SAVEETHA SCHOOL OF ENGINEERING
SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES
COMPUTER SCIENCE AND ENGINEERING PROGRAMME

CSA51 – CRYPTOGRAPHY AND NETWORK SECURITY

Required Software

C / Java / Python

LAB QUESTIONS

1. Write a C program for Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.

2. Write a C program for monoalphabetic substitution cipher maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.

3. Write a C program for Playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

4. Write a C program for polyalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

5. Write a C program for generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C: C = E([a, b], p) = (ap + b) mod 26 A basic requirement of any encryption algorithm is that it be one-to-one. That is, if p q, then E(k, p) E(k, q). Otherwise, decryption is impossible, because more than one plaintext character maps intothe same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example,for a = 2 and b = 3, then E([a, b], 0) = E([a, b], 13) = 3.
a. Are there any limitations on the value of b?
b. Determine which values of a are not allowed.

6. Write a C program for ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is “B,” and the second most frequent letter of the ciphertext is “U.”Break this code.

7. Write a C program for the following ciphertext was generated using a simple substitution algorithm.
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83
(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8¶8*
;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806*81 (‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

Decrypt this message.
1. As you know, the most frequently occurring letter in English is e. Therefore, the first or second (or perhaps third?) most common character in the message is likely to stand for e. Also, e is often seen in pairs (e.g., meet, fleet, speed, seen, been,
agree, etc.). Try to find a character in the ciphertext that decodes to e.
2. The most common word in English is “the.” Use this fact to guess the characters that stand for t and h.
3. Decipher the rest of the message by deducing additional words.

8. Write a C program for monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated.
For example, using the keyword *CIPHER*, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: C I P H E R A B D F G J K L M N O Q S T U V W X Y Z

9. Write a C program for PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:

KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBNT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

10. Write a C program for Playfair matrix:

M F H I/J K
U N O P Q
Z V W X Y
E L A R G
D S T B C

Encrypt this message: Must see you over Cadogan West. Coming at once.

11. Write a C program for possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.

a. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?

12. a. Write a C program to Encrypt the message “meet me at the usual place at ten rather than eight oclock” using the Hill cipher with the key.

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

a. Show your calculations and the result.
b. Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

13. Write a C program for Hill cipher succumbs to a known plaintext attack if sufficient plaintext–ciphertext pairs are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted.

14. Write a C program for one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 . . . , then the first letter ofplaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of5 letters, and so on.

a. Encrypt the plaintext send more money with the key stream
9 0 1 7 23 15 21 14 11 11 2 8 9

b. Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plaintext cash not needed.

15. Write a C program that can perform a letter frequency attack on an additive cipher without human intervention. Your software should produce possible plaintexts in rough order of likelihood. It would be good if your user interface allowed the user to specify “give me the top 10 possible plaintexts.”

16. Write a C program that can perform a letter frequency attack on any monoalphabetic substitution cipher without human intervention. Your software should produce possible plaintexts in rough order of likelihood. It would be good if your user interface allowed the user to specify “give me the top 10 possible plaintexts.”

17. Write a C program for DES algorithm for decryption, the 16 keys (K1, K2, c, K16) are used in reverse order. Design a key-generation scheme with the appropriate shift schedule for the decryption process.

18. Write a C program for DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and that the second 24 bits of each subkey come from a disjoint subset of 28 bits of the initial key.

19. Write a C program for encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Both of which follow from the definition of CBC.
Which of the two would you choose:

a. For security?
b. For performance?

20. Write a C program for ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C1 obviously corrupts P1 and P2.
a. Are any blocks beyond P2 affected?
b. Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?

21. Write a C program for ECB, CBC, and CFB modes, the plaintext must be a sequence of one or more complete data blocks (or, for CFB mode, data segments). In other words, for these three modes, the total number of bits in the plaintext must be a positive multiple of the block (or segment) size. One common method of padding, if needed, consists of a 1 bit followed by as few zero bits, possibly none, as are necessary to complete the final block. It is considered good practice for the sender to pad every message, including messages in which the final message block is already complete. What is the motivation for including a padding block when padding is not needed?

