COURSEPACK (Winter 2025-26)

1. THE SCHEME

Course Title	Fundamentals of Cyber Security			Course Type				Theory	
Course Code	R1UC426T			Class				B-Tech Core and All specialization (II-YR)	
Instruction delivery	**Activity**	**Credits**	**Credit Hours**	**Total Number of Classes per Semester**				**Assessment in Weightage**	
	Lecture	3	3						
	Tutorial	0	0	**Theory**	**Tutorial**	**Practical**	**Self-study**	**CIE**	**SEE**
	Practical	0	0						
	Self-study	0	0						
	Total	3	3	40	0	0	0	50%	100%
Course Lead	Dr. Mukesh Kumar		Course Coordinator	Dr. Garima Pandey					
Names Course Instructors	**Theory**			**Practical**					
	1 Indrajeet Gupta 2 Siddharth Gautam 3 FIROJ AHAMAD 4 Alok Kumar 5 Pawan Kumar 6 Omdev 7 Mrinmoy Kayal 8 Ms. Rajeshwari Sisodia 9 Dr Neeraj Tantubay 10 Garima Verma 11 Sunil Kumar Patel 12 Priyanka Das 13 Mr. Aditya Raj Shukla 14 Ms. Garima Pandey 15 Mr. Deepak Sonker 16 Bhupal Arya 17 Mr. S P Ramesh 18 Dr. Neha Kumari 19 Bhupal Arya 20 Dr. D. Salangai Nayagi 21 Dr. Nidhi Agarwal 22 Mr. Rishabh Prasad 23 Mukesh Kumar 24 Dr. Aditya K Saxena 25 Bijay Singh 26 Ms. Rajeshwari Sisodia								

2. COURSE OVERVIEW

Cyber Security is base for providing different security services like confidentiality, integrity and ensuring availability. Network Security encompasses various security measures, such as, file encryption and firewalls, to safeguard digital assets. This course presupposes that student possesses a strong foundation in computing and aims to elucidate the dynamic realm of network security. By delivering into the critical aspects of building resilience against cyber threats, this course equips students with the knowledge needed to navigate this evolving landscape effectively.

3. COURSE OBJECTIVES

This course is designed to introduce students to classical encryption techniques, including DES, RSA encryption and decryption. It also aims to clarify authentication requirements and the utilization of various cryptographic methods such as MAC, MD5, RIPEMD, HMAC, digital signatures, with a specific focus on their applications in the realms of communication and e-commerce. Additionally, students will gain hands-on experience by developing programs for encryption and decryption techniques.

4. PREREQUISITE COURSE

PREREQUISITE COURSE REQUIRED	No	
If, yes please fill in the Details	Course code	Course Title
	NA	NA

5. PROGRAM OUTCOMES (POs):

PO No.	Description of the Program Outcome
PO1	Engineering Knowledge: Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop to the solution of complex engineering problems.
PO2	Problem Analysis: Identify, formulate, review research literature and analyse complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4).
PO3	Design/Development of Solutions: Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5).
PO4	Conduct Investigations of Complex Problems: Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).
PO5	Modern Tool Usage: Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6).
PO6	The Engineer and The World: Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).
PO7	Ethics: Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9).
PO8	Individual and Collaborative Team work: Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.

PO9	Communication: Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences.
PO10	Project Management and Finance: Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one’s own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments..
PO11	Life-Long Learning: Recognize the need for, and have the preparation and ability for: i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8).

6. PROGRAM SPECIFIC OUTCOMES (PSOs):

Program Specific Outcomes (PSO) are statements that describe what the graduates of a discipline-specific program should be able to do. Two to Three PSOs per program should be designed.

PO No.	Description of the Program-Specific Outcome
PSO1	Have the ability to work with emerging technologies in Computer Science and Engineering requisite to Industry 4.0.
PSO2	Demonstrate Engineering Practice learned through industry internship and research project to solve live problems in various domains.

7. COURSE CONTENT (THEORY)

CONTENT (Syllabus)

THEORY:

Introduction: Cyber Security Concepts, Security Attacks, Security Services, Security Mechanism, OSI Security Architecture, A Model for Network Security, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques.

