

# Cryptography and Security — Midterm Exam

Serge Vaudenay

23.11.2017

- 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 RSA over $\mathbf{Z}_{p^\alpha q^\beta}$

We consider a variant of RSA in which the modulus is selected of form  $n = p^\alpha q^\beta$  and two different large prime numbers  $p$  and  $q$ . As usual, the public key is a pair  $(n, e)$  and the secret key is a pair  $(n, d)$ . We assume that  $\alpha$  and  $\beta$  are two constants in this cryptosystem.

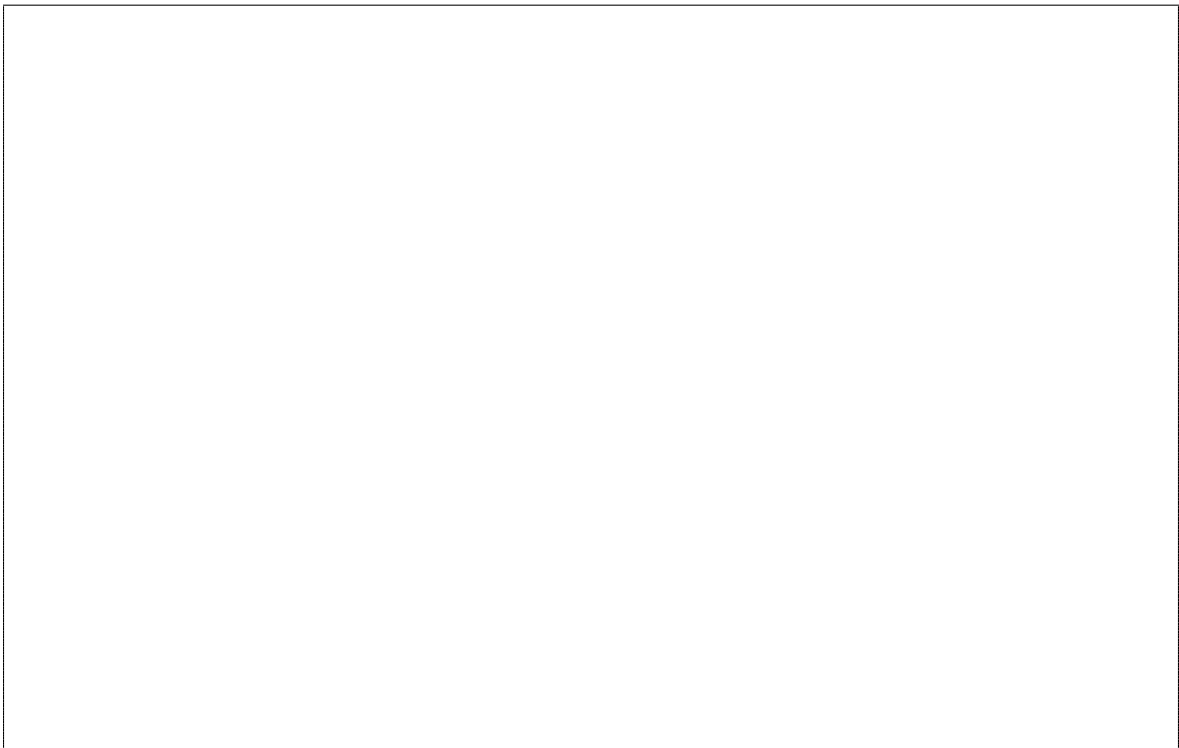
**Q.1** Explain the **encryption algorithm** Enc, the **decryption algorithm** Dec, and the **key generation algorithm** Gen. What **relation** must exist between the public key and the secret key?

**Q.2** Prove that for all  $x \in \mathbf{Z}_n^*$  we have  $\text{Dec}_{n,d}(\text{Enc}_{n,e}(x)) = x$  but that there exist some (rare)  $x \in \mathbf{Z}_n$  such that  $\text{Dec}_{n,d}(\text{Enc}_{n,e}(x)) \neq x$  when  $e > 1$ .