22. Write a C program for Encrypt and decrypt in cipher block chaining mode using one of the following ciphers: affine modulo 256, Hill modulo 256, S-DES, DES. Test data for S-DES using a binary initialization vector of 1010 1010. A binary plaintext of 0000 0001 0010 0011 encrypted with a binary key of 01111 11101 should give a binary plaintext of 1111 0100 0000 1011. Decryption should work correspondingly.

23. Write a C program for Encrypt and decrypt in counter mode using one of the following ciphers: affine modulo 256, Hill modulo 256, S-DES. Test data for S-DES using a counter starting at 0000 0000. A binary plaintext of 0000 0001 0000 0010 0000 0100 encrypted with a binary key of 01111 11101 should give a binary plaintext of 0011 1000 0100 1111 0011 0010. Decryption should work correspondingly.

24. Write a C program for RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo f(n).

25. Write a C program for set of blocks encoded with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext

blocks has a common factor with n. Does this help us in any way?

26. Write a C program for RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

27. Write a C program for Bob uses the RSA cryptosystem with a very large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (A S 0, c, Z S 25) and then encrypting each number separately using RSA with large e and large n. Is this method secure? If not, describe the most efficient attack against this encryption method.

28. Write a C program for Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant ax mod q for some public number a. What would happen if the participants sent each other xa for some public number a instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers?

29. Write a C program for SHA-3 option with a block size of 1024 bits and assume that each of the lanes in the first message block (P0) has at least one nonzero bit. To start, all of the lanes in the internal state matrix that correspond to the capacity portion of the initial state are all zeros. Show how long it will take before all of these lanes have at least one nonzero bit. Note: Ignore the permutation. That is, keep track of the original zero lanes even after they have changed position in the matrix.

30. Write a C program for CBC MAC of a oneblock message X, say T = MAC(K, X), the adversary immediately knows the CBC MAC for the two-block message X || (X ⊕ T) since this is once again.

31. Write a C program for subkey generation in CMAC, it states that the block cipher is applied to the block that consists entirely of 0 bits. The first subkey is derived from the resulting string by a left shift of one bit and, conditionally, by XORing a constant that depends on the block size. The second subkey is derived in the same manner from the first subkey.
a. What constants are needed for block sizes of 64 and 128 bits?
b. How the left shift and XOR accomplishes the desired result.

32. Write a C program for DSA, because the value of k is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. This is not true of RSA signatures. Write a C program for implication of this difference?

33. Write a C program for Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits**.** Implement in C programming.

34. Write a C program for ECB, CBC, and CFB modes, the plaintext must be a sequence of one or more complete data blocks (or, for CFB mode, data segments). In other words, for these three modes, the total number of bits in the plaintext must be a positive multiple of the block (or segment) size. One common method of padding, if needed, consists of a 1 bit followed by as few zero bits, possibly none, as are necessary to complete the final block. It is considered good practice for the sender to pad every message, including messages in which the final message block is already complete. What is the motivation for including a padding block when padding is not needed?

35. Write a C program for one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 . . . , then the first letter ofplaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

36. Write a C program for Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C: C = E([a, b], p) = (ap + b) mod 26 A basic requirement of any encryption algorithm is that it be one-to-one. That is, if p q, then E(k, p) E(k, q). Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3, then E([a, b], 0) = E([a, b], 13) = 3.

37. Write a C program that can perform a letter frequency attack on any monoalphabetic substitution cipher without human intervention. Your software should produce possible plaintexts in rough order of likelihood. It would be good if your user interface allowed the user to specify “give me the top 10 possible plaintexts.”

38. Write a C program for Hill cipher succumbs to a known plaintext attack if sufficient plaintext–ciphertext pairs are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted. Implement in C programming.

