Exam – Cryptology 1 – 01410

16.05.2022

Instructions and advice

- For all computations in Part III: explain how you have computed your results. Unexplained results will receive few or no points. If you use a computer (or similar), then you need to be able to explain how the computer arrived at the answer.
- The problems have been created such that it is possible to solve them without the help of a computer or similar.
- Read all the questions first, and begin to work on the ones you find easy.

Part I – Select all that apply (11 points)

You get 1 point for every correct selection and -1 point for every incorrect selection, but never less then 0 points for a question.

1. Which of the following equations involving modular arithmetic hold? As in the lecture, "=" is used for modular arithmetic, where "≡" is used in the book. Select all that apply.

   A. $6^2 = 6 \bmod 10$

   B. $4^{-1} = 8 \bmod 43$

   C. $4 = 25 \bmod 11$

   D. $11^2 = 1 \bmod 8$

   E. $4 \cdot 7 = -4 \bmod 29$

   F. $8^{17} = 1 \bmod 14$

   Solution: AD

2. Which of the following statements about block ciphers are true? Select all that apply.

   A. Modes of operation are mostly used for public-key encryption.

   B. CTR mode is more secure than ECB mode.

   C. The block length is always larger than the key length.

   D. ECB mode is more secure than CBC mode.

   E. If $3 \to 7 \to d$ is the most likely two-round characteristic, then d is the most likely difference after two rounds are applied to an input pair of difference 3.

   F. If $e \to 5$ is the most likely one-round characteristic, then 5 is the most likely difference after one round is applied to an input pair of difference e.

   G. AES offers different block lengths.

   Solution: BF

3. Which of the following statements about RSA encryption are true? Select all that apply.

A. RSA uses arithmetic modulo a composite number.

B. The ciphertext $N - 2 \in \mathbb{Z}_N$ is in general easy to decrypt for an adversary

C. The ciphertext $N - 1 \in \mathbb{Z}_N$ is in general easy to decrypt for an adversary

D. The encryption algorithm of the RSA encryption scheme requires the secret key.

E. The key generation algorithm of the RSA encryption scheme gets the secret key as an input.

F. Encryption often uses the square-and-multiply algorithm.

G. Decryption requires prime number generation.

Solution: ACF

4. Which statements about the Miller-Rabin test are true? Select all that apply.

A. If the Miller-Rabin prime number generation algorithm outputs n, n is prime.

B. If the Miller-Rabin prime number generation algorithm finds during execution that n is not prime, n is not prime.

C. The Miller-Rabin algorithm is randomized.

D. The Miller-Rabin algorithm is deterministic.

Solution: BC

Part II – Select the right answer (4 points)

You get 2 points if (only) the right answer is selected.

5. How many elements does $\mathbb{Z}_{91}^*$ have? Select the right answer.

A. 91 B. 18 C. 90 D. 84 E. 78 F. 72

Solution: F

6. Assume you want to brute-force a collision of the SHA3 hash function with outputs of length 512 bits. How many evaluations of the function on random inputs do you require approximately? Select the most appropriate answer.

A. 512 B. 2^{256} C. 256 D. 256^2 E. 2^{512} F. $\frac{2^{512}}{2}$

Solution: B

Part III (25 points)

7. (3 points) Recall the CBC mode of operation, where a block cipher e encrypts the ith n-bit block m_i of a message $m = (m_1, m_2, ...)$ as

$$c_i = e_k(m_i \oplus c_{i-1}), \tag{1}$$

where $c_0 = iv$ is a uniformly random n-bit string.

Define a new mode of operation, "reverse CBC" (rCBC) mode, by swapping the role of encryption and decryption, i.e., for rCBC mode encryption, on input a message $m = (m_1, m_2, ...)$, sample a random n-bit string iv, set $c' = (iv, m_1, m_2, ...)$ and apply CBC mode decryption to c' do obtain the ciphertext c.

For CBC and rCBC mode, the initial value $c_0 = iv$ is prepended to the ciphertext, i.e., it is considered to be the 0-th ciphertext block.

In addition, recall ECB mode where a block cipher e encrypts the ith n-bit block m_i of a message $m = (m_1, m_2, ...)$ as

$$c_i = e_k(m_i). \tag{2}$$

(a) How is decryption done in rCBC mode?

