Birla Institute of Technology & Science, Pilani
Work Integrated Learning Programmes Division
First Semester 2023-2024,
Mid-Semester Test (EC-2 Regular)

Course No.	:	CSI ZG513 / ES ZG513 / SS ZG513
Course Title	:	Network Security
Nature of Exam	:	Open Book
Weightage	:	35%
Duration	:	X Hours
Date of Exam	:	20/09/2024 (FN)

No. of Pages = 11
No. of Questions = 11x3 sets

Note to Students:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.

Q.1 Set. (A) Two 16-bits values are provided. One as binary and its value is 10011111 01110110. Another in hexadecimal and its value is 0xB6C5. Perform Exclusive-OR between them and answer in the decimal (base-10) system. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.1 Set. (B) Two 16-bits values are provided. One as binary and its value is 01100111 10011100. Another in decimal and its value is 60874. Perform Exclusive-OR between them and answer in the hexadecimal (base-16) system. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.1 Set. (C) Two 16-bits values are provided. One as hexadecimal and its value is 0xABCD. Another in decimal and its value is 32589. Perform Exclusive-OR between them and answer in the decimal (base-10) system. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.2 Set. (A) Assuming case insensitive English language without space or any other punctuation symbol, find out if the following matrix can be used as a key in the Hill Cipher. Show all the calculations and justify your answer. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

$$\begin{bmatrix} 21 & 5 & 17 \\ 23 & 2 & 5 \\ 6 & 14 & 12 \end{bmatrix}$$

Q.2 Set. (B) Assuming case insensitive English language without space or any other punctuation symbol, find out if the following matrix can be used as a key in the Hill Cipher. Show all the calculations and justify your answer. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

$$\begin{bmatrix} 11 & 7 & 3 \\ 1 & 3 & 5 \\ 12 & 13 & 2 \end{bmatrix}$$

Q.2 Set. (C) Assuming case insensitive English language without space or any other punctuation symbol, find out if the following matrix can be used as a key in the Hill Cipher. Show all the calculations and justify your answer. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

$$\begin{bmatrix} 9 & 3 & 2 \\ 12 & 16 & 7 \\ 25 & 6 & 12 \end{bmatrix}$$

Q.3 Set. (A) Using the keyword **CAPTAIN** and Playfair Cipher, encrypt the plaintext **INFANTRY**. The alphabets I and J need to share the same matrix cell. Assume case insensitive English language without space or any other punctuation symbol. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.3 Set. (B) Using the keyword **MILITARY** and Playfair Cipher, encrypt the plaintext **BATTALION**. The alphabets P and Q need to share the same matrix cell and alphabet X can be used as a filler. A plaintext digram should not have the duplicate alphabets. Assume case insensitive English language without space or any other punctuation symbol. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.3 Set. (C) Using the keyword **ADMIRAL** and Playfair Cipher, encrypt the plaintext **SUBMARINE**. The alphabets P and Q need to share the same matrix cell and alphabet X can be used as a pad. A plaintext digram cannot not have the same alphabet twice. Assume case insensitive English language without space or any other punctuation symbol. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.4 Set. (A) A communication takes place using the case insensitive English language, using a mono-alphabetic substitution cipher. Assume you are an intelligent ethical hacker who knows that the most frequent word in English language is **the**, the most frequently used alphabet is **e** and many times **e** appears twice in the words like **been**, **teeth** etc. From the past cryptanalysis you also know that the plaintext **film** is being encrypted as *!2& and the word **spindle** as **%@!n]28**. With all this information, decrypt the following ciphertext. Reasoning is must for marks. **[2.5 Marks]**

Ciphertext: **1?8** *2881 **&881** **1?8** **%@88]**

Q.4 Set. (B) A communication takes place using the case insensitive English language, using a mono-alphabetic substitution cipher. Assume you are an intelligent ethical hacker who knows that the most frequently used alphabet is **e** and many times **e** appears twice in the words like **been**, **teeth** etc. From the past cryptanalysis you also know that the plaintext **film** is being encrypted as *!2&, the word **spindle** as **%@!n]28** and the word **from** as *73&. With all this information, decrypt the following ciphertext. Reasoning is must for marks. **[2.5 Marks]**