39. Write a C program that can perform a letter frequency attack on an additive cipher without human intervention. Your software should produce possible plaintexts in rough order of likelihood. It would be good if your user interface allowed the user to specify “give me the top 10 possible plaintexts.”

40. Write a C program that can perform a letter frequency attack on any monoalphabetic substitution cipher without human intervention. Your software should produce possible plaintexts in rough order of likelihood. It would be good if your user interface allowed the user to specify “give me the top 10 possible plaintexts.”

41. Explain the process of deriving eighty 80-bitwords from 1024 bits for processing of a single blocks and also discuss single round function in SHA algorithm. Show the values of W16, W17, W18 and W19.

42. Explain the process of deriving a single block of 512-bits from the original message , padding and length is1 536 bits for processing of a single blocks and also discuss single round function in MD5 algorithm.(i.e, original message =1000,padding=472 and length=64 bit) using c program

43. Implementing Blowfish encryption in C involves using the Blowfish algorithm to encrypt and decrypt data. We can leverage the OpenSSL library, which provides a robust implementation of Blowfish. Below is an example demonstrating how to perform Blowfish encryption and decryption in C.

44. Implementing Triple DES (3DES) using the Data Encryption Standard (DES) algorithm three times to increase security. Here's a basic outline and example of how you can implement Triple DES in C. This example assumes that you have a basic understanding of C programming, encryption concepts, and how DES works

45. Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

46. Given a plain-text message and a numeric key, cipher/de-cipher the given text using Columnar Transposition Cipher The Columnar Transposition Cipher is a form of transposition cipher just like Rail Fence Cipher. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

47. Bob uses the SHA-3 cryptosystem with a block size of 512 bits and initializes the capacity lanes in the internal state matrix to all zeros. Each lane in the first message block (P0) is ensured to have at least one nonzero bit. Write a C program to show how many iterations it takes before all the capacity lanes have at least one nonzero bit, ignoring the permutation step.

48. Alice uses the SHA-3 algorithm with a block size of 1024 bits and initializes the capacity lanes in the internal state matrix with random nonzero values. Each lane in the first message block (P0) also contains

at least one nonzero bit. Write a C program to count the iterations required for all capacity lanes to become nonzero, disregarding the permutation step.

49. Write a C program that includes a string (char pointer) initialized with the value "Hello world". The program should XOR each character in this string with 0 and display the result.

50. Write a C program that contains a string (char pointer) with the value "Hello world". The program should AND and XOR each character in this string with 127 and display the result.

51. Write a C or Java program to implement the logic of the DES (Data Encryption Standard) algorithm.

52. Write a C or Java program to implement the logic of the Blowfish algorithm

53. Write the RC4 logic in Java. Using Java cryptography, encrypt the text "Hello world" with Blowfish. Generate your own key using the Java key tool.

54. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript

55. Demonstrate Intrusion Detection System (IDS) using Snort or any other tool.

56. User A wants to encrypt the message "Meet me very urgently" using DES algorithms at the sender end and then decrypt it at the receiver end before sending it to User B. Perform this operation using C program.

57. User C wishes to encrypt the message "welcome to CSE" using the AES algorithm before transmitting it to User D. The message will be decrypted by User D upon receiving it. Perform this operation using C program.

58. User A wants to send an encrypted message to User B using the Blowfish algorithm for secure communication. Implement using C program.

59. User A wishes to communicate with User B using Asymmetric Key Cryptography, specifically the RSA algorithm. The message will be encrypted by User A before being sent, and decrypted by User B upon receipt. Perform this operation using C

60. In order to transmit an encoded message between individuals, both parties must possess the cipher key to encrypt and decrypt the message. In the case of the caesar cipher, the key refers to the number of characters by which the cipher alphabet is shifted.For example, let's encrypt and decrypt the message 'defend the east wall of the castle' using a shift (key) of 1. Write a C program to implement the above operation.