Solution: To decrypt an rCBC mode ciphertext $c = (c_0, c_1, c_2, ...)$, apply the CBC mode encryption function to the message $m = (c_1, c_2, ...)$ with IV c_0, to obtain "ciphertext" $c' = (c'_0, c'_1, c'_2, ...)$. Then output $m = (c'_1, c'_2, ...)$.

(b) Like ECB mode, rCBC mode is insecure as a general-purpose encryption scheme. Describe a problem that both rCBC mode and ECB mode have.

Solution: By definition, for rCBC mode, $c_i = d_k(m_i) \oplus m_{i-1}$, where $m_0 = iv$. We can observe that for $i > 1$, the ciphertext block does not depend on iv and is thus a deterministic function of the plaintext, like in ECB mode.

(c) Give an example of a two-block plaintext where a ciphertext produced using ECB mode reveals some information about the plaintext, but encryption with rCBC mode does not.

Solution: For $m = m_1, m_1$, the ECB ciphertext consists of two equal blocks, revealing that the two plaintext blocks are equal. For rCBC mode, this is not the case.

8. (4 points) List all primitive elements of $\mathbb{Z}_{13}$. Describe how you have computed the list.

Solution: $\phi(13) = 12 = 2^2 \cdot 3$, and $\phi(12) = 4$, so there are 4 primitive elements, we compute the orders of the elements of $\mathbb{Z}_{13}^*$ by computing their powers mod 13:

i	1	2	3	4	5	6	7	8	9	10	11	12
order of i	1	12	3	6	4	12	12	4	3	6	12	2

9. (3 points) Compute 4^{50} mod 7 using the square-and-multiply algorithm. Write down all squaring and multiplication steps.

Solution: $50 = 2(1 + 2^3(1 + 2))$. We therefore compute

$$4^2 = 16 = 2 \bmod 7 \tag{3}$$
$$2 \cdot 4 = 8 = 1 \bmod 7 \tag{4}$$
$$1^2 = 1 \bmod 7 (\text{three times}) \tag{5}$$
$$4 \cdot 1 = 4 \bmod 7 \tag{6}$$
$$4^2 = 16 = 2 \bmod 7. \tag{7}$$

10. (4 points) Consider RSA encryption with modulus $N = 9999999983$ and public exponent $e = 5$.

(a) Compute the encryption of $m = 100$. Show the steps of the computation.

Solution: We compute m^5 mod N using square-and-mutiply. Observe that $N = 10^10 - 17$ and $5 = 1 + 4^2$. We compute $m^2 = 10^4$ mod N, $(m^2)^2 = 10^8$ mod N and $m \cdot (m^2)^2 = 10^10 = 17$ mod N. The encryption of m is thus $c = 17$.

(b) Find the plaintext corresponding to the ciphertext 32 (This is possible without factoring N).

Solution: $32 = 2^5$, so 32 is the encryption of 2 (when taking 2 to the power 5, the modulo-N operation has no effect).

(c) Explain why decrypting 32 is easy for public exponent $e = 5$, regardless of N

Solution: If 32 is a valid ciphertext, $N \geq 33$. But in that case, the equation $2^5 = 32$ mod N holds.

(d) Explain how similar vulnerabilities can be avoided when using RSA encryption with $e = 5$. (Note that a slightly larger public exponent is more common, but very small exponents $e \geq 3$ can be used without introducing known vulnerabilities.)

Solution: When using RSA encryption, a padding mechanism is used. In that way, it is ensured that the padded plaintext is never (or unlikely) equal to 2.

11. (2 points) Let

$$h : \{0,1\}^{2n} \to \{0,1\}^n \tag{8}$$

be a compression function, and define a compression function

$$h' : \{0,1\}^{3n} \to \{0,1\}^n \tag{9}$$

by setting $h'(x, y) = x \oplus h(y)$ for an n-bit string x and a $2n$-bit string y.

(a) Give an explicit collision for h'.

Solution: Any input of the form $(h(y), y)$ has hash 0^n under the hash function h', so an explicit collision is e.g. $(h(0^{2n}), 0^{2n})$ and $(h(1^{2n}), 1^{2n})$.