Fundamentals of cryptography Introduction to Cryptography, DES, Key generation, DES Encryption, DES Decryption S-Boxes, Strength of DES, AES. Public Key Cryptography, Principles of Public Key Cryptosystems, Fermat’s and Euler’s Theorems, The RSA Algorithm, Key Management, Diffie-Hellman Key Exchange.

Hash functions & digital signatures: Message Authentication and Hash Functions, Authentication Requirements, Authentication Functions, Message Authentication Codes, Message Digest Algorithm, Secure Hash Algorithms, Digital Signature concepts.

Ethical hacking concepts & Cyber Laws: Basics of digital forensics, Indian IT Act & Cyber Laws, Cyber ethics, compliance & reporting, Firewall, Types of Firewall, Secure communication protocols (SSL/TLS, HTTPS)

8. COURSE OUTCOMES (COs)

After the completion of the course, the student will be able to:

CO No.	Description of the Course Outcome
R1UC426T.1	**Recall** fundamental cyber security concepts including security attacks, services, mechanisms, OSI security architecture, and network security models.
R1UC426T.2	**Explain** cryptographic principles and techniques including symmetric ciphers, DES, AES, public key cryptography, RSA, and key exchange mechanisms.
R1UC426T.3	**Apply** cryptographic algorithms, hash functions, and digital signature techniques to ensure confidentiality, integrity, and authentication.
R1UC426T.4	**Explain and apply** ethical hacking concepts, cyber laws, firewalls, and secure communication protocols (SSL/TLS, HTTPS) for secure systems.

9. TAXONOMY LEVEL OF THE COURSE OUTCOMES

Mapping of COs with Bloom's Level

CO No.	Remember **KL1**	Understand **KL 2**	Apply **KL 3**	Analyse **KL 4**	Evaluate **KL 5**	Create **KL 6**
R1UC701T.1	√		√			
R1UC701T.2			√			
R1UC701T.3						
R1UC701T.4			√			
R1UC701T.5		√				

10. COURSE ARTICULATION MATRIX

COs#/ POs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
R1UC701T.1	-	2	-	-	-	-	-	-	-	-	-	-	-	-
R1UC701T.2	1	3	1	-	-	-	-	3	-	-	-	-	2	2
R1UC701T.3	2	-	-	-	3	1	-	-	2	1	-	1	2	2
R1UC701T.4	-	2	2	-	1	-	-	-	1	1	2	-	1	-
R1UC701T.5	-	-	-	-	-	3	3	-	3	-	-	1	1	1

Note: 1-Low, 2-Medium, 3-High \ *first semester first course and first Course Outcome

11. TYPICAL EXAMPLE OF COURSES, CREDIT HOURS AND TEACHING HOURS

Type of Course	Credits Hours					Hours of engagement/ Week					12 weeks/ semester	Remarks
	Theory	Tutorial	Practical	Self-study	Total	Theory	Tutorial	Practical	Self-study	Total	Total no. of classes	
Theory Course	3	0	0	0	3	3	0	0	0	3	40	40 classes for theory

*1 credit = 3 self-learning hours (Not to mention in the lesson plan)

L-No	Topic for Delivery	Tutorial / Practical Plan	Skill	Competency
1	**Introduction:** Cyber Security Concepts	Theory		
2	Security Attacks	Theory	Exploring Basics of Cyber Security	CO1
3	Security Services, Security Mechanism	Theory		
4	OSI Security Architecture	Theory		
5	A Model for Network Security	Theory		
6	Symmetric Cipher Model	Theory		
7	Substitution Techniques	Theory		
8.	Substitution Techniques	Theory		
9	Transposition Techniques	Theory		
10.	Transposition Techniques	Theory		
11.	**Fundamentals of cryptography** Introduction to Cryptography	Theory		
12.	DES, Key generation	Theory		
13.	DES Encryption, DES Decryption	Theory		
14.	S-Boxes, Strength of DES	Theory		
15	AES. Public Key Cryptography	Theory		
16	Principles of Public Key Cryptosystems	Theory		
17	Fermat’s and Euler’s Theorems	Theory		
18	The RSA Algorithm	Theory		
19	Key Management, Diffie-Hellman Key Exchange.	Theory	Apply Classical encryption and decryption technique like substitution for securing messages in a	CO2
20	Revision : case study & industrial applications	Theory		
21	**Hash functions & digital signatures**	Theory		
22	Message Authentication and Hash Functions	Theory		
23	Authentication Requirements	Theory		

			network.	
24	Authentication Functions	Theory	Apply Asymmetric cryptographic algorithms l ike RSA for network security	CO3
25	Message Authentication Codes	Theory		
26	Message Digest Algorithm	Theory		
27	Secure Hash Algorithms	Theory		
28	Digital Signature concepts	Theory		
29	Message Authentication and Hash Functions	Theory		