61. For example, if message is ABC , and we shift each character by 3 characters, we will get DEF. Here key is 3. Given a message and key, compute its Caesar Cipher.

62.A plaintext was encrypted with a Caesar cipher with a shift of 7 (A maps to H). The resulting ciphertext is: Kvua qbknl h ivvr if paz jvcly What was the original plaintext? Implement the above operation.

63. Use Brute Force to crack the following Caesar ciphertext, to identify the person encoded: KRPCFIJNZWK. Implement the operation.

64. A plaintext was encrypted with a Caesar cipher, resulting in the following: DOOV ZHOO WKDW HQGV ZHOO Can you work out what the plaintext was?
67.After removing punctuation and spaces, a Caesar cipher was used to encrypt a plaintext. The resulting ciphertext is: cxknxawxccxkncqjcrbcqnzdnbcrxwfruurjvbqjtnbynjan Analyze the frequency of characters in the ciphertext to determine which ones are most common. What was the original plaintext?

65. Use any method (brute force, spotting patterns, frequency analysis, or invent your own) to decode the

following encoded with a Caesar Cipher. Adhz iypsspn, huk aol zspaof avclz Kpk nfyl huk nptisl pu aol dhil: Hss tptzf dlyl aol ivyvnvclz, Huk aol tvtl yhaoz vbanyhil. Ildhyl aol Qhiilydvjr, tf zvu! Aol qhdz aoha ipal, aol jshdz aoha jhajo! Ildhyl aol Qbiqbi ipyk, huk zobu Aol mybtpvbz Ihuklyzuhajo!

66.Encrypt the message "short example" with the keyword hill and a 2 x 2 matrix.Implement using C program.

67. Decrypt the ciphertext message "SYICHOLER" using the keyword *alphabet* using Hill Cipher technique.

68. Find the inverse of the following matrix whose entries are considered modulo 26:

$$\begin{pmatrix} 11 & 13 \\ 2 & 3 \end{pmatrix}$$

69. The matrix given in the last exercise was used as a key to a Hill cipher to encrypt a favourite vegetable of mine, and the resulting ciphertext was YGFI. What is the vegetable?

70. A 2×2 Hill cipher encrypted the plaintext SOLVED to give the ciphertext GEZXDS. Find the encryption matrix.

71. Suppose the matrix

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

is used for a 2 × 2 Hill cipher.
1. Compute the determinant. What is bad about this determinant?
2. Find two plaintexts that encrypt to the same ciphertext.

72. To encrypt a message using the rail fence cipher, you must first choose the number of rails. The message is then written diagonally in a zigzag pattern based on the selected number of rails. Finally, the characters along each rail are combined from left to right to create the encrypted message.Illustrate this process with the example of encrypting the message "RAILFENCE".

73. Using the keyword "KEY", the Vigenere's cipher encodes the message "Attack at Dawn" as follows: "Kttnyq da Xnhg". Implement the above operation using C.

74. The Kryptonian alphabet consists of only 5 letters whose frequencies of occurrence are shown below:

A	*B*	*C*	*D*	*E*
0.05	0.10	0.20	0.30	0.35

If a plaintext Kryptonian message is encoded using a Vigenere's Cipher with keyword "BED", determine the probability that the first and third letters of the message match.Implement the above operation using C program.

75.Consider the message “Cryptography is fun” with the key is “SECRETKEY”. Perform the Vignere operation.

76. The key for the columnar transposition cipher is a keyword e.g. GERMAN. The row length that is used is the same as the length of the keyword. To encrypt a piece of text, e.g.defend the east wall of the castle. Perform the operation using C program.

77.Alice configures the SHA-3 algorithm with a block size of 1024 bits, but this time, the initial state of the matrix is randomly set except for the capacity lanes, which are all zero. Each lane in the first message block (P0) has at least one nonzero bit. Write a C program to determine how many iterations are needed before all capacity lanes have at least one nonzero bit without considering permutation.

