

CS 6343 CRYPTOGRAPHY

EXAM #1, SUMMER 2022

TIME: 90 MINUTES

Name:

.....
.


R Number:

.....

Exam Conditions:

This is a closed book exam; No dictionary, or “cheat sheet” is allowed.

You are not allowed to go out of the exam room during examination.

Turn off all communication devices (i.e., smart shoes  , mobile phones, smart watches, etc.) for the duration of the exam.

PART 1 (MULTIPLE CHOICE QUESTIONS — 5 POINTS)

1. Which of the following is not true about the CBC mode of operation
 - a. If one block of the cipher text is altered, the error propagates for at most two blocks.
 - b. The IV must be kept secret
 - c. The plaintext blocks of a given message cannot be encrypted in parallel
 - d. It has a self-healing property.
2. In a brute force attack against a monoalphabetic cipher based on the English alphabet, the following is true:
 - a. The amount of time required to find the key exceeds that needed to find the key in a similar attack against DES
 - b. The amount of time to find the key is twice that needed for DES in a similar attack against DES

- c. The amount of time required to find the key exceeds that needed to find the key in a similar attack against AES
- d. The amount of time to find the key is twice that needed for AES in a similar attack against AES

3. Given the key, 1 0 1 0 0 0 0 1 0 used by the S-DES algorithm.

The two subkeys derived from this key are:

- a. Key-1: 1 0 1 0 0 1 0 0; Key-2: 0 1 0 0 0 0 1
- b. Key-1: 1 1 1 0 0 1 0 1; Key-2: 0 1 1 0 1 0 1 1
- c. Key-1: 0 0 1 0 0 1 0 1; Key-2: 0 0 0 0 1 0 1 0
- d. None of the above

(see S-DES key derivation algorithm in appendices).

4. The string MOR is encrypted using the hill cipher with key

$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$. The ciphertext from this encryption is:

- a. ZPA
- b. MWB
- c. QRN
- d. None of the above

5. A block cipher using a block/key size of n -bits is found vulnerable to brute force. To overcome this problem, it has been suggested that double encryption be done (i.e., to use 2 keys in sequence). An engineer indicates that this scheme will fall to a meet-in-the-middle attack. Which of the following is not true:

- a. The computation effort needed by a brute force attack is 2^{n-1} times that needed by the meet-in-the-middle attack
- b. The space requirement of the meet-in-the-middle attack is $n2^n$ bits
- c. The time complexity of the brute force attack is $O(2^{2n})$
- d. The space requirement of the meet-in-the-middle attack is $O(2^{n+1})$.

PART 2 (STRUCTURED QUESTIONS — 15 POINTS)

1. The following text (with minor edits) is got from:
<http://users.telenet.be/d.rijmenants/en/onetimepad.htm>

*One-time pad is a crypto algorithm where plaintext is combined with a random key. **It is the only existing mathematically unbreakable encryption**. Used by Special Operations teams and resistance groups during WW2, popular with intelligence agencies and their spies during the Cold War and beyond, protecting diplomatic and military message traffic around the world for many decades, the one-time pad gained a reputation as a simple yet solid encryption system with an absolute security which is unmatched by today's modern crypto algorithms. Whatever technological progress may come in the future, one-time pad encryption is, and will remain, the only truly unbreakable system that provides real long-term message secrecy. We can only talk about one-time pad if some important rules are followed. If these rules are applied correctly, the one-time pad can be proven unbreakable. Even infinite computational power and infinite time cannot break one-time pad encryption, simply because it is mathematically impossible. However, if only one of these rules is disregarded, the cipher is no longer unbreakable.*

- a) The key is at least as long as the message or data that must be encrypted.
- b) The key is truly random (not generated by a simple computer function or such)
- c) Each key is used only once, and both sender and receiver must destroy their key after use.
- d) There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers)

Questions:

- (i) [3 points] Provide a mathematical proof to support the claim in underlined and bold fonts in the above paragraph.

- (ii) Explain the reasons behind the rules in (a) and (b) above
[1 point] Rule (a)

[1 point] Rule (b)

- (iii) [2 points] Illustrate a line of attack that will be made possible if rule (c) is not followed (For this illustration, assume a key 1100101 that is reused to encrypt the two plain texts 1010101 and 0001111).

2. [1 point] (a) Why is an ideal block cipher not practical for most applications?

(b) Given the failures of the ideal block cipher, a student proposes the following block cipher scheme instead. In this scheme, x_i are the four binary digits of the plaintext block, y_i are the four binary digits of the ciphertext block, and k_{ij} are the binary coefficients representing the key, and arithmetic is mod 2. The scheme illustrates encryption for a block size of 4 bits, but could be extended to n -bits as needed.

$$y_1 = k_{11}x_1 + k_{12}x_2 + k_{13}x_3 + k_{14}x_4$$

$$y_2 = k_{21}x_1 + k_{22}x_2 + k_{23}x_3 + k_{24}x_4$$

$$y_3 = k_{31}x_1 + k_{32}x_2 + k_{33}x_3 + k_{34}x_4$$

$$y_4 = k_{41}x_1 + k_{42}x_2 + k_{43}x_3 + k_{44}x_4$$

[1 point] (i) Which aspect of an ideal block cipher would this cipher improve upon, if any?

[2 points] (ii) Sketch out a line of attack that would defeat the cipher proposed by the student.

3. [2 points] a) Use diagrams to illustrate the mechanism of the CTR and OFB modes of operation.

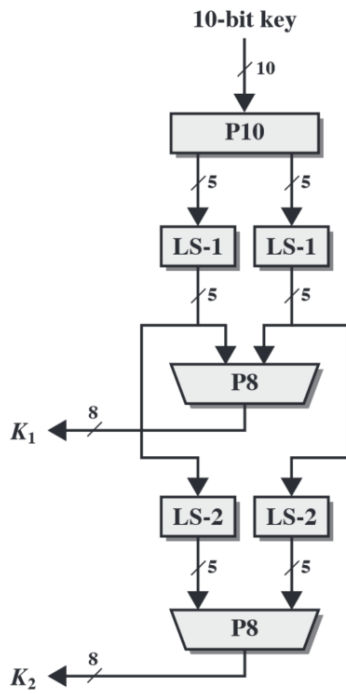
b) A novice engineer makes the following errors when implementing these schemes. Explain the weaknesses that will result, or line(s) of attack that will be made possible in each case.

[1 point] (i) In OFB, he keeps the nonce constant while encrypting a bunch of files with a given key.

[1 point] (ii) In CTR, he keeps the counter constant while encrypting a bunch of files with a given key.

Appendices

Figure 1: Generating the sub keys



P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9