Cryptography and Security — Midterm Exam
Solution

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?

Assign 0 to Friday, 1 to Saturday, 2 to Sunday, 3 to Monday and so on. Also number every day of the year starting with 0 for January 1st. Let x be the number of my birthday. Since it was a Monday, we have $x \bmod 7 = 3$. Since it was the 5th of a month in a calendar with 30 days per month, we have $x \bmod 30 = 4$. We observe that 7 and 30 are coprime. Thanks to the Chinese Remainder Theorem, we can compute $x \bmod 210$. We obtain

$$x \equiv 3 \cdot 30 \cdot (30^{-1} \bmod 7) + 4 \cdot 7 \cdot (7^{-1} \bmod 30) \pmod{210}$$

Since $30 \bmod 7 = 2$ and $2 \times 4 \bmod 7 = 1$, we have $30^{-1} \bmod 7 = 4$. Similarly, since $13 \times 7 = 91$ and $91 \bmod 30 = 1$ we have $7^{-1} \bmod 30 = 13$. Now, we compute

$$x \equiv 3 \cdot 30 \cdot 4 + 4 \cdot 7 \cdot 13 \pmod{210}$$

so $x = 724 \bmod 210 = 94$. Since there are 365 days in a year, we have $0 \leq x < 365$ and $x \bmod 210 = 94$, we have $x = 94$ or $x = 304$. That is, the birthday can either be the 95th or 305th day of the year, which is either April 5th or October 31st. We know that it was in Spring, so it is April 5th.

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

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

Since $77 = 7 \times 11$ *is the complete factorization of* 77*, we have* $\varphi(77) = 6 \times 10 = 60$.

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 $\varphi(77)$.

Due to the Lagrange Theorem, the order of 2 *must be a factor of 60, the order of the group. We have* $60 = 2^2 \times 3 \times 5$ *so we can try all factors of 60. There are* 24 *in total. The order* n *is such that* $2^n \bmod 77 = 1$*. For all* k *such that* nk *divides* 60*, we also have* $2^{nk} \bmod 77 = 1$.
We have $2^{2^2 \times 3} \bmod 77 = 4\,096 \bmod 77 = 15$ *so there is no* k *such that* $nk = 2^2 \times 3$*. Since* n *divides* $2^2 \times 3 \times 5$*, this means that* 5 *divides* n.
We have $2^{2^2 \times 5} \bmod 77 = 67$ *so, by the same argument,* 3 *must divide* n.
We deduce that n *is of form* $2^\alpha \times 3 \times 5$ *with* $\alpha \in \{0, 1, 2\}$*. We have* $2^{3 \times 5} \bmod 77 = 32\,768 \bmod 77 = 43$ *so* $\alpha > 0$.
We have $2^{2 \times 3 \times 5} \bmod 77 = 1$.
So, the order is 30.

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

We have $36 \bmod 7 = 1 = 2^0 \bmod 7$*. So, it is a power of* 2.

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

We have $36 \bmod 11 = 3 = 2^8 \bmod 11$*. So, it is a power of* 2.

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

Let us try a power equal to 0 *modulo* $7-1$ *and to* 8 *modulo* $11-1$*. Let* $e \bmod 6 = 0$ *and* $e \bmod 10 = 8$ *be an equation. Note that* 6 *and* 10 *are not coprime, so we cannot invoke the Chinese remainder theorem. However* $e = 18$ *is clearly a solution. Now, if we compute* $2^e \bmod 77$*, we obtain that it is congruent to* 36 *modulo* 7 *and modulo* 11*. Then, due to the Chinese remainder theorem, we have that* $2^{18} \bmod 77 = 36$.

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

We have $\mathbf{Z}_{77} \approx \mathbf{Z}_7 \times \mathbf{Z}_{11}$ *so* $\mathbf{Z}_{77}^* \approx \mathbf{Z}_7^* \times \mathbf{Z}_{11}^*$*. Since* $\mathbf{Z}_7^* \approx \mathbf{Z}_6$ *and* $\mathbf{Z}_{11}^* \approx \mathbf{Z}_{10}$*, we have* $\mathbf{Z}_{77}^* \approx \mathbf{Z}_6 \times \mathbf{Z}_{10}$ *which is not cyclic. Indeed, for any* $(a, b) \in \mathbf{Z}_6 \times \mathbf{Z}_{10}$*, we have* $30(a, b) = (0, 0)$ *so there is no element of order 60. Therefore, there is no generator.*

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.

Perfect secrecy means that X and Y are independent variables. An equivalent definition is that for all x and y, we have $\Pr[X = x|Y = y] = \Pr[X = x]$.

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.

Take the Abelian group $G = \mathbf{Z}_6$. The cipher is equivalent to the generalized version of the Vernam cipher over the Abelian group G. For any x and Y, we have

$$\Pr[X = x, Y = y] = \Pr[X = x, k_i = y - x \bmod 6] = \Pr[X = x] \Pr[k_i = y - x \bmod 6]$$

so $\Pr[X = x, Y = y] = \frac{1}{6} \Pr[X = x]$. Furthermore,

$$\Pr[Y = y] = \sum_x \frac{1}{6} \Pr[X = x] = \frac{1}{6}$$

Thus, $\Pr[X = x, Y = y] = \Pr[X = x] \Pr[Y = y]$ for all x and y. That is, X and Y are independent. So, the 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 $\frac{1}{6}$.

Let $\mathcal{A}(y)$ pick a random value in $\{0, 1, 2, 3, 4, 5\}$ with uniform distribution. Clearly, $\mathcal{A}(Y)$ and X are independent. Since one is uniform, they match with probability is $\frac{1}{6}$. This is the winning probability.

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?

