TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 18 January 2016

Name :

TU/e student number :

Exercise	1	2	3	4	5	6	7	total
points								

Notes: Please hand in this sheet at the end of the exam. You may keep the sheet with the exercises.
This exam consists of 7 exercises. You have from 13:30 – 16:30 to solve them. You can reach 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem requires usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
All answers must be submitted on TU/e letterhead; should you require more sheets ask the proctor. State your name on every sheet.
Do not write in red or with a pencil.
You are not allowed to use any books, notes, or other material.
You are allowed to use a simple, non-programmable calculator without networking abilities. Usage of laptops and cell phones is forbidden.

1. This exercise is about LFSRs. Do the following subexercises for the sequence

$$s_{k+4} = s_{k+3} + s_{k+2} + s_k$$

   (a) Draw the LFSR corresponding this sequence. $\boxed{\text{2 points}}$

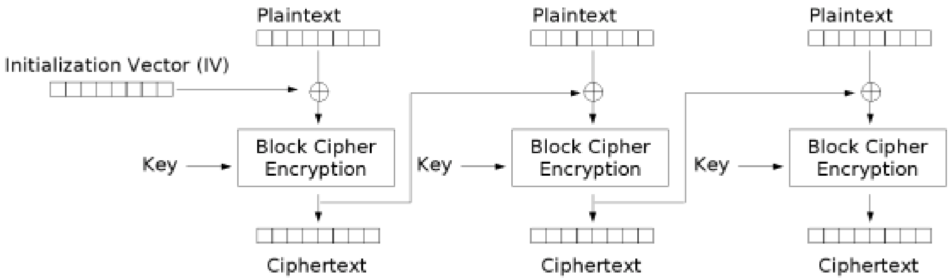
   (b) State the characteristic polynomial f and compute its factorization. You do not need to do a Rabin irreducibility test but you do need to argue why a factor is irreducible. $\boxed{\text{10 points}}$

   (c) For each of the factors of f compute the order. $\boxed{\text{10 points}}$

   (d) What is the longest period generated by this LFSR? Make sure to justify your answer. $\boxed{\text{4 points}}$

   (e) State the lengths of all subsequences so that each state of n bits appears exactly once. $\boxed{\text{8 points}}$

2. This exercise is about modes. Here is a schematic description of the CBC (Cipher Block Chaining) mode.



Cipher Block Chaining (CBC) mode encryption

Let $e_k()$ denote a block cipher of block length b using key k. Let IV be a nonce of length b, let m_i be the b-bit strings holding the message and c_i be the b-bit strings holding the ciphertexts.

Describe how encryption and decryption work, i.e., write c_0, c_1, and a general c_i in terms of IV, m_0, m_1, m_i, and (if necessary) m_j and c_j with $j < i$; and write m_0, m_1, and a general m_i in terms of IV, c_0, c_1, c_i, and (if necessary) other m_j and c_j. $\boxed{\text{10 points}}$

3. This problem is about RSA encryption.

(a) Alice's public key is $(n, e) = (14017, 3)$. Encrypt the message $m = 4321$ to Alice using schoolbook RSA (no padding). 4 points

(b) Let $p = 523$ and $q = 673$. Compute the public key using $e = 5$ and the corresponding private key. 8 points

4. This problem is about the DH key exchange. The public parameters are that the group is $(\mathbb{F}_{1009}^*, \cdot)$ and that it is generated by $g = 11$.

   (a) Compute the public key belonging to the secret key $b = 18$. 4 points

   (b) Alice's public key is $h_a = 648$. Compute the shared DH key with Alice using b from the previous part. 6 points

5. The integer $p = 17$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{17}^*$ with generator $g = 3$. Alice's public key is $h_a = g^a = 14$. Use the Baby-Step Giant-Step method to compute Alice's private key a. Verify your result, i.e. compute g^a. 10 points

6. Bob uses ElGamal encryption to communicate with Alice in some group $\langle g \rangle$, i.e. he encrypts m as $r = g^k$, $c = h_a^k \cdot m$. Alice's public parameters are $p = 8237, g = 3$, and $h_a = 5616$.

   He didn't pass the introduction to cryptology course and doesn't understand symmetric-key crypto, so he uses ElGamal. Even worse, he uses the same nonce k for all his messages $m_1, m_2, m_3, \ldots$.

   You happen to know that he is kind of predictable and always sends `Hi` in his first message, which gets represented as $m_1 = 7 \cdot 26 + 8 = 190$.

   You observe the following ciphertexts: $(r_1, c_1) = (7830, 4537)$, $(r_2, c_2) = (7830, 1647)$. Compute m_2. 10 points

7. Bob has learned his lesson from the attack above and now "upgrades" his nonce generation to one that is very likely not to repeat. Namely he uses $k_i = k_{i-1} + \mathrm{MD5}(i), 1 \leq i$ and chooses k_0 at random.

   Bob generates n ciphertexts to Charlie (public key h_c) as follows:

$$r_i = g^{k_i}, c_i = h_c^{k_i} \cdot m_i, \text{ for } 1 \leq i \leq n.$$

   Assume that Eve knows the last message m_n because Bob always closes his letters with "Yours Bob".

   Provide an abstract formula with which Eve can compute any of the messages m_j for $1 \leq i \leq n-1$. $\boxed{\text{14 points}}$