Register Number									

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

Continuous Assessment Test – II

Answer Key

Degree & Branch	B.E CSE				**Semester**	V
Subject Code & Name	UCS1505 & INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES				**Regulation: 2018**	
Academic Year	2022-23 ODD	**Batch**	2020-24	**Date**	**19.10.2022**	**FN**
Time: 8.15 – 9.45 AM (90 Minutes)	**Answer All Questions**				**Maximum: 50 Marks**	

Part – A (6×2 = 12Marks)

K2	1. What is diffusion and confusion? Confusion and diffusion area unit the properties for creating a secure cipher. Each Confusion and diffusion area unit wont to stop the secret writing key from its deduction or ultimately for preventing the first message. Confusion is employed for making uninformed cipher text whereas diffusion is employed for increasing the redundancy of the plain text over the foremost a part of the cipher text to create it obscure. The stream cipher solely depends on confusion, or else, diffusion is employed by each stream and block cipher.	CO1	1.4.1
K2	2. Explain the avalanche effect? In cryptography, the avalanche effect is a term associated with a specific behavior of mathematical functions used for encryption. Avalanche effect is considered as one of the desirable property of any encryption algorithm. A slight change in either the key or the plain-text should result in a significant change in the cipher-text. This property is termed as avalanche effect. In simple words, it quantifies the effect on the cipher-text with respect to the small change made in plain text or the key.	CO1	1.3.1
K2	3. Outline Fermat's little theorem. Fermat's Theorem: $a^{p-1} mod\ p = 1$ where p is prime and gcd(a,p)=1 also known as Fermat's Little Theorem useful in public key and primality testing	CO3	1.4.1
K2	4. Compare DES and AES AES — DES AES stands for Advanced Encryption Standard — DES stands for Data Encryption Standard	CO1	1.3.1 1.4.1

<table>
<tr><td></td><td><table>
<tr><td>Byte-Oriented.</td><td>Bit-Oriented.</td></tr>
<tr><td>Key length can be 128-bits, 192-bits, and 256-bits.</td><td>The key length is 56 bits in DES.</td></tr>
<tr><td>Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)</td><td>DES involves 16 rounds of identical operations</td></tr>
<tr><td>The structure is based on a substitution-permutation network.</td><td>The structure is based on a Feistel network.</td></tr>
<tr><td>The design rationale for AES is open.</td><td>The design rationale for DES is closed.</td></tr>
<tr><td>The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition</td><td>The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation</td></tr>
<tr><td>AES can encrypt 128 bits of plaintext.</td><td>DES can encrypt 64 bits of plaintext.</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>K3</td><td>5. Apply Euclid’s algorithm to find the gcd (1076, 1970)

