Cryptography and Security — Midterm Exam

Serge Vaudenay

11.11.2010

- duration: 1h45
- no documents is allowed
- a pocket calculator is allowed
- communication devices are not allowed
- answers to every 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 Birthday Computation

In 2010, January 1st was a Friday. My birthday last Spring was a Monday. If every months had 30 days, it would have been the 5th day of a month. When was it?

2 The Group $\mathbf{Z}_{77}^*$

Q.1 Compute $\varphi(77)$.

Q.2 What is the order of 2 in $\mathbf{Z}_{77}^*$?
Hint: invoke Lagrange and try $2^{\frac{\varphi(77)}{p}} \bmod 77$ for all prime factors p of $\varphi(77)$.

Q.3 Is 36 mod 7 a power of 2 in $\mathbf{Z}_7^*$?
If yes, give the power.

Q.4 Is 36 mod 11 a power of 2 in $\mathbf{Z}_{11}^*$?
If yes, give the power.

Q.5 Is 36 a power of 2 in $\mathbf{Z}_{77}^*$?
If yes, give the power.

Q.6 Is there any generator in $\mathbf{Z}_{77}^*$? If yes, give one.
Hint: use a Chinese argument.

3 Vernam playing Dices

We play with 6-face dices. For simplicity, we assume that the faces of a dice are numbers from 0 to 5. Assume that Alice and Bob exchange a sequence $k_1, k_2, \ldots, k_n$ of independent trials with a dice.

Q.1 Given a cipher where X denotes the plaintext, Y denotes the ciphertext, and K denotes the key, recall the definition of perfect secrecy.

Q.2 To encrypt a number X between 0 and 5, they take the next unused k_i number and compute $Y = X + k_i \bmod 6$.
Assuming that dices are unbiased, show that this cipher provides perfect secrecy.

Q.3 An adversary is an algorithm $\mathcal{A}$ taking the ciphertext Y as input and producing a result $\mathcal{A}(Y)$. We say that the adversary wins if $\mathcal{A}(Y) = X$.
Propose an adversary with winning probability $\frac{1}{6}$.

Q.4 We use the same encryption scheme but with a biased dice to draw the k_i's. That is, there is a vector p such that for all i and k, we have $\Pr[k_i = k] = p_k$ where p_k is not necessarily $\frac{1}{6}$.
Assuming that X is uniformly distributed, provide an adversary with optimal winning probability. What is this probability?

Q.5 Assuming that X is not uniformly distributed but that its distribution is known, show that the following adversary has optimal winning probability.

$$\mathcal{A}(y) = \arg\max_x \frac{\Pr[X = x]\Pr[K = y - x]}{\sum_{x'} \Pr[X = x']\Pr[K = y - x']}$$

(Recall that $\arg\max_x f(x)$ denotes the x such that $f(x)$ is maximal. By convention, if there are several we take one of these arbitrarily.)
Hint: given y, consider maximizing $\Pr[X = x|Y = y]$ over x.
Show that its winning probability is

$$p = \sum_y \max_x \Pr[X = x]\Pr[K = y - x]$$

Show that this holds for the generalized Vernam cipher over any group G.
Hint: did we use $G = \mathbf{Z}_6$ so far?

Q.6 As an example, we assume that $\Pr[K = 0] = \frac{1}{6}(1 - \varepsilon)$, $\Pr[K = 5] = \frac{1}{6}(1 + \varepsilon)$, and $\Pr[K = a] = \frac{1}{6}$ for $a = 1, 2, 3, 4$. We also assume that $X \in \{0, 1, 2, 3, 4\}$ with uniform distribution in this set. (Note that X is not uniformly distributed in G.)
Give the $y \mapsto \mathcal{A}(y)$ table of the optimal $\mathcal{A}$ and its winning probability.
Hint: apply the results of Q.5.

Q.7 We now assume that dices are unbiased and that X is distributed in $\{0, 1, 2\}$ with $\Pr[X = 1] = \frac{1}{2}$ and $\Pr[X = 0] = \Pr[X = 2] = \frac{1}{4}$. We assume that we encrypt two independent plaintexts X and X' with this distribution, by using the same key K. We denote by $Y' = X' + K$ the ciphertext corresponding to X'.
Given Y and Y', give an optimal strategy to output x and x'.
Hint: use Q.5 over $\bar{G} = \mathbf{Z}_6^2$ with $\bar{X} = (X, X')$ and some weird distribution for a key $\bar{K}$.
What is its winning probability?