Test Pearl 100 — Cryptography

Pearls of Computer Science (201300070)
6 October 2017, 13:45–14:45
Module coordinator: Maurice van Keulen, Doina Bucur
Instructor: Andreas Peter

- You may use 1 A4 sheet with your own notes for this test, as well as a *simple* calculator
- Scientific or graphical calculators, laptops, mobile phones, books etc. are not allowed. ***Put those in your bag now (with the sound switched off)!***
- Always motivate/explain your answers, unless it is explicitly stated not to!
- Total number of points: 31

12 points **Question 1**

(a) Encrypt the message `CRYPTO` with key `EASILY` using the Vigenère cipher.
(b) What is the main practical drawback of the One-Time-Pad?
(c) Consider the following keyed-function

$$F : \{0,1\}^3 \times \{0,1\}^3 \to \{0,1\}^3 \quad \text{whereas} \quad F(K,x) = K \oplus x.$$

Encrypt the 6-bit message $m = 110011$ using the Feistel cipher with 3 rounds, above keyed-function F, and the round-keys $K_0 = 111$, $K_1 = 010$, and $K_2 = 011$.

(d) Consider the following plaintext message (a 4-bit string)
`1001`
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 $k =$ `01` 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 $IV =$ `11`.

7 points **Question 2**

(*Hint.* Do **not** try to solve any of the following by using the efficient exponentiation modulo N.)

(a) Write down all the elements in $\mathbb{Z}_{16}^*$.
(b) Compute $(25^{2212122} - 2) \mod 13$ using modular arithmetic (recall that the result needs to be ≥ 0).
(c) Let $p = 43$ and $q = 41$ be primes, and $N = pq = 1763$ an RSA-modulus. Compute $1326^{1680} \mod 1763$.

8 points **Question 3** Let $p = 37$, $q = 31$, and $N = pq = 1147$. Assume that we use $(N,e) = (1147,463)$ as the public key in the RSA signature scheme.

(a) Compute Euler's totient function $\varphi(N)$.
(b) Use the extended Euclidean algorithm (it is mandatory to use the table method here!) to compute the secret key $d \geq 0$ that corresponds to the public key $(N,e) = (1147,463)$.
(c) Sign the message $m = 2$ using the RSA signature scheme with the in (b) computed secret key $d \geq 0$ (if you couldn't solve (b), then use the key $d = 11$, which is different from the correct result in (b)!).

4 points **Question 4** Let (N,e_1) and (N,e_2) be two RSA public keys with the same RSA-modulus N but different public exponents $e_1 \neq e_2$ such that $\gcd(e_1,e_2) = 1$. Suppose that you are given the following two ciphertexts of the same message m (the message m is **not** known to you):

$$c_1 = m^{e_1} \mod N \quad \text{and} \quad c_2 = m^{e_2} \mod N.$$

Provide a way to get to the underlying plaintext m by finding integers x and y such that

$$c_1^x \cdot c_2^y \mod N = m.$$