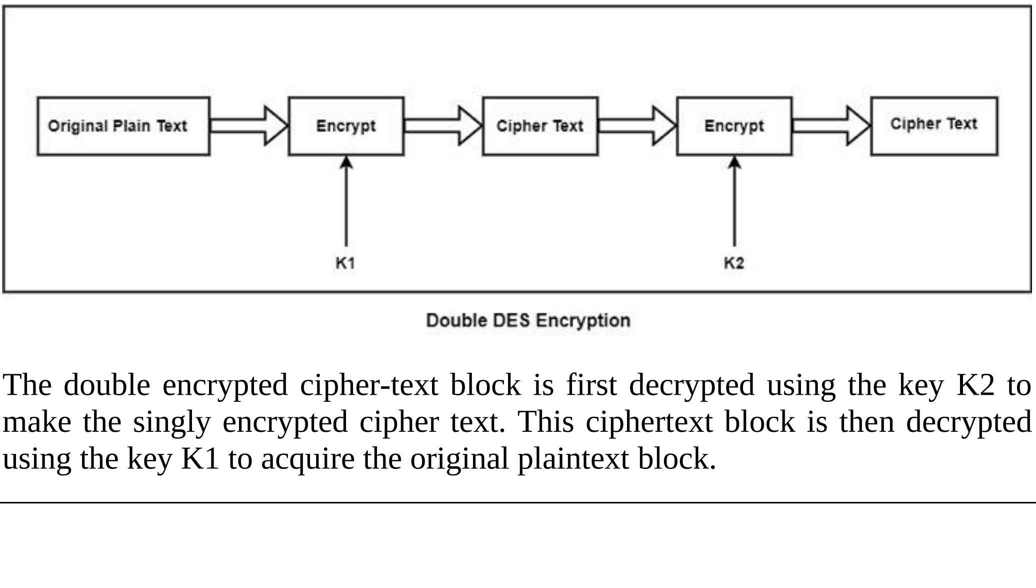
1970= 1 x 1076 + 894 gcd(1076, 894)
1076= 1 x 894 + 182 gcd(894, 182)
894 = 4 x 182 + 166 gcd(182, 166)
182 = 1 x 166 + 16 gcd(166, 16)
166 = 10 x 16 + 6 gcd(16, 6)
16 = 2 x 6 + 4 gcd(6, 4)
6 = 1 x 4 + 2 gcd(4, 2)
4 = 2 x 2 + 0 gcd(2, 0)
Therefore, gcd(1970, 1076) = 2
6.</td><td>CO3</td><td>1.3.1
2.1.3</td></tr>
<tr><td>K2</td><td>7. Explain any two algebraic structures used in cryptographic algorithms.
Group: a set S of elements or "numbers" may be finite or infinite with some operation '.' so G=(S,.)
Obeys CAIN:
Closure: a,b in S, then a.b in S
Associative law: (a.b).c = a.(b.c)
has Identity e: e.a = a.e = a
has inverses a^{-1} : $a:a^{-1}$ = e
if commutative a.b = b.a then forms an abelian group
Ring: a set of "numbers" with two operations (addition and multiplication) which form: an abelian group with addition operation and multiplication: has closure -is associative-distributive over addition: a(b+c) = ab + ac
if multiplication operation is commutative, it forms a commutative ring
if multiplication operation has an identity and no zero divisors, it forms an integral domain</td><td>CO3</td><td>1.4.1</td></tr>
</table>

Part – B (3×6 = 18 Marks)

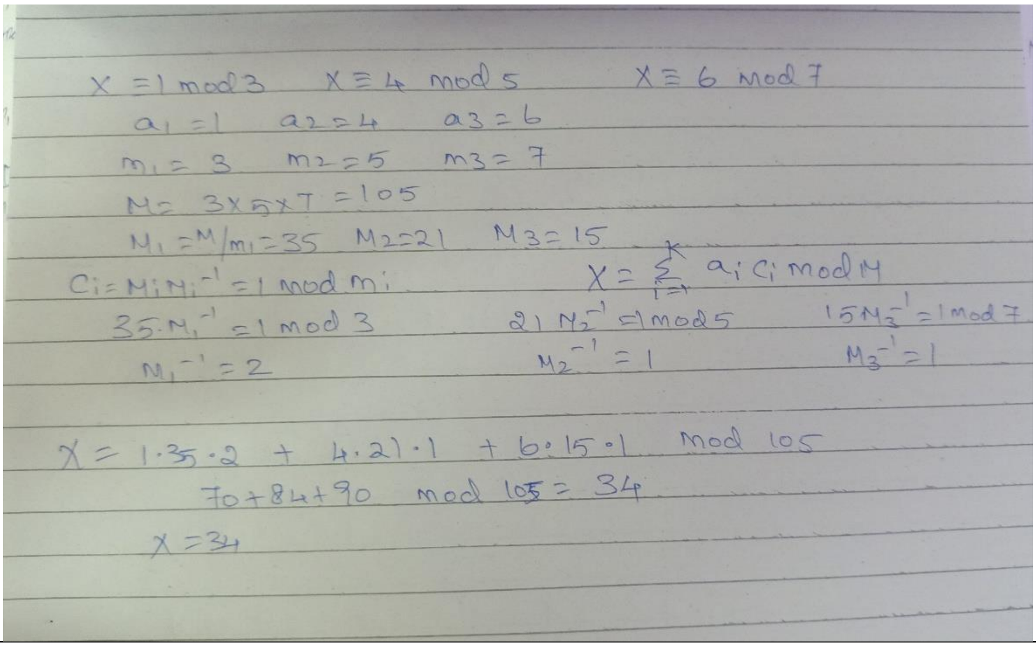
K2	8. What is a message authentication code? What is the difference between a message authentication code and a one-way hash function? A message authentication code (MAC) is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data. A MAC requires two inputs: a message and a secret key known only to the originator of the message and its intended recipient(s). The main difference is conceptual: while hashes are used to guarantee the integrity of data, a MAC guarantees integrity AND authentication. This means that a hashcode is blindly generated from the message without any kind of external input: what you obtain is something that can be used to check if the message got any alteration during its travel. A MAC instead uses a private key as the seed to the hash function it uses when generating the code: this should assure the receiver that, not only the message hasn't been modified, but also who sent it is what we were expecting: otherwise an attacker couldn't know the private key used to generate the code.	CO1	1.4.1 13.3.1
K3	9. Solve using Euler's Totient function Ø(440), Ø(27) and Ø(231) Ø(440) = 160 Ø(27) =18 Ø(231)= 120	CO3	1.4.1 13.3.1
K3	10. Apply extended Euclid algorithm to find the multiplicative inverse of 23 mod 100. 100=23*4+8 23=8*2+7 8=7*1+1 7=1*7+0 Now in revers way 1=8-(7*1) 1=8-(23-8*2) 1=8-23+8*2 1=3*8-23 1=3x(100-23x4)-23=3x100-12x23-23=3x100-13x23 So the multiplicative inverse of 23 mod 100 is -23 or 87(-23 mod 100)	CO3	1.4.1 13.3.1

