

Family Name:

First Name:

Section:

Security and Cryptography

Midterm Exam

November 12th, 2009

Duration: 1 hour 45 min

This document consists of 12 pages.

Instructions

Documents are *not* allowed apart from linguistic dictionaries.

Electronic devices are *not* allowed, except *simple calculators*.

Answers must be written on the exercises sheet.

This exam contains 3 *independent* exercises.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered.

Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages *stapled*.

1 Modulo 101 Computation

Through *all* this exercise, we will let $p = 101$.

1. Show that p is a prime number.

What is the order of \mathbf{Z}_p^* ?

2. If $x = \sum_{i=0}^{2\ell-1} d_i 10^i$ with $0 \leq d_i < 10$ for all i , show that

$$x \equiv \sum_{i=0}^{\ell-1} (-1)^i (d_{2i} + 10d_{2i+1}) \pmod{101}$$

Deduce an algorithm to compute $x \bmod 101$ easily.

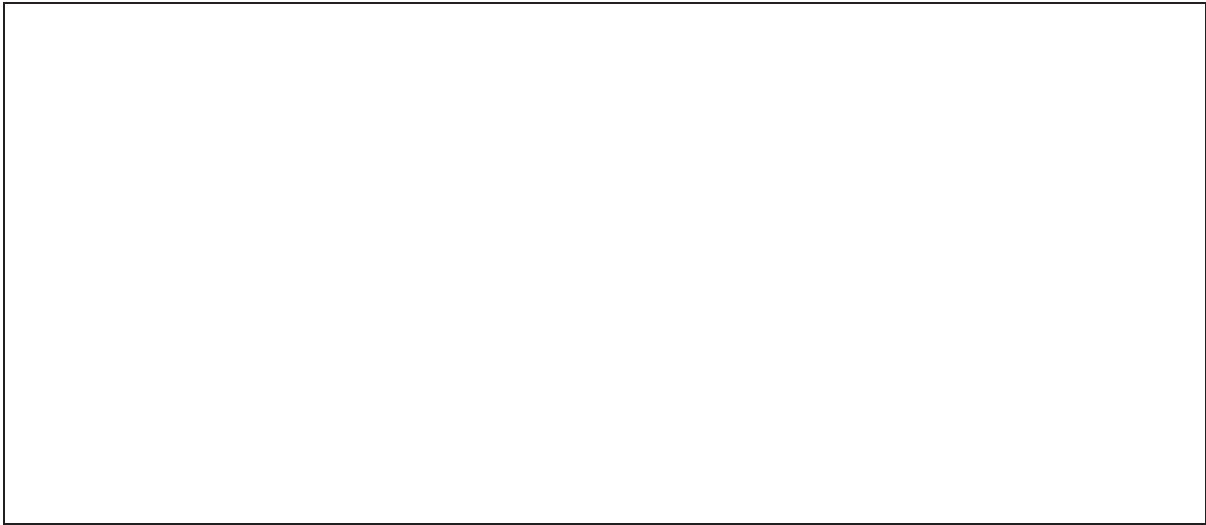
3. Show that every element of \mathbf{Z}_p^* has a unique 7th root and give an explicit formula to compute it (recall that $p = 101$).

Application: Find the 7th root of 2 in \mathbf{Z}_p^* .

4. Given $g \in \mathbf{Z}_p^*$ we let $y = g^{10} \pmod p$. Using 3 multiplications modulo p and 2 tests, give an algorithm with input y to decide whether g is a generator or not (recall that $p = 101$).

Application: show that 2 is a generator.

5. Under which condition is x a quadratic residue in \mathbf{Z}_p^* ?



6. Show that 5 is a quadratic residue in \mathbf{Z}_p^* .



7. Show that 10 is a 4th root of 1 in \mathbf{Z}_p^* .



8. Show that for all $y \in \mathbf{Z}_p^*$ we have that $y^{\frac{p-1}{4}}$ is 10^k for some $k \in \{0, 1, 2, 3\}$.

9. Show that $y^{\frac{p+3}{4}}$ can be written $y \times 10^k$.

10. Deduce that if x is a quadratic residue then either $x^{\frac{p+3}{8}}$ or $10x^{\frac{p+3}{8}}$ is a square root of x . Provide an algorithm to extract square roots in \mathbf{Z}_p^* .

11. Find a square root of 5.

2 Guess my Age

I am human. My age is a prime number. Last year, it was multiple of 5. Next year, it will be multiple of 7. How old am I?

Provide a detailed proof of the result.

3 Authentication, Encryption and the OFB Mode of Operation

In many situations, an encryption scheme does provide confidentiality without authentication. In this exercise, we will look at some constructions and see whether they satisfy the above properties.

