Cryptography and Security — Midterm Exam

Serge Vaudenay

30.10.2024

- 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 Perfect Secrecy Except Message Length

We consider the set of finite bitstrings $\{0,1\}^*$. Given a string s, we denote by $|s|$ the length of s (i.e. the number of bits). We denote by $\perp$ a special symbol which is not an element of $\{0,1\}^*$ and which represents an exception in computation. A *cipher* $C = (X, K, \mathsf{Enc}, \mathsf{Dec})$ is defined by random variables X and K in their respective domains $\mathcal{X} \subseteq \{0,1\}^*$ and $\mathcal{K} \subseteq \{0,1\}^*$, a function $\mathsf{Enc} : \mathcal{K} \times \mathcal{X} \to \{0,1\}^*$, and a function $\mathsf{Dec} : \mathcal{K} \times \{0,1\}^* \to \mathcal{X} \cup \{\perp\}$, such that for any $x \in \mathcal{X}$ and any $k \in \mathcal{K}$, we have $\mathsf{Dec}(k, \mathsf{Enc}(k, x)) = x$. We denote $Y = \mathsf{Enc}(K, X)$. In the Shannon model, X and K are independent.

Q.1 Recall what it means for C to provide perfect secrecy for X of support $\mathcal{X}$.

Q.2 Can C provide perfect secrecy in the Shannon model for X of support $\mathcal{X} = \{0,1\}^*$? Why?

Q.3 In practice, we want to be able to encrypt a message X of arbitrary length but we want to have a length-preserving cipher, i.e. such that $|\mathsf{Enc}(k, x)| = |x|$ for any $x \in \mathcal{X}$ and $k \in \mathcal{K}$. Justify why we want to encrypt messages of arbitrary length and to have a length-preserving cipher. (There are many good answers for this.)

Q.4 We consider a random variable L which models what leaks about X. We assume that L can be easily deduced from Y. Formally define the notion of "perfect secrecy except for the leakage of L".

Q.5 Construct a cipher providing perfect secrecy except for the leakage of $L = |X|$ for any X of support included in $\{0,1\}^*$. Prove that it provides perfect secrecy except for the leakage of $L = |X|$.
HINT: we can leave the Shannon model.

2 Diffie-Hellman as a Group Action

A group action by a group G on a set E is a function α with input $(a, u) \in G \times E$ returning an output $\alpha(a, u) \in E$. (We assume that G is multiplicatively denoted.) It must satisfy $\alpha(1, u) = u$ and $\alpha(ab, u) = \alpha(a, \alpha(b, u))$ for any $a, b \in G$ and $u \in E$. For simplicity, we denote $\alpha(a, u) = a * u$. Given a, the function $\alpha_a : u \mapsto a * u$ is a permutation of E. Actually, we can see the group action as a group homomorphism from G to the the group of permutations over E (i.e., the symmetric group of E). We say that the action is transitive if for any pair $u, v \in E$, there exists a such that $a * u = v$.

We define an algorithm $\mathsf{Setup}(1^\lambda)$ which essentially defines a transitive group action by a group of order n, with n of length depending on λ, and which returns some group action parameters, n, and a fixed element $w \in E$.

Q.1 Assume that E is a multiplicative group of prime order q in which we removed the neutral element. Show that $a * u = u^a$ defines a group action from a group G to E and that there is a set $Z \subseteq \mathbf{Z}$ and a surjective function $\mathsf{rep} : Z \to G$ such that $\mathsf{rep}(xy) = \mathsf{rep}(x)\mathsf{rep}(y)$ for all $x, y \in Z$. (For $\mathsf{rep}(xy)$, the multiplication is the one in $\mathbf{Z}$. For $\mathsf{rep}(x)\mathsf{rep}(y)$, the multiplication is the one in G.) Precisely define Z, rep, and G, and give its order n.

Q.2 Prove that it is transitive.

Q.3 Rewrite the Diffie-Hellman protocol with that group action.

Q.4 Reformulate the discrete logarithm problem in terms of group action.

3 Square Root Modulo a Prime p s.t. $p \bmod 8 = 5$

Let p be a prime number.

Q.1 When $p \bmod 4 = 3$, recall a method to compute the square root of a quadratic residue modulo p.

Q.2 When $p \bmod 4 \neq 3$, what values can $p \bmod 8$ be?

Q.3 In the $p \bmod 8 = 5$ case, prove that if x is a quadratic residue in $\mathbf{Z}_p^*$, then $x^{\frac{p+3}{8}}\theta^{\frac{p-1}{4}}$ is a square root of either x or $-x$ modulo p, for any $\theta \in \mathbf{Z}_p^*$.

Q.4 In the $p \bmod 8 = 5$ case, let θ be a non-quadratic residue modulo p. Prove that if x is a quadratic residue in $\mathbf{Z}_p^*$, then either $x^{\frac{p+3}{8}}$ or $x^{\frac{p+3}{8}}\theta^{\frac{p-1}{4}}$ is a square root or x.