Part – C (2×10 = 20 Marks)

K2	11. Alice wants to send message M to Bob, without Eve observing it. Alice and Bob have agreed to use a symmetric cipher Data Encryption Standard (DES). Key exchange has already been done, and so they share a key K for a specific encryption algorithm E.	CO1	1.4.1 13.3.1

	a. Outline the steps that Alice must follow for encrypting M and sending it to Bob. b. Outline the steps that Bob must follow for decrypting the received ciphertext C Alice Applies DES encryption on M using the following steps 1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function. 2. The initial permutation (IP) is then performed on the plain text. 3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT). 4. Each LPT and RPT goes through 16 rounds of the encryption process. 5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block. 6. The result of this process produces the desired 64-bit ciphertext. The encryption process step (step 4, above) is further broken down into five stages: Key transformation Expansion permutation S-Box permutation P-Box permutation XOR and swap For decryption, we use the same algorithm, and we reverse the order of the 16 round keys.		
OR			
K2	11.What is double DES? What kind of attack on double DES makes it useless? What is triple DES? Double DES is an encryption approach which uses two example of DES on same plain text. In both examples it provides different keys to encode the plain text. Double DES is easily to learn. Double DES uses two keys, such as k1and k2. It can implement DES on the original plain text using k1 to get the encrypted text. It can implement DES on the encrypted text, but this time with the different key k2. The final output is the encryption of encrypted text  Original Plain Text Encrypt Cipher Text Encrypt Cipher Text K1 K2 Double DES Encryption The double encrypted cipher-text block is first decrypted using the key K2 to make the singly encrypted cipher text. This ciphertext block is then decrypted using the key K1 to acquire the original plaintext block.	CO1	1.4.1 13.3.1

