Sept 16,2024

ICS 505 Cryptography

Practice Assignment 1- Introduction and Recap

Dr. Muhammad Hataba, muhammad.hataba@giu-uni.de
TA. John Ehab, john.ehab@giu-uni.de

Q1) Choose the correct answer:

1. What is a cipher?

a) A function used in cryptanalysis

b) The original message after encryption

c) An algorithm for transforming plaintext to ciphertext

d) The process of recovering plaintext from ciphertext

2. What is the objective of cryptanalysis?

a) To determine the ciphertext message from the plaintext

b) To recover the encryption key

c) To encrypt messages securely

d) To prevent unauthorized access to data

3. What principle suggests that the security of a cryptosystem should depend solely on the secrecy of the key?

a) The Shannon Principle

b) The Diffie–Hellman

c) Kerckhoff's Principle

d) The Adversary Model

4. Snooping is a …… attack which threaten the …….. of the system

a) Passive/ Confidentiality

b) Passive/Integrity

c) Active/Availability

d) Active/ Confidentiality

5. Which of the following is NOT a characteristic of a secure hash function?

a) Pre-image resistance

b) Collision resistance

c) Deterministic output

d) Reversible output

6. Which type of attack exploits weaknesses in the execution of cryptographic algorithms rather than breaking the algorithms themselves?

a) Timing side-channel attack

b) Differential cryptanalysis

c) Brute-force attack

d) Frequency analysis

7. What is the main difference between a stream cipher and a block cipher?

a) Stream ciphers operate on fixed-size blocks of plaintext, while block ciphers operate on variable-length plaintext.

b) Stream ciphers encrypt plaintext one bit at a time, while block ciphers encrypt plaintext in variable-size blocks.

c) Stream ciphers use a fixed key length, while block ciphers use a variable key length.

d) Stream ciphers encrypt plaintext one bit at a time, while block ciphers encrypt plaintext in fixed-size blocks.

8. Which of the following is a symmetric key encryption algorithm commonly used in WEP Protocol?

a) AES

b) RSA

c) ECC

d) RC4

9. Non-Repudiation refers to

a) The sender of the message might later deny that she has sent the message.

b) The receiver of the message might later deny that he has received the message.

c) Prevent an authorized party from denying the existence or contents of a communication session

d) All of the above

10. The relationship between key and ciphertext bits should be complicated. Ciphertext and plaintext should appear to be statistically independent. This property is called

a) Diffusion

b) Avalanche Effect

c) Confusion

d) Efficiency

11. What property of stream ciphers makes them advantageous when transmission errors are probable?

a) Error correction

b) Error propagation

c) Error detection

d) Error isolation

12. In a chosen-plaintext attack,

a) The adversary can choose plaintexts and obtain the corresponding ciphertexts

b) The adversary can choose ciphertexts and obtain the corresponding plaintexts

c) The adversary can obtain corresponding plaintext-ciphertext pairs produced with the same encryption key

d) The adversary can only observe chosen ciphertexts produced by the same encryption key

Q2) What are Digital Certificates? How are they verified?

Q3) Alice has a long message m. She breaks m into blocks of 64 bits: m = m1||m2||⋯||mN. She regards each block as a number between 0 and 264 − 1, and she signs the sum t = m1 + m2 +⋯+ mN. This means her signed message is (m, sig(t)), where sig is the signing function. Is this a good idea? Why or why not?

Q4) For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where Cipher message=11 and thus find the plain text. (Hint: You can use a computer)