30	Revision : case studey & industrial applications	Theory	Ethical hacking concepts & Cyber Laws	CO4
31	**Ethical hacking concepts & Cyber Laws**	Theory		
32	Basics of digital forensics	Theory		
33	Indian IT Act & Cyber Laws	Theory		
34	Cyber ethics, compliance & reporting, Firewall	Theory		
35	Types of Firewall	Theory		
36	Secure communication protocols (SSL/TLS, HTTPS)	Theory		
37	Secure communication protocols : SSL/TLS/HTTPS	Theory		
38	Cyber ethics, compliance & reporting, Firewall	Theory		
39	Revision : case studey & industrial applications	Theory		
40	Revision : case studey & industrial applications	Theory		

12. BIBLIOGRAPHY

Text Books

1) Stallings, W. Cryptography and Network Security: Principles and Practice, 4th ed., Prentice Hall PTR.,2006

Reference books:

1) Kaufman, c., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nded., Prentice Hall PTR., 2002.
2) Cryptography and Network Security; McGraw Hill; Behrouz A Forouzan.
3) Atul Kahate, Cryptography and Network Security, McGraw Hill.
4) Johannes A. Buchmann, "Introduction to Cryptography", Springer-Verlag.

Journals/Magazines/Govt. Reports/Gazatte/Industry Trends

Journals:

1. Journal of Network and Computer Applications
2. **IEEE Transactions on Dependable and Secure Computing**

Magazines:

1. SC Magazine
2. Dark Reading
3. CSO Online

Webliography

1. https://csrc.nist.gov/
2. https://owasp.org/
3. http://almuhammadi.com/sultan/sec_books/Whitman.pdf

SWAYAM/NPTEL/MOOCs Certification /Industry Courses

https://swayam.gov.in/nd1_noc20_cs92/preview https://cisco.netacad.com

https://login.paloaltonetworks.com/lms/PreRegister?UserType=CUST&source=Beacon

13. COURSE ASSESSMENT

Assessment forms an integral part of curriculum design. A learning-teaching system can only be effective if the student's learning is measured at various stages which means while the student processes learning (Assessment for Learning) a given content and after completely learning a defined content (Assessment of Learning). Assessment for learning is referred to as formative assessment, that is, an assessment designed to inform instruction.

The ability to use and apply the knowledge in different ways may not be the focus of the assessment. With regard to designing assessments, the faculty members must be willing to put in the time required to create a valid, reliable assessment, that ideally would allow students to demonstrate their understanding of the information while remaining. The following are the five main areas that assessment reporting should cover.

1. **Learning Outcomes**: At the completion of a program, students are expected to know their knowledge, skills, and attitude. Depending on whether it is a UG or PG program, the level of sophistication may be different. There should be no strict rule on the number of outcomes to be achieved, but the list should be reasonable, and well-organized.
2. **Assessable Outcomes**: After a given learning activity, the statements should specify what students can do to demonstrate. Criteria for demonstration are usually addressed in rubrics and there should be specific examples of work that doesn't meet expectations, meets expectations, and exceeds expectations. One of the main challenges is faculty communication whether all faculty agreed on explicit criteria for assessing each outcome. This can be a difficult accomplishment when multiple sections of a course are taught or different faculty members. Hence there is a need for common understanding among the faculty on what is assessed and how it is assessed.
3. **Assessment Alignment**: This design of an assessment is sometimes in the form of a curriculum map, which can be created in something as easy as an Excel spreadsheet. Courses should be examined to see which program outcomes they support, and if the outcome is assessed within the course. After completion, program outcomes should be mapped to multiple courses within the program.
4. **Assessment Planning**: Faculty members need to have a specific plan in place for assessing each outcome. Outcomes don't need to be assessed every year, but faculty should plan to review the assessment data over a reasonable period of time and develop a course of action if the outcome is not being met.
5. **Student Experience**: Students in a program should be fully aware of the expectations of the program. The program outcomes are aligned on the syllabus so that students are aware of what course outcomes they are required to meet, and how the program outcomes are supported. Assessment documents should clearly communicate what is being done with the data results and how it is contributing to the improvement of the program and curriculum.