	Double DES needed a key search of (22*56), i. e. , 2^{112}keys. It introduce the terms of the meet-in-the-middle attack. This attack contains encryption from one end, decryption from the other and connecting the results in the middle. Consider that the cryptanalyst understand two basic pieces of information including P (a plain-text block) and C (the corresponding final cipher-text block) for a message. The numerical expression of Double DES as shown in the figure. The result of the first encryption is known as T and is indicated as T = Ek1(P) [i.e., encrypt the block P with key K1]. After this encrypted block is encrypted with another key K2, it indicate the result as C = EK2(EK1(P)) [i.e., encrypt the already encrypted block T, with a different key K2, and call the final ciphertext as C]. Given a plaintext P and two encryption keys K1 and K2, ciphertext C is produced as C = Ek2(Ek1, (m)) decryption needed that the keys be used in reverse order − P = Dk1(Dk2, (C)) A Meet-in-the-Middle (MitM) Attack is a type of cryptanalytic attack where the attacker need some type of space or time tradeoff to support the attack. MITM attempt can decrease the amount of difficulty needed to perform the assault in its ori The encryption-decryption process is as follows − Encrypt the plaintext blocks using single DES with key K1. Now decrypt the output of step 1 using single DES with key K2. Finally, encrypt the output of step 2 using single DES with key K3. The output of step 3 is the ciphertext. Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1. Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES. Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 again. Therefore, 2TDES has a key length of 112 bits. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.		
K3	12. Apply the Chinese remainder Theorem to solve the following congruences and explain the algorithm. $x \equiv 1 \bmod 3$ $x \equiv 4 \bmod 5$ $x \equiv 6 \bmod 7$	CO2	2.1.3 13.3.1

	 $X = 1 \bmod 3$ $X \equiv 4 \bmod 5$ $X \equiv 6 \bmod 7$ $a_1 = 1$ $a_2 = 4$ $a_3 = 6$ $m_1 = 3$ $m_2 = 5$ $m_3 = 7$ $M = 3 \times 5 \times 7 = 105$ $M_1 = M/m_1 = 35$ $M_2 = 21$ $M_3 = 15$ $C_i = M_i M_i^{-1} = 1 \bmod m_i$ $X = \sum_{i=1}^{k} a_i C_i \bmod M$ $35 \cdot M_1^{-1} = 1 \bmod 3$ $21 M_2^{-1} = 1 \bmod 5$ $15 M_3^{-1} = 1 \bmod 7$ $M_1^{-1} = 2$ $M_2^{-1} = 1$ $M_3^{-1} = 1$ $X = 1 \cdot 35 \cdot 2 + 4 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1 \bmod 105$ $70 + 84 + 90 \bmod 105 = 34$ $X = 34$		
OR			
K3	13. Make use of a Feistel cipher composed of sixteen rounds with a block length of 128 bits and a key length of 128 bits. Suppose that, for a given k, the key scheduling algorithm determines values for the first eight round keys, $k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8$, $k_9 = k_8,\ k_{10} = k_7,\ k_{11} = k_6,\ k_{12} = k_5,\ k_{13} = k_4,\ k_{14} = k_3,$ $k_{15} = k_2,\ k_{16} = k_1,$ Suppose you have a ciphertext c. Explain how, with access to an encryption oracle, you can decrypt c and determine m using just a single oracle query. (5 Marks) Consider a notion of indistinguishable encryption for multiple distinct messages, i.e., where a scheme need not hide whether the same message is encrypted twice. Give a suitable definition Complete set of keys are $k9 = k8$, $k10 = k7$, $k11 = k6$, $k12 = k5$, … , … , … , $k16 = k1$	CO3	2.1.3 13.3.1

	From the given key schedule encryption and decryption have similar keys which are identical. Suppose an encryption oracle is used to encrypt the message m is encrypt(m, key_value)=c. The ciphertext will be returned by an oracle C. Again decryption key used is oracle ciphertext C to decrypt the message decrypt(m, key_value)=m Hence, use of ciphertext is unsafe to create plaintext using the technique. Let G be a pseudorandom generator with expansion factor `(n). Define a fixed-length private-key encryption scheme for messages of length `(n) as follows: Gen: on input 1n, choose uniform k ∈ {0,1}n and output it as the key. Enc: on input a key k ∈ {0,1}n and a message m ∈ {0,1}`(n), output the ciphertext c := G(k) ⊕ m. Dec: on input a key k ∈ {0,1}n and a ciphertext c ∈ {0,1}`(n), output the message m := G(k) ⊕ c.		

