Toets Parel 010 — Cryptografie

20 september 2013

The mark for this test is computed as the sum of all achieved points divided by 10.

☞ **1** *(10 points)* Suppose that the following ciphertext is an encryption of an English message using the Caesar cipher, whereas the underlying plaintext consists of the capital letters (A-Z) only and the letter `S` occurs most often:

`UIJTXBTFBTZ`

Recall that the Caesar cipher is a substitution cipher, where the secret key is a shift of the alphabet (A-Z).

(a) What is the secret key that was used to create the ciphertext (i.e., the number of positions the alphabet was shifted)?
(b) What is the original plaintext message that is concealed in the above ciphertext?

☞ **2** *(20 points)*

(a) Is it correct that the same plaintext blocks encrypt to the same ciphertexts in the OFB-mode of operation for block ciphers? (YES/NO)
(b) Consider the following plaintext message (a 9-bit string)
`111011110`
Encrypt this message in the CBC-mode by using the following 3-bit block cipher

$$\mathsf{E}_k(b_2b_1b_0) = b_2b_1b_0 \oplus k$$

with the bit-string $k = 010$ as secret key (note that $b_2b_1b_0$ denotes an arbitrary 3-bit plaintext message). As initialization vector for the CBC-mode, use the bit-string $IV = 101$.

☞ **3** *(20 points)*

(a) Briefly describe the concept of "hybrid encryption".
(b) Suppose that you want to encrypt one of your holiday photos of file size 60 Byte (= 480 bits) using the One-Time-Pad encryption. What is the required minimal bit-length of your secret key?
(c) Write down all the elements in $\mathbb{Z}_{12}^*$.

☞ **4** *(30 points)* Let $N = 65$ and $e = 7$. Assume that we use $(N,e) = (65,7)$ as the public key in RSA.

(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 $(N,e) = (65,7)$.
(c) Assume that you receive the RSA ciphertext $c = 2$, i.e., an encryption under the public key $(N,e) = (65,7)$. Decrypt this ciphertext with the secret key d that you have computed in part (b) of this question. What is the underlying plaintext message m that $c = 2$ encrypts?

☞ **5** *(10 points)* Assume that Alice uses $(N,e) = (221,5)$ as her public signature key in the textbook RSA signature scheme. Alice is the only person who knows the private signature key d corresponding to (N,e). Now, Alice uses her private key d to sign the message $m = 41$. She sends the resulting signature $s = 6$ together with the message $m = 41$ and her public signature key (N,e) to you.

(a) Write down the general formula for the verification algorithm of the textbook RSA signature scheme.
(b) Is $s = 6$ indeed a *valid* signature on the message $m = 41$ (i.e., does the verification algorithm on input s, m, and (N,e) indeed output "YES")?

(Turn page!)

☞ **6** *(10 points)* Assume that Alice uses the public signature key (N, e) in the textbook RSA signature scheme (no concrete values in this assignment!).

Generate a valid signature $s \in \mathbb{Z}_N^*$ under Alice's private signature key on an arbitrary message $m \neq 1$, **without** using Alice's private signature key. To do so, you can choose this message m yourself (even at random, if you want), but you have to guarantee that $m \in \mathbb{Z}_N^*$, $m \neq 1$, and that you didn't use Alice's private signature key at all!