The best approach is to output the most likely value x for $X = x$ given the value y of $Y = y$. That is,

$$\mathcal{A}(y) = \arg\max_x \Pr[X = x|Y = y]$$

We have $\Pr[X = x|Y = y] = \frac{\Pr[X=x]\Pr[K=y-x]}{\Pr[Y=y]}$. If X is uniformly distributed, this is of form $f(y)\Pr[K = y - x]$. So, $\mathcal{A}(y) = y - k$ where $k = \arg\max_k p_k$. That is, $\mathcal{A}$ hopes that the key is $K = k$ where k is the most likely key and outputs $x = y - k$. The winning probability is $\Pr[K = k] = \max_k p_k = 2^{-H_{\min}(K)}$ where $H_{\min}(K)$ is called the min-entropy of K. That is, $\Pr[\mathcal{A}\ \mathsf{wins}] = \max_k \Pr[K = k]$.

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.

Clearly, the optimal strategy consists of giving one x such that the probability that $X = x$ given the available information $Y = y$ is maximal. Hence, we can consider

$$\mathcal{A}(y) = \arg\max_x \Pr[X = x|Y = y]$$

Now,

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

which is what we wanted to prove.

Show that its winning probability is

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

The winning probability is

$$p = \Pr[\mathcal{A}(Y) = X] = \sum_y \Pr[Y = y]\Pr[\mathcal{A}(y) = X|Y = y]$$

We know that the probability that $\mathcal{A}(y) = X$ given that $Y = y$ is precisely the maximum over x of $\Pr[X = x|Y = y]$. *Thus,*

$$p = \sum_y \Pr[Y = y] \max_x \frac{\Pr[X = x]\Pr[K = y - x]}{\Pr[Y = y]} = \sum_y \max_x \Pr[X = x]\Pr[K = y - x]$$

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

Clearly, our above proofs do not depend on the choice $G = \mathbf{Z}_6$.

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.

We have

$$\begin{aligned}\mathcal{A}(y) &= \arg\max_x \frac{\Pr[X=x]\Pr[K=y-x]}{\sum_{x'}\Pr[X=x']\Pr[K=y-x']}\\ &= \arg\max_{0\leq x<5} \frac{\frac{1}{5}\Pr[K=y-x]}{\sum_{x'=0}^{4}\frac{1}{5}\Pr[K=y-x']}\end{aligned}$$

which is $y-5 \bmod 6$ *if* $y \neq 4$ *or any* $x \in \{0,1,2,3\}$ *if* $y=4$.

y	0	1	2	3	4	5
$\mathcal{A}(y)$	1	2	3	4	$\{0,1,2,3\}$	0

The winning probability is

$$\begin{aligned}p &= \sum_y \max_x \Pr[X=x]\Pr[K=y-x]\\ &= \sum_{y\neq 4} \max_{0\leq x<5} \frac{1}{5}\Pr[K=y-x] + \max_{0\leq x<5}\frac{1}{5}\Pr[K=4-x]\\ &= \frac{1}{6}(1+\varepsilon) + \frac{1}{5}\times\frac{1}{6}\end{aligned}$$

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 $\bar{K}$.

We consider $\bar{G} = \mathbf{Z}_6^2$ *where we encrypt* $\bar{X} = (X, X')$ *with a key of form* $\bar{K} = (K, K)$ *with* K *uniformly distributed over* G*. We apply Q.5, an optimal strategy is defined by*

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

Event $\bar{K} = \bar{y} - \bar{x}$ *has nonzero probability if and only if* $(\bar{y} - \bar{x})_1 = (\bar{y} - \bar{x})_2$*. That is,* $\bar{x}_2 - \bar{x}_1 = \bar{y}_2 - \bar{y}_1$*. We can restrict the sum over all* $\bar{x}'$ *of this form as well. Then the probability over the distribution of* K *is always* $\frac{1}{6}$ *and the ratio simplifies into*

$$\mathcal{A}(\bar{y}) = \arg\max_{\bar{x}_1} \frac{\Pr[\bar{X} = \bar{x}]}{\sum_{\bar{x}'_1} \Pr[\bar{X} = \bar{x}']}$$

where $\bar{x}_2$ *and* $\bar{x}'_2$ *are computed from the above equations. Now,* $\bar{X} = \bar{x}$ *is equivalent to* $X = \bar{x}_1 = x$ *and* $X' = \bar{x}_1 + \bar{y}_2 - \bar{y}_1 = x + y' - y$*. So,*

$$\mathcal{A}(y, y') = \arg\max_{x} \frac{\Pr[X = x, X' = x + y - y']}{\Pr[X' - X = y' - y]}$$

That is,

$$\mathcal{A}(y, y') = \arg\max_{x} \Pr[X = x | X' - X = y' - y]$$

We can then easily compute

$y' - y$	-2	-1	0	1	2
$\mathcal{A}(y, y')$	$(2,0)$	$(1,0)$	$(1,1)$	$(0,1)$	$(0,2)$

Other values for $y' - y$ *are impossible.*

What is its winning probability?

With the same type of computation, the winning probability is

$$p = \sum_{\bar{y}} \max_{\bar{x}} \Pr[\bar{X} = \bar{x}]\Pr[\bar{K} = \bar{y} - \bar{x}] = \sum_{y,y'} \max_{x} \frac{1}{6} \Pr[X = x, X' = x + y' - y]$$

That is,

$$p = \sum_{\delta=-2}^{2} \max_{x} \Pr[X = x, X' = x + \delta]$$

So $p = \frac{1\cdot 1}{4^2} + \frac{1\cdot 2}{4^2} + \frac{2\cdot 2}{4^2} + \frac{2\cdot 1}{4^2} + \frac{1\cdot 1}{4^2}$ *which leads us to* $p = \frac{5}{8}$*.*