TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Test Exam for Introduction to Cryptology

Name :

TU/e student number :

Exercise	1	2	3	4	5	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 6 exercises. You have from 13:30 – 16:30 to solve them. You can reach 50 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

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

   (a) Draw the LFSR corresponding this sequence. [1 point]

   (b) The ciphertext is the xor of the message with the output of the LFSR. You know that the plaintext started with `100` and observe ciphertext `011`. Compute the initialization vector.
   The next four output bits are `1010`, compute the corresponding plaintext. [4 points]

   (c) State the associated matrix corresponding to the LFSR state update and compute its order. [3 points]

   (d) State the characteristic polynomial f and compute its factorization. [2 points]

   (e) For each of the factors of f compute the order. [3 points]

   (f) What is the longest period generated by this LFSR? Make sure to justify your answer. [2 points]

   (g) State the lengths of all subsequences so that each state of n bits appears exactly once. [2 points]

2. This exercise is about block ciphers and modes.

   (a) An implementation for DES takes as input an 8-character password and uses that directly as the key for DES. A company deploying the code advises their users to choose an 8-digit PIN (numbers only). How large is the effective key space? How long does a brute-force attack on this key space take?
   Hint: Remember how DES uses the key in the generation of round keys. [3 points]

   (b) Alice and Bob are using DES in ECB mode to encrypt a long message. One ciphertext block gets lost in transmission. How many block is Bob missing after decrypting? [2 points]

   (c) Alice and Bob are using DES in CBC mode to encrypt a long message. One ciphertext block gets lost in transmission. How many block is Bob missing after decrypting? [2 points]

3. This problem is about RSA encryption.

(a) Alice's public key is $(n, e) = (13589, 5)$. Encrypt the message $m = 2801$ to Alice using schoolbook RSA (no padding). [2 points]

(b) Let $p = 653$ and $q = 701$. Compute the public key using $e = 3$ and the corresponding private key. [4 points]

4. Users A, B, and C are friends of S. They have public keys $(e_A, n_A) = (3, 62857), (e_B, n_B) = (3, 64541)$, and $(e_C, n_C) = (3, 69799)$. You know that S sends the same message to all of them and you observe the ciphertexts $c_A = 38014, c_B = 53719$, and $c_C = 46093$. Compute the message. [7 points]

5. 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 $b = 17$. [2 points]

(b) Alice's public key is $h_a = 902$. Compute the shared DH key with Alice using b from the previous part. [3 points]

(c) Alice and Bob keep the prime but change the generator to $g = 1008$. Simulate one round of DH key exchange. Why would you avoid this generator in practice? [3 points]

6. 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 $g = 3$. You observe $h_a = 12$ and $h_b = 14$. What is the shared key of Alice and Bob?
Use the Baby-Step Giant-Step method. [5 points]