Designing quality assessment tools or tasks involves multiple considerations if it is to be fit for purpose. The set of assessments in a course should be planned to provide students with the opportunity to learn as they engage with formative tasks as well as the opportunity to demonstrate their learning through summative tasks. Encouraging the student through the use of realistic, authentic experiences is an exciting challenge for the course faculty team, who are responsible for the review and quality enhancements to assessment practices.

14. FORMATIVE AND SUMMATIVE ASSESSMENT

Assessment Pattern for Theory Course:

Type of Course (T)	CIE			Total Marks		Final Marks CIE*0.5+SEE*1
	IA1#	MTE	IA2#	CIE	SEE	
THEORY	25	50	25	100	50	100

#Typical Rubric for the Internal Assessments

Type of Assessment Tools	QUIZ	AAT$/MOOC Certifications
Internal Assessments	10	15

$AAT is Literature survey, Seminar, Assignment, Term Paper, Slip Test (or) MOOC Certificate relevant to the course

15. PASSING STANDARDS

Passing Criteria for Different Course Types Effective from AY 2022-23 Onwards

S.No.	Course Type	Passing Criterion
1.	**Theory Course (T)**	A student shall secure a minimum of **30% of the maximum marks** in the semester-end examination (SEE/ETE) and **40% of aggregate marks** in the course including Continuous internal examination (CIE) and SEE/ETE marks. i.e., the minimum Passing Grade is "P".

Note: Students unable to meet the overall passing criteria as mentioned shall be eligible for the following options to clear the course:

- Appear in the Back Paper Examinations and have to meet the criteria to score 40% in marks overall
- Appear in summer examinations (Internal +External) to meet the criteria as mentioned.

16. PROBLEM-BASED LEARNING/CASE STUDIES/CLINICS

S.No	Problems	KL
1.	Use the one-time pad method with key "XMCKL" to encipher the message "HELLO".	K3
2.	A 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.	K6
	One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. The particular scheme discussed in this problem is from one of the best suspense novels involving secret codes, Talking to Strange Men, by Ruth Rendell. Work this problem without consulting that book! Consider the following message: SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA This ciphertext was produced using the first sentence of The Other Side of Silence (a book about the spy Kim Philby): The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars. A simple substitution cipher was used. a. What is the encryption algorithm? b. How secure is it? c. To make the key distribution problem simple, both parties can agree to use the first or last sentence of a book as the key. To change the key, they simply need to agree on a new book. The use of the first sentence would be preferable to the use of the last. Why?	K6
4.	In one of his cases, Sherlock Holmes was confronted with the following message. 534 C2 13 127 36 31 4 17 21 41	K3

	DOUGLAS 109 293 5 37 BIRLSTONE 26 BIRLSTONE 9 127 171 Although Watson was puzzled, Holmes was able immediately to deduce the type of cipher. Can you?	
5.	A disadvantage of the general 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 If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns: 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 This yields the sequence C A K S Y I B L T Z P D M U H F N V E G O W R J Q X Determine the keyword.	K 5
6.	When the 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 The key used was royal New Zealand navy. Decrypt the message. Translate TT into tt.	K4
7.	a. Construct a Playfair matrix with the key largest. b. Construct a Playfair matrix with the key occurrence. Make a reasonable assumption about how to treat redundant letters in the key.	K4
8.	Consider a Feistel cipher composed of 16 rounds with block length 128 bits and key length 128 bits. Suppose that, for a given k, the key scheduling algorithm determines values for the first 8 round keys, k_1, k_2, ..., k_8, and then sets $k_9 = k_8$, $k_{10} = k_7$, $k_{11} = k_6$, ..., $k_{16} = k_1$ 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. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details of the device are not known to you and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)	K3
9.	Let □ be a permutation of the integers 0, 1, 2, ... (2^n - 1) such that □(*m*) gives the permuted value of *m*, 0 ≠ ≤ *m* 2^n. Put another way, □ maps the set of *n*-bit integers into itself and no two integers map into the same integer. DES is such a permutation for 64-bit integers. We say that □ has a fixed point at *m* if □(*m*) = *m*. That is, if □ is an encryption mapping, then a fixed point corresponds to a message that encrypts to itself. We are interested in the probability that □ has no fixed points. Show the somewhat unexpected result that over 60% of mappings will have at least one fixed point.	K2
10	Develop a program that can encrypt and decrypt using a general substitution block cipher.	K3

