VE475
Introduction to Cryptography

Homework 4

Manuel — UM-JI (Summer 2021)

Non-programming exercises:

- Write in a neat and legible handwriting, or use LaTeX
- Clearly explain the reasoning process
- Write in a complete style (subject, verb and object)

Progamming exercises:

- Write a README file for each program
- Upload an archive with all the programs onto Canvas

Ex. 1 — *Euler's totient*

Let φ be Euler's totient function.

1. Prove that for any prime p, $\varphi(p^k) = p^{k-1}(p-1)$.
2. Prove that for any two coprime integers m and n, $\varphi(mn) = \varphi(m)\varphi(n)$.
3. Using the previous results prove that for any integer $n > 1$, we have
$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$
4. What are the three last digits of 7^{803}?

Ex. 2 — *AES*

Supposed a round 0 AES key is composed of 128 1.

1. What is the key used for round 1?
2. Observe $K(5)$ and express it in term of $K(4)$.
3. Prove that $K(10) = \overline{K(8)}$ and $K(11) = \overline{K(9)}$.

Note: $\overline{x}$ denotes the complement of x, that is 0s become 1s and 1s become 0s.

Ex. 3 — *Simple questions*

1. A plaintext is split into blocks and then encrypted. If one block is corrupted during transmission show that the number of plaintext decrypted incorrectly is one for the ECB mode and two for CBC.
2. Show that using CBC mode with an IV incremented by 1 each time, instead of being random, results in schemes that are not CPA secure.
3. Prove that 2 is a generator of $\mathsf{U}(\mathbb{Z}/29\mathbb{Z})$.
4. Determine $\left(\frac{1801}{8191}\right)$.
5. Let a, b, c be three integers and p be an odd prime not dividing a. Prove that the number of solutions mod p to the equation $ax^2 + bx + c = 0$ is $1 + \left(\frac{b^2-4ac}{p}\right)$.
6. Let p and q be two primes such that $p > q > 2$ and $q-1$ divides $p-1$. Show that if $\gcd(n, pq) = 1$, then $n^{p-1} \equiv 1 \bmod pq$.
7. Let p be an odd prime. Prove that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 3$.

8. Let p be a prime. Prove that if $\left(\frac{a}{p}\right) = 1$, then a is not a generator of $\mathbb{F}_p^*$.

Ex. 4 — *Prime vs. irreducible*

In a commutative ring R, a non-zero, non-invertible element p is said to be *prime* if for any $x, y \in R$,

$$p \mid (x \cdot y) \qquad \text{implies} \qquad p \mid x \quad \text{or} \quad p \mid y. \qquad (*)$$

The goal of this exercise is to prove that this definition generalizes the definition of primality for integers, i.e., $p \in \mathbb{Z}$ is prime if

$$p > 1 \text{ and } a \mid p \qquad \text{implies} \qquad a = 1 \text{ or } a = p. \qquad (**)$$

1. Prove that in an integral domain, i.e. a commutative ring in which the product of two nonzero elements is nonzero, any prime element (in the sense of $(*)$) is irreducible.
2. Prove that in $\mathbb{Z}$ any irreducible integer is prime in the classical sense $(**)$.
3. Prove that for $p \in \mathbb{Z}$, $(**)$ implies $(*)$.
4. Conclude that $(*)$ and $(**)$ are equivalent for integers.

Ex. 5 — *Primitive root mod 65537*

1. Show that $\left(\frac{3}{65537}\right) = -1$.
2. Show that $3^{32768} \not\equiv 1 \bmod 65537$.
3. Conclude that 3 is a primitive root mod 65537.