**VE475**
**Introduction to Cryptography**

*Homework 7*
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 —** *Cramer-Shoup cryptosystem*

1. Detail the construction of the Cramer-Shoup cryptosystem.
2. Explain why this cryptosystem is secure even against adapative chosen ciphertext attacks (no formal proof is required, only some basic explanations).
3. Compare this construction to the Elgamal cryptosystem (highlight the similarities and differences).

**Ex. 2 —** *Simple questions*

1. Let $p$ be a prime and $\alpha$ be an integer such that $p \nmid \alpha$. Explain why $h(x) \equiv \alpha^x \bmod p$ is not a good cryptographic hash function.
2. Express $\lfloor 2^{30}\sqrt{i} \rfloor$ for $i = 2, 3, 5$ and 10, in hexadecimal. Compare your results to the constants $K_i$, $0 \leq i \leq 79$, in SHA-1.

**Ex. 3 —** *Birthday paradox*

In this exercise we derive the approximation of the probability of having at least one match in a list of length $r$ over $n$ possible birthdays.

1. Let $f(x) = \ln(1 - x)$ and $g(x) = \ln(1 - x) + x + x^2$. Study the functions $f$ and $g$ over $[0, 1/2]$ and conclude that over this interval

$$-x - x^2 \leq \ln(1 - x) \leq -x.$$

2. Prove that if $r \leq n/2$ then

$$-\frac{(r-1)r}{2n} - \frac{r^3}{3n^2} \leq \sum_{j=1}^{r-1} \ln\left(1 - \frac{j}{n}\right) \leq -\frac{(r-1)r}{2n}.$$

3. Let $\lambda = r^2/(2n)$, and suppose $\lambda \leq n/8$. Prove that

$$e^{-\lambda} e^{c_1/sqrtn} \leq \prod_{j=1}^{r-1} \left(1 - \frac{j}{n}\right) \leq e^{-\lambda} e^{c_2/sqrtn}, \text{ where } c_1 = \sqrt{\frac{\lambda}{2}} - \frac{(2\lambda)^{3/2}}{3} \text{ and } c_2 = \sqrt{\frac{\lambda}{2}}.$$

4. Prove that when $n$ is large and $\lambda$ is a constant less than $n/8$, then

$$\prod_{j=1}^{r-1} \left(1 - \frac{j}{n}\right) \approx e^{-\lambda}.$$

**Ex. 4 —** *Birthday attack*

Suppose we observe 40 licence plates, each ending with a 3-digit number.

1. What is the probability of seeing two plates ending with the same three digits?
2. Assuming we have one ending with 123. What is the probability that one of the 40 license plates observed has the same 3 last digits?
3. Explain how these results relate to how Alice overcomes the birthday attack in chapter 5.

**Ex. 5 —** *Faster multiple modular exponentiation*

Let $\alpha, \beta$, $a, b$ and $n$ be five integers. The most obvious strategy for compute $\alpha^a \beta^b \bmod n$ consists in using the modular exponentiation (Square and Multiply) algorithm (3.38) to compute $\alpha^a \bmod n$, and $\beta^b \bmod n$ and then multiply the results mod $n$.

1. What is the time complexity of this method?
2. Assuming the product $\alpha\beta$ is known, rewrite the square and multiply algorithm, such that at most one multiplication is calculated at each iteration.
3. Suppose $a$ and $b$ are $l$ bits long; how many squaring and multiplications are necessary to compute $\alpha^a \beta^b \bmod n$?
4. Implement the two strategies and compare their speed on large numbers.