11	Compute the bits number 1, 16, 33, and 48 at the output of the first round of the DES Decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones.	K2
12	Show that DES decryption is, in fact, the inverse of DES encryption.	K3
13	Show that in 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.	K2
14	Compare AES to DES.	K2
15	For the group S_n of all permutations of n distinct symbols, What is the number of elements in S_n? Show that S_n is not abelian for n > 2.	K 2
16	A modulus of 0 does not fit the definition, but is defined by convention as follows: a mod 0 = a. With this definition in mind, what does the following expression mean: $a \equiv b \pmod 0$?	K2
17	Demonstrate that the set of polynomials whose coefficients form a field is a ring.	K3
18	Write a simple four-function calculator in GF(2^4). You may use table lookups for the multiplicative inverses.	K3
19	Write a simple four-function calculator in GF(2^8). You should compute the multiplicative inverses on the fly.	K3
20	Illustrate the difference between Rijndael and AES.	K3
21	In the discussion of MixColumns and Inverse MixColumns, it was stated that $b(x) = a^1(x)$ mod $(x^4 + 1)$ where $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ and $b(x) = \{03\}x^3 + \{0D\}x^2 + \{09\} x + \{0E\}$. Show that this is true.	K 3
22	Compute the output of the MixColumns transformation for the following sequence of input bytes "67 89 AB CD". Apply the InvMixColumns transformation to the obtained result to verify your calculations. Change the first byte of the input from '67' to '77', perform the MixColumns transformation again for the new input, and determine how many bits have changed in the output. Note: You can perform all calculations by hand or write a program supporting these computations. If you choose to write a program, it should be written entirely by you; no use of libraries or public domain source code is allowed in this assignment.	K3
23	Use the key 1010 0111 0011 1011 to encrypt the plaintext "ok" as expressed in ASCII, that is 0110 1111 0110 1011. The designers of S-AES got the ciphertext 0000 0111 0011 1000. Do you?	K3
24	Write a program that can encrypt and decrypt using S-AES. Test data: a binary plaintext of 0110 1111 0110 1011 encrypted with a binary key of 1010 0111 0011 1011 should give a binary ciphertext of 0000 0111 0011 1000 less ecb $$$). Decryption should work correspondingly.	K3
25	CBC-Pad is a block cipher mode of operation used in the RC5 block cipher, but it could be used in any block cipher. CBC-Pad handles plaintext of any length. The ciphertext is longer then the plaintext by at most the size of a single block. Padding is used to assure that the plaintext input is a multiple of the block length. It is assumed that the original plaintext is an integer number of bytes. This plaintext is padded at the end by from 1 to bb bytes, where bb equals the block size in bytes. The pad bytes are all the same and set to a byte that represents the number of bytes of padding. For example, if there are 8 bytes of padding, each byte has the bit pattern 00001000. Why not allow zero bytes of padding? That is, if the original plaintext is an integer multiple of the block size, why not refrain from padding?	K4
26	Create software that can 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.	K3
27	Electronic mail systems differ in the manner in which multiple recipients are handled. In some systems, the originating mail-handler makes all the necessary copies, and these are sent out independently. An alternative approach is to determine the route for each destination first. Then a single message is sent out on a common portion of the route, and copies are made only when the routes diverge; this process is referred to as mail bagging.	K4

