TECHNISCHE UNIVERSITEIT EINDHOVEN
Faculty of Mathematics and Computer Science
Introduction to Cryptology, Monday 22 January 2024

Name :

TU/e student number :

Exercise	1	2	3	4	5	6	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 100 points.
Make sure to justify your answers in detail and to give clear arguments. Document all steps and intermediate results, in particular of algorithms; it is not sufficient to state the correct result without the explanation and the steps that lea. 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

$$s_{i+6} = s_{i+5} + s_{i+3} + s_i.$$

   (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.
   Reminder: Factors may appear with multiplicity larger than one. **13 points**

   (c) Write the factorization of f from (b) in the form $f = \prod f_i^{e_i}$ with integers $e_i > 0$ and f_i different irreducible polynomials, i.e., group equal factors.
   For each of the $f_i^{e_i}$ compute the order. **7 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. **13 points**

2. This exercise is about modes.

CCM is a mode for authenticated encryption which permits to authenticate additional data block A which is not encrypted but only authenticated. CCM is specified for a block cipher E_k with block length $n = 128$. Let k denote the key shared by Alice and Bob. Here is a schematic description of the CCM mode.

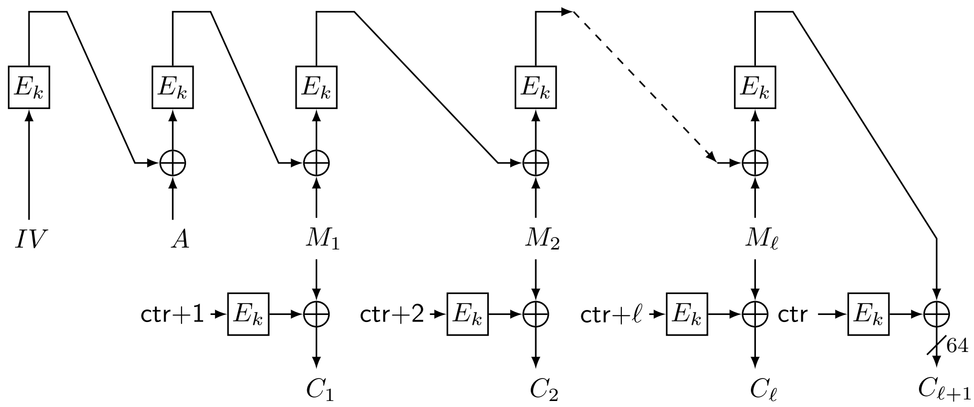

Image credit: adapted from Håkon Jacobsen.

CCM is used with a nonce N, a string that must never repeat, and there are two fixed strings flags_1 and flags_2. With that the initialization vector IV and counter ctr are defined as follows

$IV = \mathsf{flags}_1 || N || \mathsf{length}_{16}(A + M),$
$\mathsf{ctr} = \mathsf{flags}_2 || N || 0^{16},$

Where 0^{16} denotes a vector of 16 zeros, and $\mathsf{length}_{16}(A + M)$ indicates the length of $A + M$ as a 16-bit number

Let $E_k(M)$ denote encryption of a single block M using this block cipher with key k and let $D_k(C)$ denote decryption of a single block C using the block cipher with key k.

Let A be some additional data to be authenticated, $M_i, i = 1, 2, \ldots, \ell$ be the n-bit blocks holding the message, $C_i, i = 1, 2, \ldots \ell$ be the n-bit blocks holding the ciphertexts, and $C_{\ell+1}$ hold the authentication tag. The 64 in the drawing indicates that the authentication tag is limited to just 64 bits.

The ciphertext send is $N, A, C_1, C_2, \ldots, C_\ell, C_{\ell+1}$.

(a) Describe how authenticated encryption of long messages works by writing C_1, $C_{\ell+1}$, and a general C_i in terms of ctr, A, M_1, M_i, and (if necessary) other M_j and C_j. 3 points

(b) Describe how decryption of long messages and verification of the authentication tag works by writing M_1 and a general M_i in terms of ctr, A, C_1, C_i, and (if necessary) other M_j and C_j and describe how the authentication tag $C_{\ell+1}$ confirms the authenticity of the message and the additional data A. 3 points

(c) Assume that ciphertext C_j gets modified in transit. Show which message blocks get decrypted incorrectly and explain why others get decrypted correctly. Show how the authentication tag $C_{\ell+1}$ catches this error. 5 points

(d) Assume that the additional data A gets modified in transit. Show which message blocks get decrypted incorrectly and explain why others get decrypted correctly. Show how the authentication tag $C_{\ell+1}$ catches this error. 3 points

3. This problem is about RSA encryption. Let $p = 313$ and $q = 431$. Compute the public key using $e = 65537$ and the corresponding private key.
Reminder: The private exponent d is a positive number. 8 points

4. This problem is about the DH key exchange. The public parameters are the group G and generator g, where $G = (\mathbb{F}_{1031}^*, \cdot)$ and $g = 37$. Alice's public key is $h_A = 123$. Bob's private key is $b = 19$,
Compute the DH key that Bob shares with Alice. 8 points

5. The integer $p = 29$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{29}^*$ with generator $g = 2$. Alice's public key is $h_A = g^a = 10$. Use the Baby-Step Giant-Step method to compute Alice's private key a.
Verify your result, i.e. compute g^a. 12 points

6. This exercise introduces the NTRU public-key encryption system which you will analyze. The system has two parameters: namely positive integers N, and prime q, where $\gcd(3, q) = 1$ and q is much larger than 3.