Prepared By	Reviewed By	Approved By
Course Coordinator	PAC Team	HOD

Guidelines for the Preparation of Question Paper

1. It is necessary that the question paper should be of the pattern approved and standard as stipulated and confined to the syllabus.
2. The question paper should be set in accordance with Bloom's Taxonomy (as in the attachment). The same knowledge level of questions should be asked in both either / or questions even if the questions have sub divisions. The Knowledge level (K1 to K6) should be mentioned against each question and subdivisions.
3. The Course outcomeshould be mentioned against each question and subdivisions.
4. The question paper should contain questions to test all the knowledge levels. 50% of questions shall be prepared to test the base level competencies (Remembering (K1) and Understanding (K2)) of students. 20 to 25% of questions shall be prepared to test the medium level competencies (Applying (K3), Analyzing (K4)) of students. Remaining questions shall be prepared to test the highest level of competencies (Evaluating (K5), Creating (K6)) of students.
5. The font shall be Times New Roman with font size 12.
6. All questions should be neatly typed on one side of the A4 sheet.
7. All figures should be neatly drawn using available drawing tools or imaging tools.
8. The details of the examination such as the programme, regulation, semester, subject code and name, maximum marks, duration, number of questions to be should be stated clearly.
9. The marks assigned to each question and subdivisions question should be mentioned clearly.
10. Special instructions such as Data books, Tables, Charts, Graph sheets to be supplied are to be permitted are to be mentioned in the question paper.
11. S.I. units must be adopted throughout the question paper. Abbreviations of all kinds except those in special subjects should be avoided. Mathematical symbols and index figures should be clearly delineated.

Revised Bloom's Taxonomy Knowledge Levels Action Verbs

Definitions	Bloom'sDefinition	Action Verbs
Remembering (K1)	ExhibitMemory of previously learned material by recalling facts, terms, basic concepts and answers.	Choose, Define, Find, Flow, Label, List, Match, Name, Omit, Recall, Relate, Select, Show, Spell,Tell, What, When, Where, Which, Who, Why
Understanding (K2)	Demonstrate understanding of facts and ideas by organizing, comparing, translating, interpreting, giving descriptions and stating main ideas.	Classify, Compare, Contrast, Demonstrate, Explain, Extend, Illustrate, Infer, Interpret, Outline, Relate, Rephrase, Show, Summarize, Translate
Applying (K3)	Solve problems to new situations by applying acquired knowledge facts, techniques and rules in a different way.	Apply, Build, Choose, Construct, Develop, Experiment, With, Identity, Interview, Make use of, Model, Organize, Plan, Select, Solve, Utilize
Analyzing (K4)	Examine and break information into parts by identifying motives or causes. Make inference and find evidence to support generations.	Analyze, Assume, Categorize, Classify, Compare, Conclusion, Contrast, Discover, Dissect, Distinguish, Divide, Examine, Function, Inference, Inspect, List, Motive, Relationships, Simplify, Survey, Take part in, Test for, Theme
Evaluating (K5)	Present and defend opinions by making judgments about information, validity of ideas or quality of work based on a set of criteria.	Agree, Appraise, Assess, Award, Choose, Compare, Conclude, Criteria, Criticize, Decide, Deduct, Defend, Determine, Disprove, Estimate, Evaluate, Explain, Importance, Influence, Interpret, Judge, Justify, Mark, Measure, Opinion, Perceive, Prioritize, Prove, Rate, Recommend, Rule on, Select, Support, Value
Creating (K6)	Compile information together in a different way by combining elements in a new pattern or proposing alternative solutions.	Adapt, Build, Change, Choose, Combine, Compile, Compose, Construct, Create, Delete, Design, Develop, Discuss, Elaborate, Estimate, Formulate, Happen, Imagine, Improve, Invent, Make up, Maximize, Minimize, Modify, Original, Originate, Plan, Predict, Propose, Solution, Solve, Suppose, Test, Theory