studocu

Crypto-mid QP - Mid semester examination answers

Cryptography (Birla Institute of Technology and Science, Pilani)

Studocu is not sponsored or endorsed by any college or university
Downloaded by Saptak (burningsoulofdarkness@gmail.com)

Birla Institute of Technology & Science – Pilani
Hyderabad Campus
2nd Semester 2019-2020
Cryptography (BITS F463) – Mid Sem Test (Regular)
Date: 05.03.2020 Weightage: 30% Duration: 1 hr. 30 min. Type: Closed Book

---

Instructions: Answer all questions. Answer all parts of a question consecutively. No of pages: **2**

Q1. (a) Consider the Playfair cipher. Given the keyword KEYWORD, encrypt the message **"Why, don't you?"**
(b) Consider the Hill cipher encryption of the form

$$\begin{bmatrix} y1 \\ y2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x1 \\ x2 \end{bmatrix} \bmod 26.$$

Encipher the word MISSISSIPPI, with K as the padding character and given a = 22, b = 13, c = 11 and d = 5.
(c) Given the plaintext **MICHIGAN TECHNOLOGICAL UNIVERSITY** and the keyword as **HOUGHTON,** find the outcome of Vigenere cipher encryption.
(d)(i) Consider the rail fence cipher with key = 4. Find the ciphertext for the plaintext **"This is a secret message".**
(ii) Decrypt the message **DEZCDZGAOIG** with depth = 3 using rail fence decryption.
(e) Monoalphabetic substitution cipher can be constructed using *alphabet mixing via columnar transposition*. The steps are (i) The letters from the keyword form the headings of the columns, and the remaining letters of the alphabet fill in order in the rows below (ii) Mixing is achieved by transcribing columns (i.e., transcribing columns left-to-right gives the substitution). If the keyword **is CORNELL**, use this scheme to encrypt the message **"FAR ABOVE CAYUGA'S WATERS".**

(4 + 4 + 4 + 4 + 4 = 20 marks)

Q2. (a) In cryptography congruence relations play a major role. Solve the following using congruences. (i) $5^{-1} \bmod 7$ (ii) $23x \equiv -9 \bmod 60$ (iii) $5x \equiv 1 \bmod 12$ (iv) $x \equiv 13/8 \bmod 29$ (v) Show that the number 345,546,711 is divisible by 9 using congruences.
(b) Consider the finite field $GF(2^m)$. Given the polynomials $P1 = (x^2+x+1)$ and $P2 = (x+1)$, show that the results of P1 + P2 and P1-P2 will be the same if we perform modulo 2 arithmetic.
(c) Let us assume that the equation xyz = 1 holds in a group G. (i) Does it follow that yzx = 1 ?(ii) Does it follow that yxz = 1? Reason your answer.
(d) Let G be the set of all 2×2 matrices (as shown below) where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Use matrix multiplication as the operation in G to show that G is a group of order 6. Also show the elements.

$$\begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}$$

(e) This problem pertains to block cipher modes of operations and their security aspects. Match every mode of operation with its correct security feature in the following table.

Mode	Security aspect
1. ECB	A. encryption would not be resistant to chosen-plain text attacks if IV is known
2. CBC	B. we should encrypt ciphertext data from the previous round
3. CFB	C. repetition of encrypting the initialization vector may produce the same state that has occurred before
4. OFB	D. nonce plays the same role as initialization vector
5. CTR	E. Created cipher text is not blurred

(4 + 4 + 4 + 4 + 4 = 20 marks)

PTO

Downloaded by Saptak (burningsoulofdarkness@gmail.com)

Q3. (a)(i) Consider the AES implementation. Find w[0], w[1], w[2], w[3] and w[5] given w[4] = (E2, 32, FC, F1). Given the 128 bit key (in hex): **54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75.**

(ii) Consider the 128-bit key implementation of Advanced Encryption Standard. The state matrix after the AddRoundKey operation in the 10^{th} round is as shown below. What is the ciphertext?

$$\begin{pmatrix} 29\ 57\ 40\ 1A \\ C3\ 14\ 22\ 02 \\ 50\ 20\ 99\ D7 \\ 5F\ F6\ B3\ 3A \end{pmatrix}$$

(b) Consider the following simple implementation of DES. Let the plaintext be the string 0010 1000. Let the 10 bit key be 1100011110. The final result of the encryption is 1000 1010. The IP and IP^{-1} functions are as defined below. Find the respective outputs of the transformations IP and IP^{-1}.

IP Table	IP^{-1} Table
2 6 3 1 4 8 5 7	4 1 3 5 7 2 8 6

(c) Consider a snapshot of the 16^{th} round of the standard DES implementation. Fill in the blanks in the following table:

L_{16} = 0100 0011 0100 0010 0011 0010 0011 0100
R_{16} = 0000 1010 0100 1100 1101 1001 1001 0101
Outcome of final permutation: _____
IP^{-1} = _____
Let the final ciphertext C = 85E813540F0AB405

(d) Fill in the blanks in the following table on 3DES implementation with 2keys.

Triple-DES is just DES with two ____bit keys applied. Given a plaintext message, the first key is used to ____the message. The second key is used to ____ the encrypted message. The twice-scrambled message is then ____ again with the ____ key to yield the final cipher text. This three-step procedure is called triple-DES.

Triple-DES is just DES done three times with two keys used in a particular order. (Triple-DES can also be done with three separate keys instead of only two. In either case the resultant key space is about 2^{112}.)

(e) The following table shows the steps in a generic stream cipher system. Fill in the blanks.

Start with a secret key called ("____") ; Generate a ____. The i-th bit/byte of keying stream is a function of the _____ and the first _____ ciphertext bits. Combine the stream with the _____ to produce the ciphertext (typically by XOR)

(4 + 4 + 4 + 4 + 4 = 20 marks)

Downloaded by Saptak (burningsoulofdarkness@gmail.com)