VE475
Introduction to Cryptography

Homework 10

Manuel — UM-JI (Summer 2020)

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 — *Group structure on an elliptic curve*

Prove proposition 8.7.

Ex. 2 — *Number of points on an elliptic curve*

Let E be the elliptic curve defined by $y^2 = x^3 + 3x + 7$ over $\mathbb{F}_{11}$ and P the point $(8, 9)$ on E.

1. Compute $[2]P$, $[5]P$, and $[10]P$.
2. How many points are on E.
3. List all the points from E.

Ex. 3 — *ECDSA*

In chapter 6 we studied the Digital Signature Algorithm. Search and explain how it can be transposed to elliptic curves. What are the benefits?

Ex. 4 — *BB84*

Describe and explain how the BB84 quantum key distribution protocol works.

Ex. 5 — *Quantum key distribution*

Alice and Bob are given two communication channels: a classical and a quantum one. The quantum channel is isolated from any environment interaction, i.e. the environment does not alter the photons.

1. Describe a simple key agreement protocol where Alice and Bob take advantage of the two channels.
2. Assuming Eve can listen to the information on the classical channel while she can observe and resend photons on the quantum channel, prove that Alice and Bob can detect Eve's interaction.

Ex. 6 — *Simple questions*

1. Given four $n \times n$ matrices U_1, U_2, V_1, V_2, prove that $(U_1 \otimes V_1) \cdot (U_2 \otimes V_2) = (U_1 U_2) \otimes (V_1 V_2)$.
2. Sow that the operator $\otimes$ is bilinear.