Cryptography and Security — Midterm Exam

Ioana Boureanu and Serge Vaudenay

30.11.2012

- duration: 1h45
- no documents is 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 put your name on every sheet!

1 Message Encoding in a Subgroup of $\mathbf{Z}_p^*$ of Prime Order

In what follows, p is an odd prime number which can be written $p = 2q + 1$ with q being another odd prime number.

Q.1 What is the order of $\mathbf{Z}_p^*$?
List all factors of this number.
What are the orders of 1 and -1 in $\mathbf{Z}_p^*$?

Q.2 If $x \in \mathsf{QR}_p$ is such that $x \neq 1$, show that x generates QR_p.
Hint: What is the order of QR_p?

Q.3 Let QR_p be the set of all quadratic residues of $\mathbf{Z}_p^*$. Show that for all $x \in \mathbf{Z}_p^*$, we have $x \in \mathsf{QR}_p$ if and only if $x^{\frac{p-1}{2}} = 1$ in $\mathbf{Z}_p$.

Q.4 Given $x \in \{1, \ldots, q\}$, show that the cardinality of $\{x, -x\} \cap \mathsf{QR}_p$ is 1.
Hint: is -1 in QR_p?

Q.5 Given $x \in \{1, \ldots, q\}$, let $\mathsf{map}(x)$ be the only element between x and $-x$ which is a quadratic residue. Show that map is an one-to-one mapping between $\{1, \ldots, q\}$ and QR_p.

2 Arithmetic Modulo 101 and 99 999

Let $m = 101$, $n = 99\,999$, $a = 4\,499\,955$ and $b = 5\,599\,945$.

Q.1 For $N = 10^k \pm 1$, $k \geq 1$, give a method to compute by hand the modulo N reduction of a big decimal number.

Q.2 Compute $a \bmod m$, $a \bmod n$, $b \bmod m$, and $b \bmod n$.

Q.3 Deduce the *lowest* positive multiple of n which is equal to 2 modulo m.

3 Every Day I'm Shuffling

Let n and r be integers. We consider the vector space $\mathsf{GF}(2)^n$ over $\mathsf{GF}(2)$. A vector $x = (x_1, \ldots, x_n)$ has n binary coordinates $x_1, \ldots, x_n$. We denote by $\oplus$ the addition of vectors. We denote by $x \cdot y$ the inner product between two vectors x and y. I.e., $x \cdot y = x_1y_1 +$

$\cdots + x_n y_n \bmod 2$. Finally, given two vectors x and y, we define the function $\max(x, y)$ giving the one vector among x and y which represents the binary expansion of the largest integer. (Assume that bits written from left to right, i.e. x_n is the least significant bit.)

Given $2r$ vectors $K_1, \ldots, K_r, L_1, \ldots, L_r$, we denote $KL = (K_1, \ldots, K_r, L_1, \ldots, L_r)$ and we define the encryption $E_{KL}(X)$ of a vector X with key KL by the following algorithm:

proc $E_{KL}(X)$
1: **for** $i = 1$ to r **do**
2: $\quad X' \leftarrow K_i \oplus X$
3: $\quad \hat{X} \leftarrow \max(X, X')$
4: $\quad$ if $L_i \cdot \hat{X} = 1$ then $X \leftarrow X'$
5: **end for**
6: return X

Q.1 Let j be the smallest index such that the jth component of K_i is 1. In iteration i, we consider the values of X and $\hat{X}$ in step 3. Show that $\hat{X} = X \oplus (1 - X_j)K_i$.

Q.2 In iteration i, we let X_{new} be the value of X after step 4 and still consider the same X and $\hat{X}$. Show that $X_{\mathsf{new}} = X \oplus (L_i \cdot \hat{X})K_i$.

Q.3 Deduce that for whatever KL, x, and y, we have $E_{KL}(x \oplus y) \oplus E_{KL}(0) = E_{KL}(x) \oplus E_{KL}(y)$.

Q.4 Propose a way to break this symmetric encryption scheme.