(b) Find a second preimage: For a given input (x, y), with $x \in \{0,1\}^n$ and $y \in \{0,1\}^{2n}$, find a different input $(x', y') \neq (x, y)$ such that $h'(x, y) = h'(x', y')$.

Solution: The second preimage $(x \oplus h(y) \oplus h(y'), y')$ works. Indeed, $h'(x \oplus h(x) \oplus h(y'), y') = x \oplus h(x) \oplus h(y') \oplus h(y') = x \oplus h(y) = h'(x, y)$.

12. (2 points) Consider the plain (=without hashing) RSA digital signature scheme with modulus N and public exponent $e = 5$. For that scheme, a pair of message m and signature σ is valid if $m = \sigma^e \bmod N$.

(a) For $N = 35$, find a message with signature $\sigma = 10$.

Solution: We can just compute $m = \sigma^e = 10^5 = 5 \bmod 35$.

(b) For $N = 9999999983$, find the signature of the message 32.

Solution: $m = 2$, by the same argument as Problem 10b.

13. (2 points) Let $p = 17$ and choose the primitive element $g = 3 \in \mathbb{Z}_{17}^*$. Consider a Diffie-Hellman key exchange where Alice chooses secret exponent $a = 4$ and Bob chooses secret exponent $b = 7$.

(a) Compute the messages Alice and Bob send back and forth during the protocol.

Solution: This is just straightforward computation, $g^4 = 13 \bmod 17$, $g^7 = 11 \bmod 17$.

(b) Compute the shared secret key.

Solution: $13^7 = 11^4 = 4$.

14. (5 points) Let $N = p_1 \cdot p_2$ for distinct odd primes p_1 and p_2 such that $p_i - 1 = 2p_i'$ for a prime p_i', for $i = 1, 2$. Suppose we would like to use N instead of a prime modulus for El Gamal.

(a) (1 point) What is the maximum order in $\mathbb{Z}_N^*$?

Solution: The maximum order in $\mathbb{Z}_N^*$ is $\gcd(p_1 - 1, p_2 - 1) = 2 \cdot p_1' \cdot p_2'$.

(b) (2 points) Let $\alpha \in \mathbb{Z}_N^*$. Just like in the case of a prime modulus, we say α is *primitive* if it has maximum order. Use the Chinese Remainder Theorem to describe how to check whether α is primitive in $\mathbb{Z}_N^*$.

Solution: According to the Chinese Remainder theorem, a number $\alpha \in \mathbb{Z}_N^*$ is uniquely determined by $\alpha_1 = \alpha \bmod p_1$ and $\alpha_2 = \alpha \bmod p_2$, and to add or multiply numbers mod N we can instead add their corresponding moduli mod p_1 and p_2. To check whether α is primitive in $\mathbb{Z}_N^*$ it thus suffices to check whether α_i is primitive in $\mathbb{Z}_{p_i}^*$.

(c) (2 points) Consider the following "double DLP". Given $\alpha_i, a_i \in \mathbb{Z}_{p_i}^*$, find integers n_i such that $\alpha_i^{n_i} = a_i \bmod p_i$, for $i = 1, 2$. Argue that the double DLP is not easier than the DLP for modulus p_i, for $i = 1$ or $i = 2$. Argue using the Chinese Remainder Theorem that El Gamal with modulus N is not less secure than El Gamal with modulus $\min(p_1, p_2)$.

Solution: The double DLP amounts to finding two discrete logarithms. It can therefore not be easier than finding one discrete logarithm. The security of El Gamal is, intuitively, based on the discrete logarithm problem. The security of El Gamal with modulus N thus requires the hardness of the discrete logarithm problem in $\mathbb{Z}_N^*$. But by the Chinese

Remainder Theorem, finding a discrete logarithm mod N is equivalent to finding two discrete logarithms, one mod p_1 and one mod p_2. In more detail, we are given numbers α and a and need to find a number n such that $\alpha^n = a \bmod N$. We can compute $\alpha_i = \alpha \bmod p_i$ and $a_i = a \bmod p_i$, for $i = 1, 2$. by the Chinese Remainder Theorem it is equivalent to find n_i such that $\alpha_i^{n_i}$ and that fulfill the equation $n = n_1 + k_1(p_2 - 1) = n_2 + k_2(p_1 - 1)$ for some integers n, k_1, k_2.