VE475
Introduction to Cryptography

Homework 9

Manuel — UM-JI (Summer 2019)

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 — *Missile or not missile...*

In a military office one general, two colonels, and five desk clerks control a powerful missile. As nobody wants the missile to be launched by mistake the following rules are set.

- The general can decide to launch to missile.
- Two colonels can decide to launch to missile.
- Five desk clerics can decide to launch to missile.
- One colonel and three desk clerks can decide to launch to missile.

Describe how a secret sharing scheme can be used to solve this problem.

Ex. 2 — *Asmuth-Bloom Threshold Secret Sharing Scheme*

Explain how to take advantage of the Chinese remainder Theorem in order to build a Threshold Secret Sharing Scheme.

Ex. 3 — *Shamir's Threshold Secret Sharing Scheme*

In the lecture it was presented how to recover the shared secret using the Vandermonde matrix. Explain how this can also be done using the Lagrange's interpolation method. Solve the lecture's example using the new approach.

Ex. 4 — *Simple questions*

1. In a Blakley scheme, suppose Alice and Bob are given the planes $z = 2x + 3y + 13$ and $z = 5x + 3y + 1$. Show that they can recover the secret without the help of Charly.
2. Prove that the determinant of the Vandermonde matrix V of order n is $\det V = \prod_{1 \leq j \leq k \leq n} (x_k - x_j)$.
3. Complete the IDEA survey for VE475 and get 5 bonus marks on the assignments.

Ex. 5 — *Reed Solomon codes*

1. Describe the Reed Solomon code $\mathcal{C}$.
2. Reusing the same notations as in the lecture and the distance of the Reed-Solomon code, give some condition on k such that for any coalition of size 2, it is possible to identify a parent of a descendant of $\mathcal{C}$.