TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 17 April 2023

Name :

TU/e student number :

Exercise	1	2	3	4	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 4 exercises. You have from 18:00 – 21:00 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 statement asks for 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

$$s_{i+6} = s_{i+5} + s_{i+4} + s_i.$$

   (a) Draw the LFSR corresponding this sequence. 3 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. 10 points

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

   (d) What is the longest period generated by this LFSR?
   Make sure to justify your answer. 3 points

   (e) State the lengths of all subsequences so that each state of 6 bits appears exactly once.
   Make sure to justify your answer and to check that all 2^6 states are covered. 10 points

2. This exercise is about modes.

   Here is a schematic description of the CBC-CBC mode.

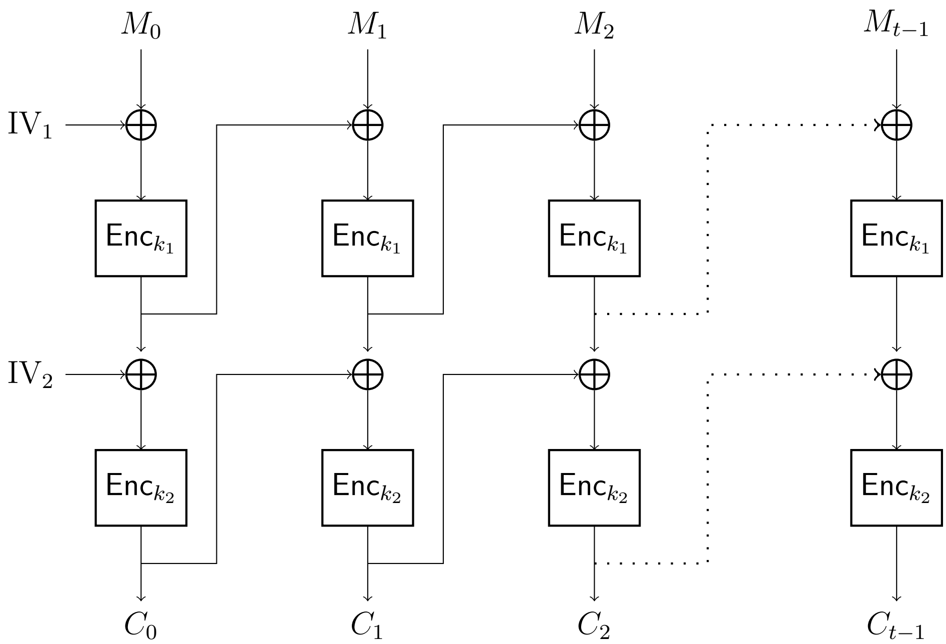

   Image credit: adapted from Jérémy Jean.

   Enc is an n-bit block cipher. Alice and Bob share a key k for Enc. Let $\mathsf{Enc}_k(m)$ denote encryption of a single block m using this block cipher with key k and let $\mathsf{Dec}_k(c)$ denote decryption of a single block c using the block cipher with key k. Let IV be the initialization vector of length n, let $M_i, i = 0, 1, 2, \ldots$ be the n-bit blocks holding the message and $C_i, i = 0, 1, 2, \ldots$ be the n-bit blocks holding the ciphertexts.

   (a) Describe how encryption of long messages works by writing C_0 and a general C_i in terms of IV, M_0, M_i, and (if necessary) other M_j and C_j. Describe how decryption of long messages works by writing M_0 and a general M_i in terms of IV, C_0, C_i, and (if necessary) other M_j and C_j. 8 points

   (b) Alice sends two messages, m and m'' which differ only in one block M_i and she uses the same IVs.

   Investigate and describe which blocks of the respective ciphertexts c and c' differ. Note that i can take any value including 0 and $t-1$. 6 points

   (c) Assume that ciphertext c gets modified in transit to c' and that c' and c which differ only in one block C_j.

Investigate and describe which blocks in the resulting plaintext m' after decryption differ from the correct plaintext m. Note that j can take any value including 0 and $t-1$. The IVs are transmitted correctly. 6 points

3. This problem is about schoolbook RSA encryption.

   (a) Let $p = 547$ and $q = 569$. Compute the public key using $e = 31$ and the corresponding private key.
   Reminder: The private exponent d is a positive number. 8 points

   (b) Describe in your own words how encryption works for schoolbook RSA and why decryption yields the correct message. 6 points

   (c) Three different parties A, B, and C each have their own RSA modulus n_A, n_B, and n_C, respectively, and all use $e = 3$, i.e. use keys $(n_A, 3)$, $(n_B, 3)$, and $(n_C, 3)$. Describe in your own words how an attacker can obtain plaintext m if m is encrypted to A, B, and C using schoolbook encryptions.

   Your answer should state the steps the attacker needs to perform and explain why the attack works. You may assume that n_A, n_B, and n_C are coprime. 11 points

4. This exercise is about the signature system in $\mathbb{F}_p^*$. In this system everybody knows prime p and a generator g of (a subgroup of) $\mathbb{F}_p^*$ order ℓ, where ℓ divides $p-1$.

   In KeyGen, user Alice picks a random $a \in [1, \ell-1]$ as her private key and computes $h_A = g^a$ as her public key.

   To sign a message m she picks a random $k \in [1, \ell-1]$ and computes $r = g^k$, $H = \mathsf{hash}(r, m)$, and

   $$s \equiv k - H \cdot a \bmod \ell.$$

   The signature is the pair (r, s) which gets sent along with m.
   Note that r is computed in $\mathbb{F}_p^*$, i.e., computing modulo p and that s is computed modulo ℓ.

   To verify that (r, s) is a valid signature on m by the user with public key h_A, one computes $H = \mathsf{hash}(r, m)$ and checks that

   $$r = g^s \cdot h_A^H.$$

   If this equation holds the signature is valid, else invalid.

   (a) Let $p = 107, \ell = 106$, and $g = 2$. Perform KeyGen for Alice with $a = 68$.

   Then compute a signature using $k = 42$ and $H = 23$.
   Note that *computing* H requires first computing r but we do not have such a small hash function anyways. This example is mostly for expository reasons so that that you go through all steps.

   Make sure to document all intermediate steps for KeyGen and signing. 7 points

   (b) Explain why the signature system works, i.e., why a signature made using Alice's private key a passes verification using h_A.

   Explain also what problems an attacker faces in forging a signature, i.e., in computing a pair (r, s) that passes verification for his choice of m and a fixed h_A without having access to the private key a. 8 points

   (c) It is very important for Schnorr's signature system that r is included when computing H. Show how you can forge a signature for Alice if the definition was $H = \mathsf{hash}(m)$.

   8 points