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

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.

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

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. $\frac{2^{512}}{2}$

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?

   (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.

   (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.

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

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

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.
    (b) Find the plaintext corresponding to the ciphertext 32 (This is possible without factoring N).
    (c) Explain why decrypting 32 is easy for public exponent $e = 5$, regardless of N
    (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.)

11. (2 points) Let
$$h : \{0,1\}^{2n} \to \{0,1\}^n \tag{3}$$
be a compression function, and define a compression function
$$h' : \{0,1\}^{3n} \to \{0,1\}^n \tag{4}$$
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'.
    (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 $h'(x, y) = h'(x', y')$.

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 $\sigma = 10$.
    (b) For $N = 9999999983$, find the signature of the message 32.

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.
    (b) Compute the shared secret key.

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 $\mathbb{Z}_N^*$?
    (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 $\mathbb{Z}_N^*$.
    (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 $\min(p_1, p_2)$.