Test Pearl 110 — Cryptography

Course 201300070
16 October 2015

Introductory remarks

- This test consists of 7 questions. The points for each question are listed in the left margin.
- The grade is calculated as the total number of points divided by 10, with a minimum of 1,0.
- During the test, you may use one A4 sheet (both sides) with your own notes and a simple calculator.
- Scientific and graphic calculators, laptops, cell phones, books and other materials are not permitted.

---

10 points **Question 1**

(a) Give a short definition of the term "Data Integrity" and state which cryptographic tool can be used to achieve it.

(b) Give a concrete example of a block cipher (if you state a known encryption scheme, then its name suffices).

10 points **Question 2** The One Time Pad encryption scheme is perfectly secure. Give at least 2 requirements on the secret key used in the One Time Pad to achieve perfect security!

10 points **Question 3**

(a) Encrypt the message `EASYPEASY` with the Vigenere cipher using the key `YES`.

(b) Assume that 31 parties want to securely communicate by using secret-key encryption. This implies that they first have to exchange a unique secret key between any two of them. How many secret keys have to be exchanged in total?

15 points **Question 4**

(a) Compute $(12^{3386092} - 88) \bmod 13$ using modular arithmetic (recall that the result needs to be ≥ 0).

(b) Is 6 an element of $\mathbb{Z}_{14}^*$?

(c) Is there a value $x \in \mathbb{Z}$ such that

$$11 \cdot x \equiv 1 \pmod{22} \quad ?$$

If so/not, why/why not? You are not required to compute an explicit solution.

20 points **Question 5**

(a) Suppose that the ciphertext `10111010110` is an encryption of the plaintext message `10000100010` by using a block cipher of length 4 in the OFB-mode (with a properly chosen initialization vector and secret key).
Your task is to construct a valid ciphertext of the message `10110010110`. The resulting ciphertext must be a valid encryption of the given message under the same block cipher in OFB-mode (with same initialization vector and secret key).

NOTE: You don't need to know the concrete details of the used block cipher, nor the used initialization vector and secret key, to solve this task.

(b) Consider the following plaintext message (an 8-bit string)
`11110010`
Encrypt this message in the CBC-mode by using the following 2-bit block cipher

$$\mathsf{E}_k(b_1 b_0) = b_1 b_0 \oplus k$$

with the bit-string $k = 11$ as secret key (note that $b_1 b_0$ denotes an arbitrary 2-bit plaintext message). As initialization vector for the CBC-mode, use the bit-string $IV = 10$.

(Turn page!)

25 points **Question 6** Let $N = 119$ and $e = 5$. Assume that we use $(N,e) = (119,5)$ as the public key in the textbook RSA signature scheme.

(a) Compute Euler's totient function $\varphi(N)$.
(b) Use the extended Euclidean algorithm (it is mandatory to use this algorithm here!) to compute the secret key $d \geq 0$ that corresponds to the public key $(N,e) = (119,5)$.
(c) Is $s = 6$ a *valid* signature on the message $m = 41$ under the public key $(N,e) = (119,5)$ (i.e., does the RSA signature verification algorithm on input $s = 6$, $m = 41$, and $(N,e) = (119,5)$ indeed output "YES")?

10 points **Question 7** Let c and c' be encryptions of messages m and m', respectively, under the RSA encryption scheme with public key (N,e).

(a) Under the assumption that you only know c, c' and the public key (N,e) (so no knowledge on neither the messages m and m', the prime factorization of N, nor the secret key corresponding to (N,e)), compute a valid RSA encryption of the product $m \cdot m'$ under the same public key (N,e).
(b) Verify that your computed ciphertext in part (a) indeed encrypts the message $m \cdot m'$ by showing that it successfully decrypts to this message using the secret key d corresponding to (N,e) (so here, you assume that you know the secret key).

End of this test.