TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 19 January 2015

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

$$s_{k+3} = s_{k+1} + s_k$$

   (a) Draw the LFSR corresponding this sequence. | 2 points

   (b) State the associated matrix corresponding to the LFSR state update and compute its order. | 6 points

   (c) State the characteristic polynomial f and compute its factorization. | 4 points

   (d) For each of the factors of f compute the order. | 6 points

   (e) What is the longest period generated by this LFSR? Make sure to justify your answer. | 4 points

   (f) State the lengths of all subsequences so that each state of n bits appears exactly once. | 4 points

2. This exercise is about modes. Describe how the Output Feedback Mode (OFB) mode can be attacked if the IV is not different for each execution of the encryption operation. | 8 points

   For your convenience, here is the definition of OFB:

   Let $e_k()$ be a cipher of block length b using key k. Let x_i, y_i, and s_i be bit strings of length b, and IV be a nonce of length b.
   Encryption (first block): $s_1 = e_k(IV)$ and $y_1 = s_1 \oplus x_1$,
   Encryption (general block): $s_i = e_k(s_{i-1})$ and $y_i = s_i \oplus x_i$ for $i \geq 2$.
   Decryption (first block): $s_1 = e_k(IV)$ and $x_1 = s_1 \oplus y_1$,
   Decryption (general block): $s_i = e_k(s_{i-1})$ and $x_i = s_i \oplus y_i$ for $i \geq 2$.

3. This problem is about RSA encryption.

   (a) Alice's public key is $(n, e) = (14803, 3)$. Encrypt the message $m = 1234$ to Alice using schoolbook RSA (no padding). | 4 points

   (b) Let $p = 659$ and $q = 709$. 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 $(\mathbb{F}^*_{1013}, \cdot)$ and that it is generated by $g = 3$.

(a) Compute the public key belonging to the secret key $b = 33$. | 4 points

(b) Alice's public key is $h_a = 528$. Compute the shared DH key with Alice using b from the previous part. | 6 points

5. The integer $p = 19$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{19}^*$ with generator $g = 2$. Alice's public key is $h_a = 11$. Use the Baby-Step Giant-Step method to compute Alice's private key. | 10 points

6. The affine encryption system is a symmetric system. The key consists of two integers $0 \leq a, b < 26$ with $\gcd(a, 26) = 1$. Messages and ciphertexts are also integers in $[0, 25]$. Message m is encrypted as $c = a \cdot m + b \bmod 26$.

   (a) Explain how decryption works. | 4 points

   (b) Your key is $(a, b) = (5, 7)$ and you receive the ciphertext 17. Compute the plaintext. | 3 points

   (c) Compute the size of the keyspace, i.e. how many different keys exist. | 3 points

7. This exercise is about LFSRs. You know that A and B use an LFSR of order 4. You observe ciphertext 001001010110 and know that start of the message was 80 and hexadecimal encoding

```
0 -> 0000  a -> 1010
1 -> 0001  b -> 1011
2 -> 0010  c -> 1100
    ...  ...
9 -> 1001  f -> 1111
```

   was used. The ciphertext is the xor of the message with the output stream of the LFSR and the stream starts from the left.

   (a) Compute the first 8 bits of the LFSR output and state the initialization vector. | 4 points

   (b) Compute the feedback coefficients of the LFSR. | 16 points

   (c) Compute the next hexadecimal digit after 80. | 4 points