DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CRYPTOGRAPHY & NETWORKSECURITY

Question Bank

Vision of Institution

To build Jeppiaar Engineering College as an Institution of Academic Excellence in Technical education and Management education and to become a World Class University.

Mission of Institution

M1	To excel in teaching and **learning, research and innovation** by promoting the principles of scientific analysis and creative thinking
M2	To participate in the production, **development and dissemination of knowledge** and interact with **national and international communities**
M3	To equip students with **values, ethics and life skills** needed to enrich their lives and enable them to meaningfully contribute to the **progress of society**
M4	To prepare students **for higher studies and lifelong learning**, enrich them with the **practical and entrepreneurial skills** necessary to excel as future professionals and contribute to **Nation's economy**

Program Outcomes (POs)

PO1	**Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO2	**Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	**Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations
PO4	**Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5	**Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6	**The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7	**Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO8	**Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO9	**Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10	**Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO11	**Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	**Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Vision of Department

To emerge as a globally prominent department, developing ethical computer professionals, innovators and entrepreneurs with academic excellence through quality education and research.

Mission of Department

M1	To create **computer professionals** with an ability to identify and **formulate the engineering problems** and also to provide **innovative solutions** through **effective teaching learning process.**
M2	To **strengthen the core-competence** in computer science and engineering and to create an ability to **interact** effectively with industries.
M3	To produce engineers with good professional skills, **ethical values** and life skills for the **betterment of the society.**
M4	To encourage students towards **continuous and higher level learning** on technological advancements and provide a platform for **employment and self-employment.**

Program Educational Objectives (PEOs)

PEO1	**To address the real time complex engineering problems using innovative approach with strong core computing skills.**
PEO2	**To apply core-analytical knowledge and appropriate techniques and provide solutions to real time challenges of national and global society**
PEO3	**Apply ethical knowledge for professional excellence and leadership for the betterment of the society.**
PEO4	**Develop life-long learning skills needed for better employment and entrepreneurship**

Program Specific Outcomes (PSOs)

Students will be able to

PSO1	An ability to understand the core concepts of computer science and engineering and to enrich problem solving skills to analyze, design and implement software and hardware based systems of varying complexity.
PSO2	To interpret real-time problems with analytical skills and to arrive at cost effective and optimal solution using advanced tools and techniques.
PSO3	An understanding of social awareness and professional ethics with practical proficiency in the broad area of programming concepts by lifelong learning to inculcate employment and entrepreneurship skills.

BLOOM TAXANOMY LEVELS(BTL)

BTL6: Creating.,
BTL 5: Evaluating.,
BTL 4: Analyzing.,
BTL 3: Applying.,
BTL 2: Understanding.,
BTL 1: Remembering

SYLLABUS

CRYPTOGRAPHY AND NETWORK SECURITY- CS6701 (VII SEMESTER)

UNIT I   INTRODUCTION & NUMBER THEORY

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid‟s algorithm-Finite fields- Polynomial Arithmetic –Prime numbers-Fermat‟s and Euler‟s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms.

UNIT II   BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography.

UNIT III   HASH FUNCTIONS AND DIGITAL SIGNATURES

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 - SHA - HMAC – CMAC - Digital signature and authentication protocols – DSS – EI Gamal – Schnorr**.**

UNIT IV   SECURITY PRACTICE & SYSTEM SECURITY

Authentication applications – Kerberos – X.509 Authentication services - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security.

UNIT V   E-MAIL, IP & WEB SECURITY

E-mail Security: Security Services for E-mail-attacks possible through E-mail - establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME. **IPSecurity:** Overview of IPSec - IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). **Web Security:** SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).

Total= 45 Periods

TEXT BOOKS:

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013. (UNIT I,II,III,IV).
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security*"*, Prentice Hall of India, 2002. (UNIT V).

REFERENCES:

1. Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill, 2007.
2. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.
3. Charles Pfleeger, "Security in Computing", 4th Edition, Prentice Hall of India, 2006.
4. Ulysess Black, "Internet Security Protocols", Pearson Education Asia, 2000.
5. Charlie Kaufman and Radia Perlman, Mike Speciner, "Network Security, Second Edition, Private Communication in Public World", PHI 2002.
6. Bruce Schneier and Neils Ferguson, "Practical Cryptography", First Edition, Wiley Dreamtech India Pvt Ltd, 2003

Course Outcomes (COs)

C401.1	**Compare** various cryptographic techniques
C401.2	**Examine** Block Ciphers methods and Public Key Cryptography
C401.3	**Analyze** hash functions and Digital Signatures
C401.4	**Classify** security protocols and methods to solve security problems.
C401.5	**Describe E-mail** Security services, web security services and IP Security services.