**Q.3** If either  $\alpha = 0$  or  $\beta = 0$ , prove that this cryptosystem is insecure. Describe an attack and show it has a low complexity.



**Q.4** If  $x^2 \equiv y^2 \pmod{n}$ ,  $x \not\equiv y \pmod{n}$ , and  $x \not\equiv -y \pmod{n}$ , formally prove that  $\gcd(x - y, n)$  is a nontrivial factor of  $n$ .



**Q.5** Explain that the ability to compute square roots in  $\mathbf{Z}_n^*$  allows to factor  $n$  efficiently. (Note that we must find  $p$  and  $q$ , not only a non-trivial factor.)



**Q.6** Further prove that the knowledge of any multiple of  $\lambda(n)$  allows to factor  $n$  efficiently.



## 2 A New Meet-in-the-Middle

Let  $x \mapsto C_k(x)$  be a block cipher encryption using a key  $k$  and  $y \mapsto C_k^{-1}(y)$  be the corresponding block cipher decryption. We assume that  $k$ ,  $x$ , and  $y$  live in the space  $\{0,1\}^\ell$ , for a given integer  $\ell$ . The key  $k$  is uniformly distributed. In this exercise, we define new block ciphers using longer keys. We do analysis in a known plaintext attack setting: we assume the adversary gets  $m$  pairs  $(x_i, y_i)$  consisting of a random  $x_i$  and its encryption  $y_i$ . The purpose is to do a key recovery with probability of success close to 1. We say that the attack succeeds if it stops with the correct secret key (and only the correct one) as output. In this exercise, we will look for attacks with a variable  $m$  and study how to select  $m$  for a high success probability in the last question.

**Q.1** For the block cipher  $x \mapsto C_k(x)$ , describe the best possible **known plaintext attack** and its **complexity**. Describe the attack with a pseudocode.

Note: in all questions of the exercise, the complexity is the average time complexity. It is given in terms of number of  $C$  or  $C^{-1}$  evaluations to make, or equivalent computation.

**Q.2** We define  $C'_{k_1, k_2}(x) = C_{k_2}(C_{k_1}(x))$ .  
Find **two functions**  $f$  and  $g$  such that

$$\begin{aligned} \forall k_1, k_2, x \quad f(k_1, x) &= g(k_2, C'_{k_1, k_2}(x)) \\ \Pr_{a, b, k_1, k_2, x} [f(a, x) &= g(b, C'_{k_1, k_2}(x))] = 2^{-\ell} \end{aligned}$$

prove **these properties**, and describe the best possible **known plaintext attack** and its **complexity**. Describe the attack with a pseudocode.

**Q.3** We let  $\star$  designate a group operation in  $\{0, 1\}^\ell$ . We define  $C''_{k_1, k_2, k_3}(x) = C_{k_3}(k_2 \star C_{k_1}(x))$ . Find **two functions**  $f$  and  $g$  such that

$$\begin{aligned} \forall k_1, k_2, k_3, x, x' \quad f(k_1, x, x') &= g(k_3, C''_{k_1, k_2, k_3}(x), C''_{k_1, k_2, k_3}(x')) \\ \Pr_{a, b, k_1, k_2, k_3, x, x'} [f(a, x, x') &= g(b, C''_{k_1, k_2, k_3}(x), C''_{k_1, k_2, k_3}(x'))] = 2^{-\ell} \end{aligned}$$

and show **the first property**. Describe the best possible **known plaintext attack** and its **complexity**. Describe the attack with a pseudocode.

