INGI2347 : Exercises
Lecture 6 *

Xavier Carpent

March 9, 2015

Exercise 1: Symmetric Encryption Modes (continued)

1. Supposing that we encrypt a hard disk's data using Triple-DES in CBC mode, what must be the disk's size for the collision probability to be higher than 40%? (The birthday paradox indicates that the probability $p(n)$ to find, among n elements of S, two identical elements can be approximated by $p(n) \approx 1 - e^{-\frac{n^2}{2 \cdot S}}$)

Exercise 2: Hash Functions and the Birthday Paradox

The SHA-1 hash function generates 160-bit digital fingerprints which are typically used when signing digital certificates. Suppose we decide to create a digital certificate for each person on Earth (6×10^9 people).

1. Calculate the probability that at least one certificate has the same signature as Gérard Mansoiffe's

`0x11c42333 330debe6 63d722a5 f34388c8 b88520bb`

(in hexadecimal notation), using the fact that $1 - x \approx e^{-x}$, for x close to 0.

2. Calculate the probability that at least two people have identical SHA-1 fingerprints.

Exercise 3: RSA Algorithm

This exercise deals with the details of the RSA public-key algorithm.
1. Detail out the procedure to be followed to generate a pair (public key, private key).

2. Encrypt the message "16" with the public key $(17, 55)$. The calculation can be easily done by hand after noticing that $16^5 \equiv 1 \pmod{55}$.

3. Decrypt the message "8" with this private key $(33, 55)$ in order to retrieve the clear message.

4. Why cannot we encrypt the message "66" with the public key $(17, 55)$?

5. How can we use RSA to compute signature of a message that has an arbitrary length ?

Exercise 4: RSA Vulnerabilities

Previous exercise uses the RSA algorithm as is presented in the introduction to cryptography manuals: in practice, we should *never* use it as it is! The RSA algorithm is, in this form, vulnerable to many attacks. To convince ourselves, let us study one amongst them: show that the product of the signatures of two messages (constructed using the same private key) is equal to the signature of the product of the two messages.

Exercise 5: Exhaustive Search for Asymmetric Keys

Knowing that $\pi(n)$, the number of prime numbers smaller than n, can be approached by

$$\pi(n) \approx \frac{n}{\ln n},$$

calculate an approximation of the worst case number of trials that a naive cryptanalyst would require to factorize a 1024-bit RSA public key using an exhaustive factors search.

Exercise 6: Authenticated Encryption and Compression

1. In *authenticated encryption* we want to transmit a message that is both encrypted and authenticated. How to achieve this ?
2. Unrelated to that, if we want to both encrypt and compress a message, in what order should we do it ?