INDEX

Unit #	Ref. Book
Unit 1	William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
Unit 2	William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
	William Stallings, Cryptography and Network Security, 6th Edition,

Unit 3	Pearson Education, March 2013.
Unit 4	William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
Unit 5	Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002.

UNIT I   INTRODUCTION & NUMBER THEORY

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid"s algorithm-Finite fields- Polynomial Arithmetic –Prime numbers-Fermat"s and Euler"s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms.

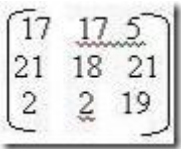| S. No.	Question	Course Outcome	Blooms Taxanomy Level
1	**Differentiate passive attack from active attack with example. (APR2011, NOV2011,DEC2016, DEC 2017)** <table><tr><th>Passive Attack</th><th>Active Attack</th></tr><tr><td>1. Passive attacks do not affect system resources • Eavesdropping, monitoring 2. Two types of passive attacks • Releasof message • Traffic analysis 3. Passive attacks are very difficult to detect</td><td>1. Active attacks try to alter system resources or affect their operation • Modification of data, or creationof false data 2. Four categories • Masquerade • Replay • Modification of messages • Denial of service: preventing normal use 3. Difficult to prevent</td></tr></table>	C401.1	BTL 1
2	**What are the 3 aspects of security?** • Security Attack • Security Mechanism • Security Service	C401.1	BTL 1
3	**Define Security attacks.** Security attack: Any action that compromises the security of information owned by an organization.	C401.1	BTL 1
4	**Define security mechanism.** Security mechanism: A process that is designed to detect, prevent, or recover from a security attack	C401.1	BTL 1

5	**Define Security service**. A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.	C401.1	BTL 1
6	**Define cryptanalysis?** The study of principles and methods of transforming an unintelligible message back into an intelligible message without the knowledge of the key. It is also called code breaking.	C401.1	BTL 1
7	**Define Steganography** It is the process of hiding the message into some cover media. It hides the existence of a message. Ex: Character marking, Pin punctures, Invisible ink etc	C401.1	BTL 1
8	**What are the two basic functions used in encryption algorithms?** The two basic functions used in encryption algorithms are • Substitution • Transposition	C401.1	BTL 1
9	**Define Threat and attack. (NOV2009)** Threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm. Attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset	C401.1	BTL 1
10	**What are the two approaches to attacking a cipher?** The two approaches to attack a cipher are: 1.Cryptanalysis 2.Brute-force attack	C401.1	BTL 1
11	**Define Brute-force attack.** The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.	C401.1	BTL 1
12	**What is Modification of messages** Modification of messages simply means that some portion of a	C401.1	BTL 1

	legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.		
13	**What is masquerade?** A **masquerade** takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges	C401.1	BTL 1
14	**What is Reply?** **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.	C401.1	BTL 1
15	**Define Denial of service.** Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance	C401.1	BTL 1
16	**List out the components of encryption algorithm.** 1. Plaintext 2. Encryption algorithm 3. Secret key 4. Cipher text 5.Decryption algorithm	C401.1	BTL 1
17	**Compare Substitution and Transposition techniques.** **Substitution techniques:** A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols. Ex: Caeser cipher. **Transposition techniques:** It process in which different kind of mapping is achieved by performing some sort of permutation on the plaintext letterset. Ex: DES, AES.	C401.1	BTL 1
18	**Specify the four categories of security threads?** • Interruption • Interception • Modification	C401.1	BTL 1

	• Fabrication		
19	**Define integrity.** It assures that the data received is sent by an authorized entity and are not modified/replayed/deleted/updated	C401.1	BTL 1
20	**Define Non repudiation.** It is the process which protects against denial by one of the parties in a communication. It can be obtained through the use of digital signature, time stamps etc,.	C401.1	BTL 1
21	**Differentiate symmetric and asymmetric encryption?** **Symmetric:** It is a form of cryptosystem in which encryption and decryption performed using the same key. **Asymmetric:** It is a form of cryptosystem in which encryption and decryption performed using two keys. Eg: DES, AES Eg: RSA, ECC	C401.1	BTL 1
22	**Compare stream cipher with block cipher with example.** **Stream cipher:** Processes the input stream continuously and producing one element at a time. Example: Caeser cipher. **Block cipher:** Processes the input one block of elements at a time producing an output block for each input block. Example: DES.	C401.1	BTL 1
23	**Convert the Given Text "CRYPTOGRAPHY" into cipher text using Rail fence Technique.** In rail fence technique the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. C Y T G A H R P O R P Y The cipher text is CYTGAH RPORPY.	C401.1	BTL 1
24	**State the Fermat's Theorem. (APR2011, APR/MAY 2017, NOV/DEC 2017)** Fermat theorem states the following. If p is prime and a is a positive integer not divisible by p, then **$A^{p-1} \equiv 1 \bmod p$**	C401.1	BTL 4
25	**State the Euler's Theorem.** Euler's theorem states that for every a and n that are relatively	C401.1	BTL 4