**Q.4** Assume a construction  $x \mapsto \text{Enc}_{k_1, \dots, k_n}(x)$  like the ones in this exercise, i.e. based on the block cipher  $x \mapsto C_k(x)$  and using  $n$  keys  $k_1, \dots, k_n \in \{0, 1\}^\ell$ . Given  $m$  pairs  $(x_i, y_i)$ , **estimate** the probability that there exists no tuple  $(k'_1, \dots, k'_n)$  different from  $(k_1, \dots, k_n)$  such that for all  $i$ , we have  $\text{Enc}_{k'_1, \dots, k'_n}(x_i) = y_i$ . **Explain** how to select a minimal  $m$  so that this probability is high (i.e. very close to 1).

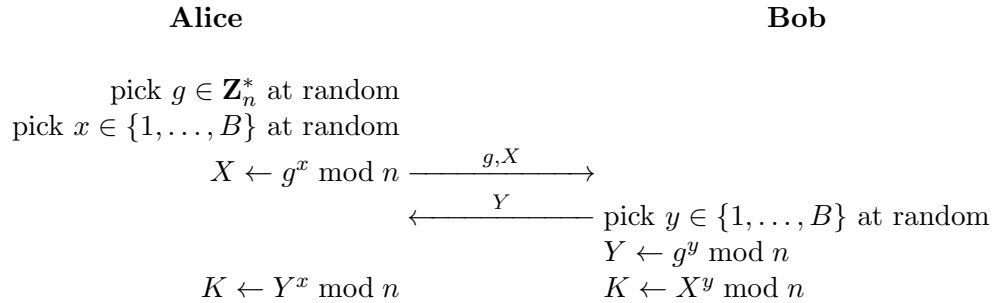
NOTE: We consider “reasonable” constructions  $\text{Enc}_{k_1, \dots, k_n}(x)$ . I.e., there may be weird counterexamples for which the results of this question are different.



### 3 A Variant of Diffie-Hellman in $\mathbf{Z}_n^*$

In this exercise, we want to adapt the Diffie-Hellman protocol in the group  $\mathbf{Z}_n^*$  for  $n = pq$  where  $p$  and  $q$  are two different odd prime numbers which are not known by anyone.

We consider the following protocol:



where  $B$  is an integer which is at least  $n^2$ . We will see that using this protocol is not a good idea.

**Q.1** What is missing in the above variant of the Diffie-Hellman protocol? (Compare to what was explained in class.)

**Q.2** Prove that  $\mathbf{Z}_n^*$  is not cyclic. Then, **explain** why the protocol added  $g$  in the communication.

HINT: Show that  $\mathbf{Z}_n^*$  is isomorphic to  $\mathbf{Z}_{p-1} \times \mathbf{Z}_{q-1}$  and find elements of order two.

HINT<sup>2</sup>: It is not necessary to follow the previous hint.

**Q.3 Explain** why can't we pick  $x, y \in \mathbf{Z}_m$  where  $m$  is the order of  $g$ ? Instead, we pick  $x, y \in \{1, \dots, B\}$  uniformly, where  $B$  is an integer such that  $B \geq n^2$ . Let  $m$  be an integer such that  $m < n$ . **Prove** that for any fixed value  $X$ ,

$$\left| \Pr[x = X] - \Pr[y \bmod m = X] \right| \leq \frac{1}{B}$$

where  $x$  is uniformly distributed in  $\mathbf{Z}_m$  and  $y$  is uniformly distributed in  $\{1, \dots, B\}$ .

**Q.4** Prove that there is a polynomial-time algorithm  $\mathcal{D}$  such that

$$\Pr[\mathcal{D}(g, g^x, g^y, g^{xy}) = 1] - \Pr[\mathcal{D}(g, g^x, g^y, g^z) = 1] \geq \frac{1}{4}$$

where  $g \in \mathbf{Z}_n^*$  is uniform and  $x, y, z \in \mathbf{Z}_m$  are uniform, with  $m$  equal to the order of  $g$  in  $\mathbf{Z}_n^*$ .

HINT: use the Jacobi symbol  $(\cdot/n)$  and reconstruct a distinguisher like the one seen in class. Consider the cases  $(g/n) = +1$  and  $(g/n) = -1$ .