Advanced Cryptography — Midterm Exam

Serge Vaudenay

2.5.2017

- duration: 3h
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade

1 DDH Solver in a Group of Order with a Small Factor

We consider a family of cyclic groups G_s generated by some element g_s, where s is the security parameter. The group has order n_s which is divisible by some $m_s > 1$. (In the rest of the exercise, the subscript s is omitted for clarity.) We assume there is a polynomially bounded (in terms of s) algorithm to implement the multiplication in G. We further assume that m is polynomially bounded. The purpose of this exercise is to solve the Decisional Diffie-Hellman (DDH) problem in G.

Q.1 Construct a subgroup H of G with order m.

Q.2 Construct a surjective group homomorphism f from G to H with a polynomially bounded complexity (in terms of s). Describe the algorithm that implements f and prove its complexity.

Q.3 Construct a discrete logarithm algorithm in H of polynomial complexity (in terms of s). Describe the algorithm and prove its complexity.

Q.4 Deduce a DDH distinguisher of polynomial complexity with large advantage. Compute the advantage.

2 MAC vs PRF

In what follows, we consider a function F from $\{0,1\}^{k_s} \times \mathcal{D}_s$ to $\{0,1\}^{\tau_s}$, where s is a security parameter. (For simplicity, s is omitted from notations hereafter.) We can see F either as a Message Authentication Code (MAC) or as a Pseudo Random Function (PRF). By default, we consider chosen message attacks and existential forgeries for the security of MAC functions.

Q.1 Give the following definitions. What does it mean for F to be a secure MAC? What does it mean for F to be a secure PRF?

Q.2 If F is a secure PRF and $2^{-\tau}$ is negligible (in terms of s), prove that it is a secure MAC.

Q.3 If $2^{-\tau}$ is not negligible (in terms of s), prove that F is not a secure MAC. Describe an attack and analyze its complexity.

Q.4 Let $0^\tau = (0, \ldots, 0) \in \{0,1\}^\tau$. We assume that $2^{-\tau}$ is negligible. Given F (which is from $\{0,1\}^k \times \mathcal{D}$ to $\{0,1\}^\tau$), we consider $G(K, x) = (F(K, x), 0^\tau)$ from $\{0,1\}^k \times \mathcal{D}$ to $\{0,1\}^{2\tau}$.

Q.4a If F is a secure MAC, prove that G is a secure MAC.

Q.4b Prove that G is not a secure PRF, even is F is a secure PRF. Describe an attack and analyze its complexity.

3 Distribution in a Subgroup

We consider two odd prime numbers p and q and $g \in \mathbf{Z}_p^*$ an element of order q. Let D_1 be the uniform distribution in $\langle g \rangle$. Let D_2 be the uniform distribution in $\mathbf{Z}_p^*$.

Q.1 Compute d, the statistical distance between D_1 and D_2.

Q.2 Construct a distinguisher between D_1 and D_2 with advantage d.

Q.3 We assume that 2 has an order bigger than q in $\mathbf{Z}_p^*$. We assume that $p > 2^n$ has n bits and we consider a binary encoding $\mathsf{bin} : \{0,1\}^n \to \mathbf{Z}_p^*$ such that

$$\mathsf{bin}(b_1, \ldots, b_n) = 1 + \sum_{i=1}^{n} b_i 2^{i-1}$$

We use the textbook Diffie-Hellman key exchange to produce a random key K with distribution D_1 between Alice and Bob, following which Alice encrypts a message $x \in \{0,1\}^n$ by sending $y = \mathsf{bin}(x) \times K \bmod p$. Prove that if $x = (b, 0, \ldots, 0)$ where b is uniformly distributed in $\{0,1\}$, we can make a decryption attack in ciphertext-only mode. Propose a countermeasure.

4 Distinguishers for 3-Round Feistel Schemes

In this exercise, we consider a 3-round Feistel scheme with round functions F_1, F_2, F_3. The input is a pair $x = (x_l, x_r)$ and the output is a pair $y = (y_l, y_r)$. We call x_l and x_r the left input and the right input, respectively. We call y_l and y_r the left output and the right output, respectively. We define

$$z = x_l \oplus F_1(x_r) \quad , \quad y_r = x_r \oplus F_2(z) \quad , \quad y_l = z \oplus F_3(y_r)$$

where $\oplus$ denotes the bitwise exclusive OR. All values are n-bit strings. We assume that F_1, F_2, F_3 are independent uniformly distributed random functions.

Q.1 In the following subquestions, we consider distinguishers between the Feistel scheme and a uniformly distributed random function over $2n$-bit strings which are limited to q chosen input queries.

Q.1a Construct a distinguisher with advantage roughly $\frac{q^2}{2}2^{-n}$.
HINT: Consider a distinguisher making q chosen inputs $x = (x_l, a)$ for a fixed value a and q different values x_l, getting $y = (y_l, y_r)$ and expecting to find two outputs sharing the same y_r. Make a decision based on the obtained input-output pairs.

Q.1b Give an upper bound for the advantage of any distinguisher limited to q queries.

Q.2 In this question, we consider a stronger security notion. The adversary has access to the encryption oracle (chosen plaintext) and to the decryption oracle (chosen ciphertext). We consider distinguishers between the Feistel scheme and a uniformly distributed random permutation over $2n$-bit strings which are limited to q chosen plaintext or ciphertext queries.

We consider the following distinguisher:

select a nonzero $\delta \in \{0,1\}^n$ arbitrarily
pick $x = (x_l, x_r) \in \{0,1\}^{2n}$ at random
set $x' = (x_l \oplus \delta, x_r)$
query with input x and x' and get $y = (y_l, y_r)$ and $y' = (y'_l, y'_r)$
set $y'' = (y_l \oplus \delta, y_r)$
query with output y'' and get $x'' = (x''_l, x''_r)$
take a decision based on x, y, x', y', x'', y''

Complete the last step to get a very good advantage and estimate it.