	prime $a^{\phi(n)} \equiv 1(\text{mod } n)$		
26	**Define Primality Test. (NOV2011)** A primality testing is a test to determine whether or not a given number is prime, as opposed to actually decomposing the number into its constituent prime factors (which is known as prime factorization).	C401.1	BTL 1
27	**Define Euler's theorem and it's application.** (**APR/MAY 2018**) Euler's theorem states that for every a and n that are relatively prime: **a ф (n)≡≡ 1 mod n**	C401.1	BTL 1
28	**Find gcd (1970, 1066) using Euclid's algorithm? (DEC2016)** gcd (1970,1066) = gcd(1066,1970 mod 1066) = gcd(1066,904)= 2	C401.1	BTL 5
29	**Find gcd (24140, 16762) using Euclid's algorithm? (APR/ MAY 2017)** gcd (24140,16762) = gcd(16762, 24140 mod 16762) = gcd(16762 , 7378)= 34	C401.1	BTL 5
30	**Why is asymmetric cryptography bad for huge data? Specify the reason**? (**APR/MAY 2018**) Asymmetric encryption takes more time. Key Management is difficult. Slower encryption speed due to long keys.	C401.1	BTL 1

PART B

1	**Explain about OSI Security architecture model with neat diagram.(DEC2016)** Williams Stalling P.No: 12-13	C401.1	BTL 1
2	**Classical cryptosystems and its types. (NOV2011, APR2012, NOV2012, NOV 2010, MAY2009, NOV2008, NOV2007)** , (**APR/MAY 2018**)Williams Stalling P.No: 28	C401.1	BTL 1

3	Convert "MEET ME" using Hill cipher with the key matrix Convert the cipher text back to plaintext - NOTES $$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$	C401.1	BTL 5
4	Encrypt the following using play fair cipher using the keyword MONARCHY . " SWARAJ IS MY BIRTH RIGHT". Use X as blank space. (NOV/DEC 2017) - NOTES	C401.1	BTL 5
5	Discuss Fermat's Theorem. (NOV2012, DEC2016, APR 2017) Williams Stalling P.No: 238-239 Discuss Euler's Theorem (APR2011, NOV2012) P.No: 241-242 Discuss Chinese Remainder Theorem. (APR2011, APR2012, DEC2016, (APR/MAY 2018) P.No: 245-247	C401.1	BTL 4, BTL 5
6	Describe : (APR/ MAY 2017) Playfair cipher Williams Stalling P.No: 40-42 Railfence cipher Williams Stalling P.No: 43-45 Vignere cipher Williams Stalling P.No: 45-48	C401.1	BTL 1
7	Discuss the properties that are satisfied by Groups, Rings and Fields. (NOV/DEC 2017) - Notes	C401.1	BTL 1

8`	State Chinese remainder theorem and find X for the given set of congruent equations using CRT (DEC 2016, APR/MAY 2017)
	Williams Stalling P.No: 245
	X = 1(mod 5) (b) X = 2(mod 3)
	   X = 2(mod 7) X = 3(mod 5)
	   X = 3(mod 9) X = 2(mod 7)
	   X = 4(mod 11)
		C401.1	BTL 4

9	Describe the various security mechanisms (DEC 2016) Williams Stalling P.No: 19	C401.1	BTL 1

UNIT II BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: **Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography**

S. No.	Question	Course Outcome	Blooms Taxanomy Level
1	**What are the different modes of operation in DES? (APR 2011 , APR 2017)** Electronic Code Book (ECB) Cipher Block Chaining (CBC) Cipher Feedback (CFB) Output Feedback (OFB) Counter Mode	C401.2	BTL 1
2	**Write down the purpose of S-Boxes in DES? (NOV 2011)** Each row of a S-box defines a general reversible substitution. It consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.	C401.2	BTL 1
3	**What is the difference between diffusion and confusion?(NOV 2011)** In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation. In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution	C401.2	BTL 1
4	**What is the difference between differential and linear cryptanalysis?(APR 2012)** Differential cryptanalysis is the first published attack that	C401.2	BTL 1

	is capable of breaking DES in less than encryptions.

Linear Cryptanalysis method can find a DES key given known 2^{43} plaintexts, as compared to 2^{47} chosen plaintexts for differential cryptanalysis | | |
| 5 | **What are disadvantages of double DES? (NOV 2012)**

Reduction to a single stage.