Ciphertext: *882 **1?8** **n88]** *37 **%@88]**

Q.4 Set. (C) A communication takes place using the case insensitive English language, using a mono-alphabetic substitution cipher. Assume you are an intelligent ethical hacker who knows that the most frequently used alphabet is **e** and many times **e** appears twice in the words like **been**, **teeth** etc. From the past cryptanalysis you also know that the plaintext **sputhnik** is being encrypted as **!26#}19r,** the word **god** as **%3]** and the word **from** as *73&. With all this information, decrypt the following ciphertext. Reasoning is must for marks. **[2.5 Marks]**

Ciphertext: **%788]** *37 **!288]** **&88#** **#}8** **81]**

Q.5 Set. (A) (i) Prime factorize **4860** and calculate the Euler Totient function value. (ii) If applicable, apply Fermat's Theorem and calculate the value of **(131 ^ 143) mod 71**. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. Caret symbol (^) represents the exponent or power. **[2.5 Marks]**

Q.5 Set. (B) (i) Prime factorize **11025** and calculate the Euler Totient function value. (ii) If applicable, apply Fermat's Theorem and calculate the value of **(131 ^ 159) mod 79**. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. Caret symbol (^) represents the exponent or power. **[2.5 Marks]**

Q.5 Set. (C) (i) Prime factorize **7875** and calculate the Euler Totient function value. (ii) If applicable, apply Fermat's Theorem and calculate the value of **(131 ^ 120) mod 59**. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. Caret symbol (^) represents the exponent or power. **[2.5 Marks]**

Q.6 Set. (A) If you select a random number 3 and use Miller-Rabin algorithm and apply it on a number 51 for primality testing, what does the algorithm yield? Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.6 Set. (B) If you select a random number 3 and use Miller-Rabin algorithm and apply it on a number 49 for primality testing, what does the algorithm yield? Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

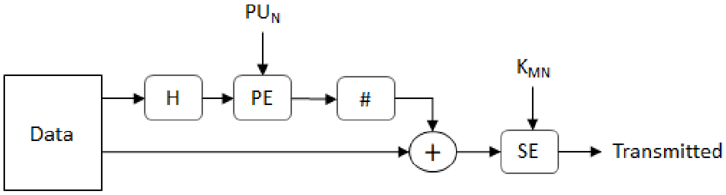
Q.6 Set. (C) If you select a random number 5 and use Miller-Rabin algorithm and apply it on a number 37 for primality testing, what does the algorithm yield? Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. **[2.5 Marks]**

Q.7 Set. (A) An engineer captured some transmission using a packet capture tool. The hex dump of a TCP segment starting from the TCP header is: 00 19 07 58 f7 8a e9 14 2d 7a 23 6f 50 18 fa 84 02 95 00 00 32 35 30 20 53 65 4f 4b 0d 0a. The TCP header is without the optional data. Who is sending this message to whom and what is being conveyed through this TCP segment? Your answer should have all the necessary reasoning, details and complete case sensitive alphabet mapping. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. In TCP header first two bytes are Source Port Address and the next two bytes are Destination Port Address. Reference ASCII Table: number 0 = 0x30, A = 0x41, a = 0x61 **[2.5 Marks]**

Q.7 Set. (B) An engineer captured some transmission using a packet capture tool. The hex dump of a TCP segment starting from the TCP header is: 10 01 00 19 f7 8a e9 14 2d 7a 23 6f 50 18 fa 84 02 95 00 00 45 48 4c 4f 20 53 65 43 75 52 65 0d 0a. The TCP header is without the optional data. Who is sending this message to whom and what is being conveyed through this TCP segment? Your answer should have all the necessary reasoning, details and complete case sensitive alphabet mapping. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. In TCP header first two bytes are Source Port Address and the next two bytes are Destination Port Address. Reference ASCII Table: number 0 = 0x30, A = 0x41, a = 0x61 **[2.5 Marks]**

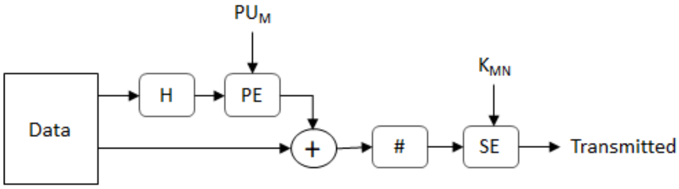
Q.7 Set. (C) An engineer captured some transmission using a packet capture tool. The hex dump of a TCP segment starting from the TCP header is: 12 34 00 19 f7 8a e9 14 2d 7a 23 6f 50 18 fa 84 02 95 00 00 44 41 54 41 0d 0a. The TCP header is without the optional data. What is TCP source port number (in decimal) and what is being conveyed through this TCP segment? Your answer should have all the necessary reasoning, details and complete case sensitive alphabet mapping. Show all the details. Direct answers or copy and paste from web/any tool will not be accepted. In TCP header first two bytes are Source Port Address and the next two bytes are Destination Port Address. Reference ASCII Table: number 0 = 0x30, A = 0x41, a = 0x61 **[2.5 Marks]**

