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. $5 = 23 \bmod 9$
   B. $5^2 = 5 \bmod 10$
   C. $6^{14} = 1 \bmod 12$
   D. $3^{-1} = 7 \bmod 43$
   E. $9^2 = 4 \bmod 7$
   F. $4 \cdot 7 = -3 \bmod 29$
2. Which of the following statements about block ciphers are true? Select all that apply.
   A. The block length and the key length are always the same.
   B. Block ciphers are mostly used for public-key encryption.
   C. AES is an iterated block cipher.
   D. CBC mode is more secure than ECB mode.
   E. ECB mode is more secure than CTR mode.
   F. If $a \to 5 \to f$ is the most likely two-round characteristic, then f is the most likely difference after two rounds are applied to an input pair of difference a.
   G. If $c \to 8$ is the most likely one-round characteristic, then 8 is the most likely difference after one round is applied to an input pair of difference c.
3. Which of the following statements about RSA encryption are true? Select all that apply.
   A. RSA uses arithmetic modulo a prime.
   B. The decryption algorithm of the RSA encryption scheme requires the secret key.

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

D. Decryption uses the square-and-multiply algorithm.

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

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

G. Decryption uses the Chinese Remainder Theorem.

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

   A. The Miller-Rabin test is a randomized algorithm.

   B. The Miller-Rabin test is a deterministic algorithm.

   C. If the test says that n is prime, n is prime.

   D. If the test says n is not prime, n is not prime.

Part II – Select the right answer (4 points)

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

5. How many elements does $\mathbb{Z}_{55}^*$ have? Select the right answer.

   A. 55 B. 54 C. 44 D. 40 E. 50 F. 16

6. Assume you want to brute-force a collision of the SHA3 hash function with outputs of length 256 bits. How many evaluations of the function on random inputs do you require approximately? Select the most appropriate answer.

   A. 128 B. 256 C. 256^2 D. 2^{128} E. $2^{256}/2$ F. 2^{256}

Part III (25 points)

7. (3 points) Recall the ECB and CTR modes of operation. For ECB, a block cipher e encrypts the ith n-bit block m_i of a message $m = (m_1, m_2, ...)$ as

$$c_i = e_k(m_i). \tag{1}$$

   CTR mode is defined by

$$c_i = m_i \oplus e_k(iv \oplus \text{`}i\text{'}), \tag{2}$$

   where 'i' is the n-bit string that represents i mod 2^n in binary, and iv is a uniformly random n-bit string.

   In addition, we define the "IEW" (for "iv everywhere") mode of operation by

$$c_i = e_k(m_i \oplus iv), \tag{3}$$

   where iv is a uniformly random n-bit string.

   For CTR and IEW, $c_0 = iv$ is prepended to the ciphertext, i.e., it is considered to be the 0-th ciphertext block.

   Remark: IEW is not a well-known mode of operation.

   (a) Describe a security problem that ECB mode has but IEW doesn't.

   (b) Describe a security problem that both ECB and IEW modes have.

   (c) Argue why CTR mode does not have any of the two problems you found.

8. (4 points) List all primitive elements of $\mathbb{Z}_{11}$. Describe how you have computed the list.

9. (3 points) Compute $3^{74} \bmod 7$ using the square-and-multiply algorithm. Write down all squaring and multiplication steps.

10. (4 points) Consider RSA encryption with modulus $N = 10^{12} - 3 = 999999999997$ and public exponent $e = 3$.
    (a) Compute the encryption of $m = 10000$. Show the steps of the computation.
    (b) Find the plain text corresponding to the ciphertext 27.
    (c) Explain why decrypting 27 is easy for public exponent $e = 3$, regardless of N
    (d) Explain how similar vulnerabilities are avoided when using RSA encryption.

11. (2 points) Let
$$h : \{0,1\}^{2n} \to \{0,1\}^n \tag{4}$$
be a compression function, and define a compression function
$$h' : \{0,1\}^{4n} \to \{0,1\}^n \tag{5}$$
by setting $h'(x, y) = h(x \oplus y)$ for $2n$-bit strings x and y.
    (a) Give an explicit collision for h'.
    (b) For a given pair (x, y), $x, y \in \{0,1\}^{2n}$, find a different pair $(x', y') \neq (x, y)$ 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 $e = 3$. 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 $N = 10^{12} - 3 = 999999999997$, find the signature of the message 8.

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 $a = 3$ and Bob chooses secret exponent $b = 5$.
    (a) Compute the messages Alice and Bob send back and forth during the protocol.
    (b) Compute the shared secret key.

14. (5 points) Fix an RSA modulus N. It is well-known that plain RSA encryption is *homomorphic* with respect to multiplication. This means that an attacker provided with a ciphertext $c = [m^e \bmod N]$ corresponding to a secret message m can choose a message m' and efficiently compute a ciphertext $\tilde{c}$ for the product $[m \cdot m' \bmod N]$ using the formula $\tilde{c} = [c \cdot m'^e \bmod N]$. But could RSA also be homomorphic with respect to addition? We will show that this is not possible assuming that RSA is secure.

    Suppose that there exists an efficient algorithm $\mathcal{A}$ to perform the following task. Given a public key (N, e), a ciphertext c corresponding to a secret message m, i.e., $c = [m^e \bmod N]$, and a message m', output a ciphertext c' such that
$$c' = [(m + m')^e \bmod N] \tag{6}$$
    (a) (3 points) For $e = 3$, given a ciphertext c corresponding to a secret message m, describe how to efficiently recover m. **Hint:** It is sufficient to run $\mathcal{A}$ twice, for $m' = 1$ and $m' = 2$.
    (b) (2 points) Sketch how to generalize the attack to larger e. How many times do you need to run $\mathcal{A}$ for a general e?