   All computations take place in $R = \mathbb{Z}[x]/(x^N - 1)$, i.e. all elements are represented by polynomials of degree $< N$ and when multiplying polynomials we reduce modulo $x^N - 1$. Some computations additionally reduce modulo 3 or modulo q.

   The private key of user Alice is a polynomial $f \in R$. This polynomial is chosen randomly with the constraint that $1 + 3f$ is invertible in R modulo q and that the coefficients are in $\{-1, 0, 1\}$. For an example with cryptographic sizes use $N = 761, q = 3449$ and pick f with exactly $w = 286$ coefficients in $\{-1, 1\}$ and the remaining $N - w = 475$ coefficients are all 0. We call a polynomial with these properties *short*.

   To generate her public key, Alice picks a polynomial $g \in R$ with coefficients in $\{-1, 0, 1\}$ and computes $f_q = (1 + 3f)^{-1}$ in R modulo q and $h = f_q \cdot g$ in R modulo q. Both steps require computing modulo $x^N - 1$ and modulo q. Alice's public key is h along with the public parameters q and N.

   To encrypt message $(m_0, m_1, \ldots, m_{N-1})$ with coefficients in $\{-1, 0, 1\}$ to Alice, who has public key h, put $m(x) = \sum m_i x^i \in R$, take a random short polynomial $r(x) \in R$ and compute $c = 3r \cdot h + m$, where the computations happen modulo $x^N - 1$ and modulo q.

   To decrypt ciphertext c Alice uses her private key f and computes $a = (1+3f) \cdot c$ in R modulo q, choosing coefficients in $[-(q-1)/2, (q-1)/2]$. [If you're a mathematician, this means you lift a to R, i.e. forget about the reduction modulo q]. Then she computes $m' \equiv a \bmod 3$, taking coefficients from $\{-1, 0, 1\}$.

   In the decryption step, Alice combines computations modulo q and modulo 3. However, these are coprime numbers and thus these computations are not compatible. To see this, take $q = 17$ for a small example: then $12 \equiv 0 \bmod 3$ and $29 \equiv 2 \bmod 3$ while 12 and 29 are in the same residue class modulo 17, i..e, $29 \equiv 12 \bmod 17$. NTRU avoids this problem of non-unique results by first reducing modulo q to an integer in $[-(q - 1)/2, (q - 1)/2]$ and then reducing modulo 3. In this example this would require computing $12 \equiv -5 \bmod 17$, using a result in $[-8, 8]$, which then gets reduced modulo 3 as $-5 \equiv 1 \bmod 3$, using a result in $\{-1, 0, 1\}$.

(a) Show that the system correctly recovers the message, i.e., that $m = m'$.
The next exercise will go into more detail on mixing reductions modulo q and modulo 3. Here you can assume that all reductions modulo q give the correct residue class. **6 points**

(b) In (a) you computed an expression for the polynomial a before reduction modulo 3. Decryption works correctly if each coefficient of this expression is in $[-(q-1)/2, (q-1)/2]$.
To check if this is the case here, compute the maximum possible size of the coefficients of rg. Remember that r and g have coefficients in $\{-1, 0, 1\}$ and that r is further limited to having only w non-zero coefficients.
With this result compute the maximum possible size of the coefficients of a as an expression in w. Then verify that for the concrete parameters given above, $N = 761, q = 3449$ and $w = 286$, decryption works correctly. **6 points**

(c) Bob misunderstands the meaning of "short" and, in addition to using the correct restrictions, he also limits the degree of r to less than w so that r has the form $r(x) = \sum_{i=0}^{w-1} r_i x^i$ with $r_i \in \{-1, 1\}$. He also does not have a lot to say, so his messages use only the first 200 coefficients of m, i., e., $m(x) = \sum_{i=0}^{199} m_i x^i$.
Find an efficient way to recover m given c. Note that the degrees of r and m are too large to permit a brute-force search.

Hint: Write the computation of $3rh$ modulo $x^N - 1$ as a vector-matrix multiplication $3R \cdot H$, where R is a vector of length w taking the first w coefficients of r, and H is a $w \times N$ matrix covering multiplication by h and reduction modulo $x^N - 1$ so that the first 3 rows of the matrix (corresponding to $1 \cdot h, x \cdot h$, and $x^2 \cdot h$) are $(h_0, h_1, h_2, \ldots, h_{N-2}, h_{N-1}), (h_{N-1}, h_0, h_1, \ldots, h_{N-3}, h_{N-2})$, and $(h_{N-2}, h_{N-1}, h_0, \ldots, h_{N-4}, h_{N-3})$ because computing modulo $x^N - 1$ replaces x^N by 1.
In this representation recover r and then m. **7 points**