Cryptography and Security — Midterm Exam

Serge Vaudenay

10.11.2022

- duration: 1h45
- no documents allowed, except one 2-sided sheet of handwritten notes
- 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
- answers should not be written with a pencil

1 Expected Ciphertext Length for Perfect Secrecy

Let $\mathcal{M}$ be a plaintext domain of size $\#\mathcal{M} \geq 2^n$. We define a random plaintext $X \in \mathcal{M}$ of distribution $\mathcal{D}_X$ and a random key $K \in \mathcal{K}$ of distribution $\mathcal{D}_K$. We assume that the support of $\mathcal{D}_X$ is $\mathcal{M}$. Let $\mathsf{Enc}/\mathsf{Dec}$ be a cipher offering *perfect secrecy* for the distributions $\mathcal{D}_X$ and $\mathcal{D}_K$. We assume that the ciphertext $Y = \mathsf{Enc}_K(X)$ is a bitstring of finite length. That is, $X \in \mathcal{M}$, $K \in \mathcal{K}$, and $Y \in \{0,1\}^*$. We denote by $|Y|$ the length of the bitstring Y. The objective of this exercise is to lower bound the expected length of a ciphertext $E(|\mathsf{Enc}_K(x)|)$ for any fixed $x \in \mathcal{M}$ and a random $K \in \mathcal{K}$.

Q.1 In the following subquestions, we consider X uniformly distributed in $\mathcal{M}$ and $k \in \mathcal{K}$ fixed. We define $Y = \mathsf{Enc}_k(X)$.

Q.1a For any i, prove that $\Pr[|Y| \leq i] \leq 2^{i+1-n}$.
HINT: start by proving $\Pr[|Y| = i] \leq 2^{i-n}$.

Q.1b Prove that

$$E(|Y|) = (n-1)\Pr[|Y| \leq n-1] + \sum_{i=n}^{+\infty} i \Pr[|Y| = i] - \sum_{i=0}^{n-2} \Pr[|Y| \leq i]$$

Q.1c Prove that $E(|Y|) \geq n-2$.

Q.2 In the following subquestions, we consider X uniformly distributed in $\mathcal{M}$ and we assume that $K \in \mathcal{K}$ follows the distribution $\mathcal{D}_K$. We define $Y = \mathsf{Enc}_K(X)$.

Q.2a Prove that $E(|Y|) \geq n-2$.

Q.2b Prove that the cipher provides perfect secrecy for X uniform in $\mathcal{M}$.
Hint: invoke a theorem from the course.

Q.2c Prove that for any $x \in \mathcal{M}$, $E(|\mathsf{Enc}_K(x)|) \geq n-2$.

2 DDH Modulo *pq*

We consider a probabilistic polynomial-time algorithm $\mathsf{Setup}(1^\lambda) \to (\mathsf{pp}, n, g)$ which takes a security parameter λ and generates a cyclic group of order n and generator g, together with the public parameters pp which are used to define the group operations. We recall the DDH problem based on Setup:

$\mathsf{DDH}(\lambda, b)$

$\mathsf{Setup}(1^\lambda) \to (\mathsf{pp}, n, g)$
pick $x, y, z \in \mathbf{Z}_n$ uniformly
if $b = 1$ **then** $z \leftarrow xy$
$X \leftarrow g^x$, $Y \leftarrow g^y$, $Z \leftarrow g^z$
$\mathcal{A}(\mathsf{pp}, n, g, X, Y, Z) \to t$
return t

The advantage of the adversary $\mathcal{A}$ playing this game is

$$\mathsf{Adv}_{\mathcal{A}}(\lambda) = \Pr[\mathsf{DDH}(\lambda, 1) \to 1] - \Pr[\mathsf{DDH}(\lambda, 0) \to 1]$$

We have seen in class that the DDH problem is easy if n has any small factor (larger than 1). In this exercise, we wonder what happens if $n = pq$ with p and q large primes. In a "Diffie-Hellman spirit", the group is public and we assume that p and q are public too (hence, provided in pp).

Q.1 In this question, we assume that n has a small prime factor p (to give an idea: a number of $10 \log_2 \lambda$ bits). In the following subquestions, we construct a probabilistic polynomial-time adversary $\mathcal{A}$ with advantage larger than $\frac{1}{2}$.

Q.1a Given a polynomial-time algorithm which takes n as input and find a prime factor p of $10 \log_2 \lambda$ bits, assuming that n has $c.\lambda^\alpha$ bits, for some constants c and α. Precisely estimate its complexity in terms of λ.

Q.1b Given $w = \frac{n}{p}$, show that it is easy to check if Z^w is the solution to the computational Diffie-Hellman problem with instance (X^w, Y^w) in the subgroup generated by g^w. Assume that T is the complexity of a group multiplication. Precisely estimate its complexity in terms of λ and T.

Q.1c By using the previous questions, construct a polynomial-time adversary $\mathcal{A}$, give its complexity in terms of λ and T and show that it has an advantage in the DDH game close to 1.

Q.2 Let m, p, and q be primes such that $p \neq q$ and pq divides $m - 1$. Let $h \in \mathbf{Z}_m^*$ be random and uniformly distributed. Prove that $h^{\frac{m-1}{p}} \bmod m = 1$ and $h^{\frac{m-1}{q}} \bmod m = 1$ are two independent events of probability $\frac{1}{p}$ and $\frac{1}{q}$ respectively.

Q.3 Given a constant c, we let $f(\lambda) = c.\lambda^3$ be the required bitlength of a modulus m. Construct $\mathsf{Setup}^*(1^\lambda) \to ((m, p, q), n, g)$ with $\mathsf{pp} = (m, p, q)$: a probabilitstic polynomial-time algorithm which generates three prime numbers m, p, q such that m is of $f(\lambda)$ bits, p and q are different and of 2λ bits, a number n such that $n = pq$ and n divides $m - 1$, and also $g \in \mathbf{Z}_m^*$ which is of order n. Analyze its complexity heuristically.

Q.4 Let Setup_1^* be defined by

$\mathsf{Setup}_1^*(1^\lambda)$

$\mathsf{Setup}^*(1^\lambda) \to ((m, p, q), n, g)$
$g_1 \leftarrow g^q \bmod m$
return (m, p, g_1)

We define Setup_2^* similarly. Prove that if DDH is hard for Setup^*, then DDH is hard for Setup_1^* and for Setup_2^*.