Cryptography and Security — Final Exam

Ioana Boureanu and Serge Vaudenay

15.1.2013

- duration: 3h
- no documents are allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will *not* answer any technical question during the exam
- if extra space is needed, the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to write your name on every sheet!

1 Modular Arithmetic

Let p and q be two different odd prime numbers and $n = pq$.

Q.1 Show that p is invertible modulo q and that q is invertible modulo p.
In what follows, $\alpha = q \times q'$ where $q' \in \mathbf{Z}$ is the inverse of q modulo p, and $\beta = p \times p'$ where $p' \in \mathbf{Z}$ is the inverse of p modulo q. We define $f(x, y) = \alpha x + \beta y$, where $x, y \in \mathbf{Z}$.

Q.2 For $x \in \{0, \ldots, p-1\}$ and $y \in \mathbf{Z}$, what is $f(x, y) \bmod p$?

Q.3 Which concept of the course corresponds to the function f?

Q.4 Show that $f(1, 1) = 1 + n$.

Q.5 Give the largest common factor of all numbers of the form $f(x, x) - x$ for $x \in \mathbf{Z}$.

Q.6 Let $x \in \mathbf{Z}_n$. Using f, list all the square roots of $x^2 \bmod n$ in $\mathbf{Z}_n$.

Q.7 Assuming that $p < q$, that $x \in \{0, \ldots, p-1\}$, $y \in \{0, \ldots, q-1\}$, that $x \neq y$, let $z = f(x, y)$. Give an algorithm to compute p and q when given z, x, and n.

2 A MAC Based on DES

We construct a (bad) MAC as follows: given a message m and a key K, we first compute $h = \mathsf{trunc}(\mathsf{SHA1}(m))$ where trunc maps onto the keyspace of DES (assume that the preimages by trunc have the same size). Then, we compute $c = \mathsf{DES}_h(K)$ which is the authentication code.

Q.1 How many bits of entropy are used from m to compute c?

Q.2 How many random messages do we need in order to see the same authentication code twice with a good probability? (Explain.)

Q.3 Describe a chosen-message forgery attack against the MAC which uses only one chosen message.

3 Secure Communication

We want to construct a secure communication channel using cryptography.

Q.1 List the three *main* security properties that we need *at the packet level* to achieve secure communication. For each property, explain what it means and say which cryptographic technique can be used to obtain it.

Q.2 Assuming that packet communication is secure, list two extra properties (other than key establishment) that we need in order to secure *an entire session*, and how to ensure these properties.

Q.3 How to secure a key establishment to initialize the secure channel? Give two solutions.

4 On Entropies

We define $\mathsf{nextprime}(x)$ as the smallest prime number p such that $p \geq x$. We want to sample a prime number greater than 40 as follows: given a random number R with uniform distribution between 1 and 16, we compute $X = \mathsf{nextprime}(40+R)$. For X secret, we consider the problem of finding X.

Q.1 Give the distribution of all possible values for X.

Q.2 Compute $H(X)$, the Shannon entropy of X and the value $c = \frac{1}{2}\left(2^{H(X)}+1\right)$.
Reminder: $H(X) = -\sum_x \Pr[X = x] \log_2 \Pr[X = x]$

Q.3 Compute $G(X)$, the guesswork entropy of X, and compare it with c. What do we deduce?
Reminder: $G(X)$ is the lowest expected complexity in the following game. A challenger samples X, keeps it secret, and answers questions as follows. The adversary, trying to guess X, can ask as many questions as he wants of the form "is the secret X equal to x?" for any value x. The complexity is the number of questions until one answer is "yes".

Q.4 By sampling two independent prime numbers X and Y following the same distribution, what is the probability that $X = Y$?

5 Pedersen Commitment

Let p and q be two prime numbers such that q divides $p-1$. Let g be an element of $\mathbf{Z}_p^*$ of order q. Let h be in the subgroup of $\mathbf{Z}_p^*$ generated by g but different from the neutral element. Given two numbers x and r, we define a commitment scheme by $\mathsf{commit}(x;r) = g^x h^r \bmod p$.

The protocol works as follows. We assume that the sender wants to commit to a message x to a receiver. In the commitment phase, the sender selects r at random, compute $y = \mathsf{commit}(x;r) = g^x h^r \bmod p$ and sends y to the receiver. In the opening phase, the sender sends some values and the receiver does some computation. (Formalizing further this phase is subject to a question.)

Q.1 Fully formalize what the sender sends to the receiver in *the opening phase* and which computation *the receiver is doing*.

Q.2 Let X and R be two independent random variables with values in $\mathbf{Z}_q$ such that R is uniformly distributed in $\mathbf{Z}_q$. Let $Y = \mathsf{commit}(X;R)$. Show that Y is uniformly distributed in the subgroup of $\mathbf{Z}_p^*$ generated by g.
Hint: use h in the subgroup of $\mathbf{Z}_p^*$ generated by g.

Q.3 With the sames settings, show that X and Y are independent.

Q.4 Given p, q, g, h, show that computing $x, r, x', r' \in \mathbf{Z}_q$ such that $\mathsf{commit}(x; r) = \mathsf{commit}(x'; r')$ and $x \neq x'$ is equivalent to computing $a \in \mathbf{Z}_q$ such that $h = g^a \bmod p$.

Q.5 Finding $a \in \mathbf{Z}_q$ such that $h = g^a \bmod p$ is called the discrete logarithm problem. Assuming that solving the discrete logarithm problem is hard, show that commit defines a *hiding* and *binding* commitment scheme.