1. Recall what are the notions of confidentiality and authenticity.

2. Recall the definition of the Vernam cipher (also known as the one-time pad).

3. Although the Vernam cipher is perfectly secure, there are functions f such that the encryption C of P can be transformed to another one $C' \neq C$ that correctly decrypts to a message $P' = f(P)$ even when P is not known. Show an example for f and this type of attack. Deduce that the Vernam cipher does not provide authentication.

Now, we consider the OFB mode of operation for a block cipher depicted in Fig. 1. The encryption under the key K is denoted E_K . Let $P = P_1 \parallel \dots \parallel P_n$ denote the plaintext and let $C = C_1 \parallel \dots \parallel C_n$ denote the ciphertext.

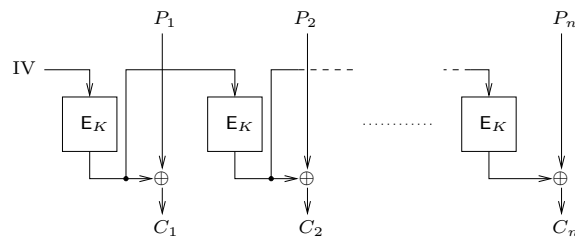
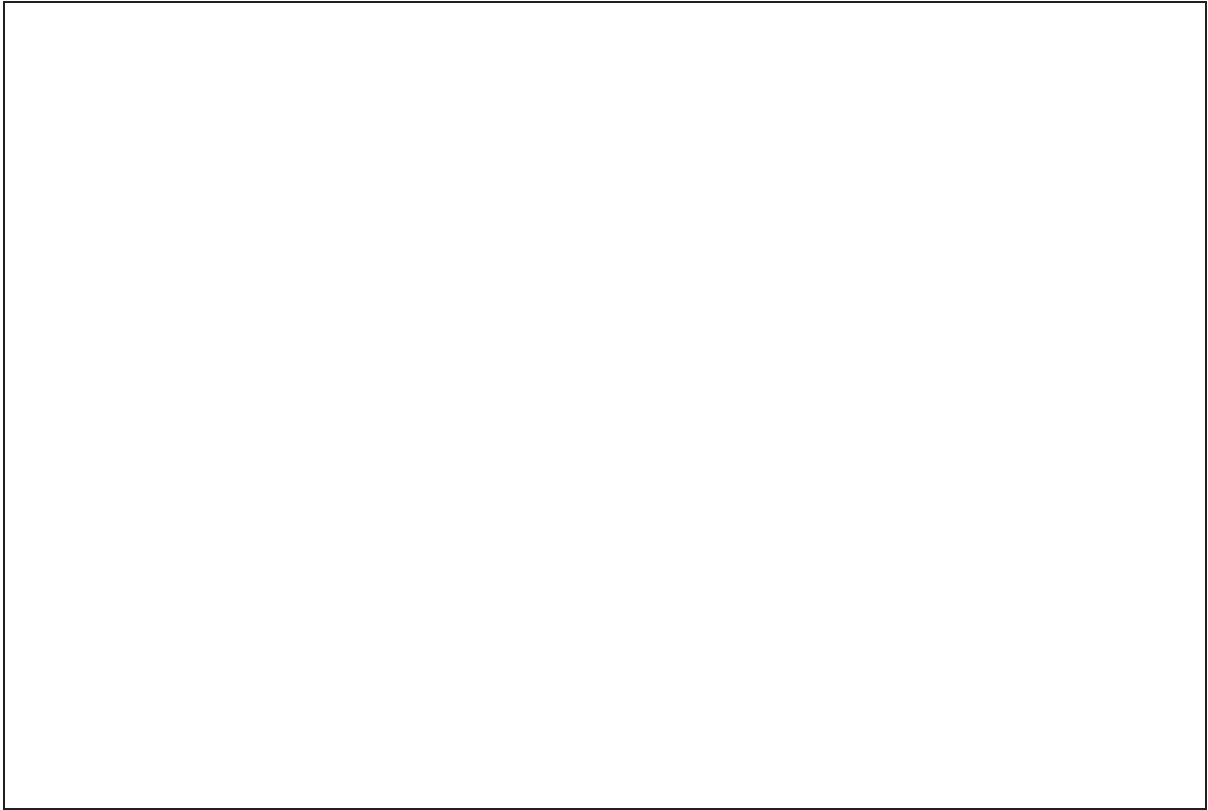


Figure 1: OFB mode

4. Give the name of two block ciphers. What is their block and key sizes?

5. Draw a picture for the decryption in OFB mode.



6. Does the message manipulation attack on the Vernam cipher above still apply?
Explain your answer.



7. Show how to perform a known plaintext attack in order to decrypt transmitted messages when the IV is secret but fixed.

Any attempt to look at
the content of these pages
before the signal
will be severely punished.

Please be patient.