78. Bob is tasked with generating sub keys for CMAC where the block size can vary between 64, 128, and 256 bits. Describe how the sub key generation process adapts to different block sizes, including the constants used for XOR operations. Write a C program that generates sub keys for these block sizes.

79. Alice is working with a lightweight block cipher with a 48-bit block size. Explain the sub key generation process, including the left shift and conditional XOR steps, and suggest an appropriate polynomial. Write a C program to demonstrate the sub key generation.

80. Bob wants to use CMAC with a stream cipher that has a 32-bit block size. Describe the process of generating sub keys using left shifts and XOR operations, including an appropriate polynomial for the block size. Write a C program to generate the sub keys and explain the security considerations.

81. Alice and Bob use a post-quantum secure variant of Diffie-Hellman, such as the one based on lattice problems. Explain the differences from the traditional protocol and its security advantages against quantum adversaries. Can Eve break this system or find the secret numbers using quantum computing?

82. Alice and Bob implement a key confirmation step after exchanging Diffie-Hellman keys to ensure they both derived the same shared key. Describe this process and its benefits. Can Eve interfere with or spoof the key confirmation step? How does this enhance the security of the key exchange.

83. Alice and Bob use the traditional Diffie-Hellman protocol to agree on a symmetric key, which they then use for AES encryption. Describe the process, including key exchange and encryption. What challenges might Eve face in trying to break the encryption or find the secret numbers?

84.Explain the Kerberos authentication process and the role of the Key Distribution Center (KDC), Ticket Granting Ticket (TGT), and Service Tickets. Write a C program to simulate the Kerberos authentication process between a client, KDC, and a service server. Include steps such as initial authentication, obtaining a TGT, requesting a service ticket, and accessing the service.

85.Write a C program to implement the signature scheme named Digital Signature Standard (DSS) – Euclidean Algorithm.

86. A diplomat needs to send an urgent encrypted message "URGENT MEETING AT NOON" using the Playfair cipher with the key phrase "CONFIDENTIAL". Construct the key matrix and encrypt the message.

87. A spy has received the ciphertext "GATLMZCLQQYG" and knows it was encrypted using the Play fair cipher with the key phrase "UNDERCOVER". The spy needs to decrypt the message. Construct the key matrix and decrypt the message.

88. Write a C program that encrypts a message using the Playfair cipher. The key phrase is "CLASSIFIED", and the plaintext message is "HELLO AGENT".

89. Write a C program that encrypts a message using the Hill cipher with a given 2x2 key matrix. The key matrix is [[3, 3], [2, 5]] and the plaintext message is "HELP".

90. Write a C program that encrypts a message using the Caesar cipher with a given shift value. The shift value is 3, and the plaintext message is "ATTACK AT DAWN".

91. Implement the Caesar cipher in C and encrypt the message "SECURITY" with shift values of 1, 5, and 13.

92. Alice and Bob want to securely share a secret key using the Diffie-Hellman key exchange algorithm. Write a C program to simulate the key exchange process using the prime number p=23 and the primitive

root g=5.

93. Analyze how different choices of prime numbers p and primitive roots g affect the Diffie-Hellman key exchange. Implement the key exchange process in C using p=29 and g=2.

94. Alice wants to send a secure message to Bob using the RSA algorithm. The public key components are e=3 and n=33, and the private key component is d=7. The plaintext message is "HELLO". Write a C program that implements RSA encryption and decryption.

95. Implementing the SHA-256 hash function in C to compute the hash of a given message. Write a C program that computes the SHA-256 hash of the message "Hello, World!”

96. Perform wireless audit on an access point or a router and decrypt WEP and WPA.

97. Calculate message digest of a text using SHA-1 algorithm.

98. Installation of rootkits and study about the variety of options

99. Analyse the security vulnerabilities of Email Application

100. Study of different types of vulnerabilities of hacking a website.