Q.8 Set. (A) The encryption side of PGP is shown below for the sender M and receiver N. Sender wants to protect the data from confidentiality as well as from the integrity attacks. Comment about the correctness of the procedure used by M in not more than 5 points. Do not assume more than what is already given in the question. Answers will not be accepted without proper reasoning. **[2.5 Marks]**



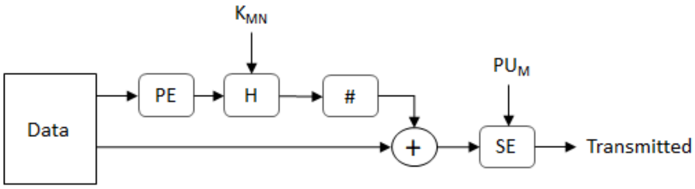
H: Hash Function, PE: Public Encryption, PU_N: Public Key of N,
SE: Symmetric Encryption, K_{MN}: Symmetric Key between M and N
+: Concatenation, #: Compression Function

Q.8 Set. (B) The encryption side of PGP is shown below for the sender M and receiver N. Sender wants to protect the data from confidentiality as well as from the integrity attacks. Comment about the correctness of the procedure used by M in not more than 5 points. Do not assume more than what is already given in the question. Answers will not be accepted without proper reasoning. **[2.5 Marks]**



H: Hash Function, PE: Public Encryption, PU_M: Public Key of M,
SE: Symmetric Encryption, K_{MN}: Symmetric Key between M and N
+: Concatenation, #: Compression Function

Q.8 Set. (C) The encryption side of PGP is shown below for the sender M and receiver N. Sender wants to protect the data from confidentiality as well as from the integrity attacks. Comment about the correctness of the procedure used by M in not more than 5 points. Do not assume more than what is already given in the question. Answers will not be accepted without proper reasoning. **[2.5 Marks]**



H: Hash Function, PE: Public Encryption, PU_N: Public Key of M,
SE: Symmetric Encryption, K_{MN}: Symmetric Key between M and N
+: Concatenation, #: Compression Function

Q.9 Set. (A) (i) Given that n = 126. Prime factorize n and calculate its discrete-log (using factors only) under base 13 which is a primitive root of 19. You are expected to use appropriate properties of discrete-log. (ii) Calculate Euler's Totient function value of n. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.9 Set. (B) (i) Given that n = 180. Prime factorize n and calculate its discrete-log (using factors only) under base 14 which is a primitive root of 19. You are expected to use appropriate properties of discrete-log. (ii) Calculate Euler's Totient function value of n. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.9 Set. (C) (i) Given that n = 150. Prime factorize n and calculate its discrete-log (using factors only) under base 15 which is a primitive root of 19. You are expected to use appropriate properties of discrete-log. (ii) Calculate Euler's Totient function value of n. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.10 Set. (A) Using the keyword "SECULAR" and the Vigenère Cipher technique, encrypt the message "REPUBLIC OF INDIA". Double quotation marks are not part of the key or the message. Space character needs to be taken as the 27th character of English. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.10 Set. (B) Using the keyword "STATES" and the Vigenère Cipher technique, encrypt the message "REPUBLIC OF INDIA". Double quotation marks are not part of the key or the message. Space character needs to be taken as the 27th character of English. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.10 Set. (C) Using the keyword "UNION" and the Vigenère Cipher technique, encrypt the message "REPUBLIC OF INDIA". Double quotation marks are not part of the key or the message. Space character needs to be taken as the 27th character of English. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.11 Set. (A) Using the keyword "PATRIOT" and the Vernam Cipher technique, encrypt the message "SECULAR". Double quotation marks are not part of the key or the message. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.11 Set. (B) Using the keyword "COUNTRY" and the Vernam Cipher technique, encrypt the message "SECULAR". Double quotation marks are not part of the key or the message. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**

Q.11 Set. (C) Using the keyword "GUJARAT" and the Vernam Cipher technique, encrypt the message "MANIPUR". Double quotation marks are not part of the key or the message. Show all the calculations. Direct answers or copy and paste from web/any tool will not be accepted. **[5 Marks]**