Midterm
CS 478/513 Computer Security
Spring 2024

Computer Science Department, New Mexico State University

Note: **Explain each answer. Try to be brief.** Please answer questions with a pen. Answers written in pencil will not be re-graded. This exam has five questions and all need to be answered.

Qn1. For each of the statements/questions, put T for True and F for False in front of the corresponding question number. [30 pts = 2 pts each]

1. A message encrypted with the public key of a receiver can be used for integrity check by the receiver.
2. Denial of service attack, DoS, targets information availability.
3. It doesn't matter if a given cryptosystem is common knowledge, as long as the key is secret.
4. The shift by n substitution-cipher approach needs 26! combinations for brute force attack.
5. In DES, the F function needs to be invertible.
6. Diffusion is process of obscuring the relationship between the ciphertext and the plaintext.
7. Feistel cipher is a template for designing block ciphers.
8. The speed of the A5/1 algorithm can be ascribed to its hardware implementation.
9. AES and DES are both based on Feistel cipher but with different key size.
10. A message authentication code, MAC, preserves integrity but not non-repudiation.
11. A one time pad offers perfect security.
12. Ciphers not based on Feistel networks can have a variable number of rounds.
13. The minimum level of security an encryption algorithm must provide to be used in practice is security against known plaintext attacks.
14. Digital certificate is composed of a user's public/private keys, bounded to its identity, encrypted by a trusted third party's public key.
15. All public-key cryptography encryption provides non-repudiation.

Qn2. This problem deals with DES. [**9** pts = 3 + 3 + 3]

a. What kind of cryptosystem is DES? Why is DES insecure?
Ans:

b. How does 3DES solve the concern(s) with DES? Illustrate.
Ans:

c. Is 2DES secure? Justify your answer.
Ans:

Qn3. Assume that we have an A5/1 stream cipher. Please justify your answers. [**10** pts = 5 pts + 5 pts]

a. What is the probability of X and Y and Z stepping?
Ans:

b. What is the probability that X and Z step?
Ans:

Qn4. Design a secure shared key communication protocol, among two entities Alice and Bob accounting for the following requirementss: [**35** pts]

a. Alice decides to use AES with block length of 256 bits and key length of 128 bits.

b. Alice encrypts 9173 bits of data using CBC mode of encryption.

c. Alice also sends a MAC over the plaintexts to Bob for integrity verification.

Please show and explain your design, with all steps, preferably as a sequence diagram. In particular:

1. (7points) Point out how many blocks of ciphertext will Alice and Bob have? What will be the size of the IV in bits?

2. (14 points) Show the encryption and MAC steps on Alice's side.

3. (14 points) Show the decryption and MAC verification steps on Bob's side.

Qn5. This problem is about the CTR-mode encryption/decryption. Using these terminologies from our slides: C_i (i-th cipher block), P_i, IV, E and K; please answer the following questions.

a. Suppose Alice encrypts plaintext blocks P_0, P_1, ..., P_n using CTR mode and obtains ciphertext blocks C_0, C_1, ..., C_n. She sends these ciphertext to Bob with *ctr* as the initial counter value (i.e., IV). During transmission, Trudy changes block C_k to X. Which blocks decrypt correctly and why? [**8** pts]

b. Suppose Trudy changes *ctr* to ctr'. Which blocks decrypt correctly and why? [**8** pts]
Ans: