INFO-F-405 : Security
Encryption and ciphers

Some exercises were inspired by exercises from the Security course given by Dan Boneh.

Exercise 1

In order to save space or bandwidth we often use compression algorithms. Suppose you want to use data compression with encryption. How should these two operations be combined? Why?

Exercise 2

Imagine that you have to use a relatively unreliable network i.e., packets often arrive with errors (bit flips) to their destination. Suppose you want to use an error correction code with encryption. How should these two operations be combined? Why?

Exercise 3

Suppose that the probability of wining the lottery is $\frac{1}{10^6}$. What is more likely guessing an AES-128 key on the first try or winning the lottery 5 times in a row? What about winning the lottery 6 times in a row?

Exercise 4

A bank defines an encryption algorithm to encrypt their account numbers. An account number is a 12-digit number, i.e., an element of $\mathbb{Z}_{10^{12}}$. Every time an account number is encrypted, a fresh key is chosen randomly and uniformly from the same set $\mathbb{Z}_{10^{12}}$. The encryption goes as follows:

$$E_k(m) = m + k \pmod{10^{12}} \quad D_k(c) = c - k \pmod{10^{12}}$$

Does this cipher have perfect secrecy?

Exercise 5

Suppose that (E, D) is an IND-CPA secure encryption scheme, i.e., there is no known way of winning the IND-CPA game other than with a probability negligibly close to $\frac{1}{2}$ or with over-astronomical resources. Let the key and plaintext spaces be $\{0,1\}^n$ with $n \geq 128$. Point out the IND-CPA secure schemes in the following list:

- $E'_k(m) = E_k(m)||E_k(m)$
  (+a side-question: will the first and last n bits of $E'_k(m)$ always be equal?)
- $E'_k(m) = E_k(m)||\text{first bit}(m)$
- $E'_k(m) = (\text{last bit}(m) \oplus \text{first bit}(m))||E_k(m)$
- $E'_k(m) = E_k(m)||1$
- $E'_k(m) = k||E_k(m)$
- $E'_k(m) = E_k(m)||(k \oplus 1^n)$
- $E'_{k1,k2}(m) = E_{k1}(m)||E_{k2}(m)$
- $E'_k(m) = E_{0^n}(m)$
- $E'_k(m) = E_k(m)||(m \oplus k)$

For each scheme that is *not* IND-CPA secure, please specify how an adversary can win the IND-CPA game, i.e., what the adversary chooses as plaintexts m_0 and m_1, what are the queries to be made before or after this choice, how the adversary distinguishes between the ciphertexts of m_0 and m_1.

Exercise 6

The Mantin-Shamir attack on RC4 shows that the second byte of keystream has a probability of about $\frac{2}{256}$ of taking value 0 and a probability slightly less than $\frac{1}{256}$ of taking each other value. What is the probability of winning the IND-CPA game when exploiting this property? Give an upper bound on the security strength s of RC4.

Exercise 7

Suppose that Alice would like to send a secret message m that they create together to Charles and Bob. Alice wants to make sure that Bob and Charles decrypt this message together by collaborating, but each one of them should not be able to decrypt the message alone. Suggest several ways of sharing the secret information among people, for each of them list their pros and cons by answering following questions. You can suppose that Alice has a special trusted and secure channel that she can use in order to communicate a key to Bob and to Charles.

- What should Alice do? How should she share a secret key k with Charles and Bob? How would the encryption/decryption would look like?
- Suppose that Alice already shared k with Bob and Charles using a scheme that you've suggested. Now she wants to send other messages to Bob, Charles and David by using the same secret key k in such way that at least two of them should collaborate during the decryption. What kind of information should she give to David? How this scheme could be extended in order to include Eve?