VE475
Introduction to Cryptography

Homework 1

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 — *Simple questions*

1. Alice want to arrange a secret meeting with Bob. Using Caesar cipher she sends the ciphertext EVIRE. Unfortunately brainless Bob has forgotten the secret key they agreed on. Help him finding where to meet Alice.
2. Using a Hill cipher the ciphertext corresponding to *dont* is ELNI. Find the encryption matrix.
3. Let a, b, and n be three positive integers such that $n|ab$ and $\gcd(a, n) = 1$. Prove that $n|b$.
4. Compute $\gcd(30030, 257)$, providing the details of your calculations. Deduce than 257 is prime.
5. Explain why using the same key twice in the OTP is dangerous.
6. Assuming that the best algorithm that determines whether two finite graphs are isomorphic has complexity $2^{O\left(\sqrt{n \log n}\right)}$, what size of graph should be used to be secure?

Ex. 2 — *Vigenère cipher*

1. Research and explain how the Vigenère cipher works.
2. Bob being exhausted he falls asleep on his Vigenère encryption device and sends the same letter repeated several hundred times. The key is a six letters long English word.
   a) Why can Eve suspect that the plaintext is one repeated letter?
   b) How can Eve guess the key length?
   c) How can Eve determine the key?

Hint: no English word of length six is a shift of another English word

Ex. 3 — *Programming*

1. Install the GNU Multi Precision Arithmetic Library (GMP) from https://gmplib.org/ or its fork MPIR available at http://mpir.org/. Note that MPIR has a better support for Windows, although no binaries are officially provided. GMP is available on any modern Linux distribution.
2. Implement the extended Euclidean algorithm.
3. Write a short program that generates two random 4096 bits integers, computes their gcd using the previous implementation and compares it to the result of the corresponding GMP function.