

# Cryptography

*information about the exam*

The exam will have a written form. The exam will consist of some number of questions and short exercises. Below I present some examples (they are in English, but on the exam they will also be written in Italian).

## Questions and exercises

1. **Question** The main reason why DES is currently considered not secure is that:

- A serious weakness in the design of DES has been found.
- The length of the key is too small.
- DES can be broken by a quantum computer.

2. **Exercise** Is the following function negligible or not? (justify your answer)

$$f(n) = \sin(n) \cdot 2^{-n^{1/3}}.$$

3. **Exercise** Suppose you are given a pseudorandom function (or a block-cipher)  $F : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ . Construct a pseudorandom generator  $G : \{0, 1\}^k \rightarrow \{0, 1\}^{100n}$  using  $F$  as a building-block (more precisely: security of  $G$  should be based on the assumption that  $F$  is a pseudorandom function). (just present the construction, without the proof).

4. **Exercise** Calculate  $101^{500} \bmod 2008$ .

5. **Exercise** A common way of strengthening DES is to cascade it three times (it is called *triple DES*). Why the *double* DES is not that popular? (give a one-sentence answer)

6. **Question** In the handbook RSA encryption we always have  $E_{pk}(1) = 1$ . Hence, if the adversary can see that  $C = 1$  then he knows that the plaintext has to be equal to 1. Explain why in the real-life implementations of RSA this is not a problem. (give a one-sentence answer)

7. **Question** What is a *nonce*?

## Answers and solutions

### 1. Answer

- A serious weakness in the design of DES has been found.
- The length of the key is too small.
- DES can be broken by a quantum computer.

2. **Solution** Yes. First, observe that  $|f(n)| \leq 2^{-n^{1/3}}$ . Therefore it suffices to show that  $2^{-n^{1/3}}$  is negligible. To prove we need to show that for every  $c$  there exists  $n_0$  such that for every  $n > n_0$  we have

$$2^{-n^{1/3}} \leq n^{-c}.$$

This follows immediately from the fact that

$$\lim_{n \rightarrow \infty} \frac{2^{-n^{1/3}}}{n^{-c}} = \lim_{n \rightarrow \infty} 2^{c \log_2 n - n^{1/3}} = 0.$$

3. **Solution** This is essentially the *counter mode* for the block ciphers. Define  $G$  as

$$G(K) := (F_K(1) || \cdots || F_K(100)),$$

where  $||$  denotes concatenation, and the numbers  $(1, \dots, 100)$  are padded with zeros to match the block length.

4. **Solution** First observe that  $2008 = 8 \cdot 251$ , and 251 is prime (this can be quickly verified manually). We calculate  $101^{500} \bmod 8$  and  $101^{500} \bmod 251$  separately. First, observe that  $\varphi(8) = 4$  and  $\varphi(251) = 250$ .

- $101^{500} \bmod 8 = 5^{500} \bmod 8$ . Since 5 is relatively prime with 8 we have  $5^4 = 1 \bmod 8$ , and hence (since  $4|500$ ) we get  $5^{500} \bmod 8 = 1$ .
- Since 251 is prime we have  $101^{250} = 1 \bmod 251$ , and hence (since  $250|500$ ) we get  $101^{500} \bmod 251 = 1$ .

Therefore, using the Chinese Remainder Theorem, we get that  $101^{500} \bmod 2008 = 1$

5. **Answer** Because the double encryption can be broken in time  $O(2^n)$  and space  $O(2^n)$  (where  $n$  is the block length), using the *meet in the middle attack*.
6. **Answer** This is not a problem because in the real-life implementations one always encodes a message before encrypting it (for example using the OEAP encoding).
7. **Answer** *Nonce* means *Number Used Once* and is a random number generated by one party and returned to that party to show that a message is newly generated.