	a. Leaving aside considerations of security, discuss the relative advantages and disadvantages of the two methods. Discuss the security requirements and implications of the two methods.	
28	The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How ca .n such an algorithm be used to test for primality?	K4
29	Write a computer program that implements the Miller-Rabin algorithm for a user- specified n. The program should allow the user two choices: (1) specify a possible witness a to test using the Witness procedure, or (2) specify a number s of random witnesses for the Miller-Rabin test to check.	K3
30	In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?	K2
31	In the 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?	K3
32	Assume that you generate an authenticated and encrypted message by first applying the RSA transformation determined by your private key, and then enciphering the message using recipient's public key (note that you do NOT use hash function before the first transformation). Will this scheme work correctly [i.e., give the possibility to reconstruct the original message at the recipient's side, for all possible relations between the sender's modulus ns and the recipient's modulus n_R ($n_S > n_R$, $n_S < n_R$, $n_S = n_R$)]? Explain your answer. In case your answer is "no," how would you correct this scheme?	K3
33.	Users A and B use the Diffie-Hellman key exchange technique with a common prime q= 71 and a primitive root x = 7. a. If user A has private key $X_A = 5$, what is A's public key Y_A? b. If user B has private key $X_B = 12$, what is B's public key Y_B? c. What is the shared secret key?	K4
34.	The following is a first attempt at an Elliptic Curve signature scheme. We have a global elliptic curve, prime p, and "generator" G. Alice picks a private signing key X_A and forms the public verifying key $Y_A = X_AG$. To sign a message M: Alice picks a value k. Alice sends Bob M, k and the signature $S = M\ kX_AG$. Bob verifies that $M = S + kY_A$ Show that this scheme works. That is, show that the verification process produces an equality if the signature is valid. Show that the scheme is unacceptable by describing a simple technique for forging a user's signature on an arbitrary message.	K4
35.	When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?	K3
36.	It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?	K3
37.	Now consider the opposite problem: using an encryption algorithm to construct a one- way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the result with the second block and encrypt again, etc. Show that this scheme is not secure by solving the following problem. Given a two-block message B1, B2, and its hash RSAH(B1, B2) = RSA(RSA (B1) $\oplus$ B2) Given an arbitrary block C1, choose C2 so that RSAH(C1, C2) = RSAH(B1, B2). Thus, the hash function does not satisfy weak collision resistance.	K3
38.	Whirlpool makes use of the construction $H_i = E(H_{i-1}, M_i) \oplus H_{i-1} \oplus M_{i-1}$ Another construction that was shown by Preneel to be secure is $Hi = E(Hi-1, M_i) \oplus M_i$. Now notice that the key	K3

	schedule for Whirlpool resembles encryption of the cipher key under a pseudo-key defined by the round constants, so that the core of the hashing process could be formally viewed as two interacting encryption $E(H_{i-1},M_i)$lines. Consider the encryption We could write the final round key for this block as $K10 = E (RC, H_{i-1})$. Now show that the two hash constructions are essentially equivalent because of the way that the key schedule is defined.	
39.	DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?	K3
40.	With DSS, 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. What is the practical implication of this difference?	K3
41	Suppose that, in PCBC mode, blocks C_i and C_{i+1} are interchanged during transmission. Show that this affects only the decrypted blocks P_i and P_{i+1} but not subsequent blocks.	K4
42	Consider radix-64 conversion as a form of encryption. In this case, there is no key. But suppose that an opponent knew only that some form of substitution algorithm was being used to encrypt English text and did not guess it was R64. How effective would this algorithm be against cryptanalysis?	K5
43	In discussing AH processing, it was mentioned that not all of the fields in an IP header are included in MAC calculation.	K4
	a. For each of the fields in the IPv4 header, indicate whether the field is immutable, mutable but predictable, or mutable (zeroed prior to ICV calculation). b. Do the same for the IPv6 header. c. Do the same for the IPv6 extension headers. In each case, justify your decision for each field.	K5
44.	Consider the following threats to Web security and describe how each is countered by a particular feature of SSL. a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm. b. Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full ciphertext to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys). C. Replay Attack: Earlier SSL handshake messages are replayed. d. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client. e. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped. f. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data. g. IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts. SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the "half-open connection" around for a few minutes. Repeated SYN messages can clog the TCP module.	K4
45.	One approach to defeating the tiny fragment attack is to enforce a minimum length of the transport header that must be contained in the first fragment of an IP packet. If the first fragment is rejected, all subsequent fragments can be rejected. However, the nature of IP is such that fragments may arrive out of order. Thus, an intermediate fragment may pass through the filter before the initial fragment is rejected. How can this situation be handled?	K4

17. STUDENT-CENTERED LEARNING (SELF-LEARNING TOWARDS LIFE-LONG LEARNING)

S.No.	Typical Project/Problem	KL
1	Students will review the Research Papers and will write a Survey Paper for IAs.	KL6