii) Let $p = \frac{1}{2} + \frac{1}{n}$. Determine a number of repetitions such that $\boxed{+4}$

$$\text{prob}(\mathcal{B}(y) = \text{bit}_0(x)) > 1 - e^{-cn}$$

for some constant $c > 0$.

Exercise 4.2 (Security notions). (6 points)

You have encountered several levels of security:

- Unbreakability (UB),
- Universal Unforgeability (UUF),
- Existential Unforgeability (EUF);

along with different means for an attacker:

- Key-Only Attack (KOA),
- Non-adaptive Chosen Message Attack (NACMA),
- Chosen Message Attack (CMA).

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

6 Consider the ElGamal signature scheme with a cyclic group G. Assume that the discrete logarithm problem for G (DL_G) is hard, ie. it is hard to compute x from g^x 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.

What can you say, if you assume that DL_G is easy?

Exercise 4.3 (Security reduction). (4 points)

4 For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is secure in the EUF-CMA model. Does that imply that the hash function is collision resistant? Prove your answer.

Exercise 4.4 (Hardcore bit for the discrete logarithm). (0+6 points)

Let G be a cyclic group of even order d with a generator g, and let $\omega = g^{d/2}$. Furthermore suppose that an algorithm for computing square roots in G is known. Let BitZero be a probabilistic algorithm that, given g^i, computes the least significant bit of i in expected polynomial time.

The square root algorithm is given g^{2i} with $0 \le i < d/2$ and computes either the square root g^i or the square root ωg^i. Let Oracle be a probabilistic expected polynomial time algorithm that decides, which of the two square roots is g^i. [Note: This could be done by an oracle for the second least significant bit, $\mathrm{bit}_1(i)$, of the discrete logarithm of g^i, where $0 \le i < d$.]

(i) Formulate an algorithm for the discrete logarithm that uses at most polynomially many calls to Oracle and otherwise uses expected polynomial time. (*Recall:* The algorithm gets as input g^i and should compute the discrete logarithm $\mathrm{dlog}_g(g^i) = i$ with $0 \le i < d$.) $\boxed{+4}$

(ii) What implications does this have on the security of ElGamal encryption scheme? $\boxed{+2}$