Meet in the middle attacks. | C401.2 | BTL 1 |
| 6 | **What is an avalanche effect? (NOV 2012)**

It is that a small change in either the plaintext or the key should produce a significant change in the cipher text.A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text | C401.2 | BTL 1 |
| 7 | **Define product cipher.**

Product cipher performs two or more basic ciphers in sequence in such a way that the final result or product is crypto logically stronger than any of the component ciphers. | C401.2 | BTL 1 |
| 8 | **What is a meet-in-the-middle attack?**

Meet-in-the-middle attack was first described in [DIFF77]. It is based on the observation that, if we have

$C=E_{k2}[E_{k1}[P]]$

Then

$X=E_{k1}[P]=D_{k2}[C]$

Given a known pair, (P,C), the attack proceeds as follows. First, encrypt P for all 256 possible values of K1. Store these results in a table and then sort the table by the values of X. Next, decrypt C using all 256 possible values of K2. As each decryption is produced, check the result against the table for a match. If a match occurs, then test the two resulting keys against a new known plaintext-cipher textpair. If the two keys produce the correct cipher text, accept them as the correct keys. | C401.2 | BTL 1 |

9	**Brief the strength of triple DES. (DEC 2016)** It is a reuse DES implementation by cascading three instances of DES. It is believed to be secure up to at least security	C401.2	BTL 1
10	**Define Cipher Feedback (CFB).** In Cipher Feedback (CFB) Input is processed s-bits at a time. Preceding cipher text is used as input to the encryption algorithm to produce pseudorandom output, which is XOR ed with plaintext to produce next unit of cipher text.	C401.2	BTL 1
11	**Define Cipher Block Chaining (CBC) mode.** In Cipher Block Chaining (CBC) mode the input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of cipher text	C401.2	BTL 1
12	**Define Counter (CTR).** In Counter (CTR) mode each block of plaintext is XOR ed with an encrypted counter. The counter is incremented for each subsequent block	C401.2	BTL 1
13	**Define electronic codebook (ECB).** The simplest mode is the electronic codebook (ECB) mode, in which plaintext is handled one block at a time and each block of plaintext is encrypted using the same key. The term *codebook* is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext.	C401.2	BTL 1
14	**Perform encryption and decryption using RSA Alg. for the following..** **P=17; q=11; e=7; M=88. (NOV/DEC 2017)** Soln: n=pq n=17*11=187 ö(n)=(p-1) (q-1) =16*10 = 160 e=7	C401.2	BTL 5

	$C = M^e \bmod n$ $M = C^d \bmod n$		
15	**Perform encryption and decryption using RSA Alg. for the following..** **P=7; q=11; e=17; M=8. (APRIL/ MAY 2018)** Soln: n=pq n=7*11=77 ö(n)=(p-1) (q-1) =6*10 = 60 e=17 d =27 $C = M^e \bmod n$ $C = 8^{17} \bmod 77 = 57$ $M = C^d \bmod n = 57^{27} \bmod 77 = 8$	C401.2	BTL 5
17	**What is an elliptic curve? (DEC 2016)** It is a plane algebraic curve defined by an equation of the form *y2 = x3 +ax +b* that is non-singular also graph has no cusps or self intersections.	C401.2	BTL 1
18	**What is the difference between Rijndael and AES?** AES was developed by NIST .AES is a symmetric block cipher that is intended to replace DES.NIST selected rijndael as the proposed AES algorithm. The two researchers who developed and submitted Rijndael for the AES are the both cryptographers from Belgium.	C401.2	BTL 1
19	**What is the difference between the AES decryption algorithm and the equivalent inverse cipher?** In AES decryption, we use inverse shift rows inverse sub bytes, add round key, inverse mix columns. But in equivalent inverse cipher, we interchange inverse shift rows and inverse sub bytes.	C401.2	BTL 1
20	**What are the operations used in AES?**	C401.2	BTL 1

	• Substitute bytes • ShiftRows • MixColumns • AddRoundKey		
21	**What is a Substitute byte transformation in AES?** The forward substitute byte transformation, called SubBytes, is a simple table lookup. AES defines a 16x16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values. Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value	C401.2	BTL 1
22	**Difference between private key and public key algorithm (APR 2017)** Public key encryption encrypts data using the recipient's public key and it cannot be decrypted without using a matching private key. i.e., you need one key to lock (encrypt the piantext) and another key to unlock (decrypt the cypertext). Private key cannot be used in the place of the public key. If the locking key is made private, this system makes it possible to verify that the documents were locked by the owner. The reason is that a message encrypted by the sender can only be opened by a person with the matching public key, thus verifying that the sender did actually hold the private key (meaning that the original and non-tampered message has been received). Therefore, this is used for digital signatures.	C401.2	BTL 1
23	**What is a Shift rows?** In shift row, a row shift moves an individual byte from one column to another, which is a linear distance of a multiple of 4 bytes. In Forward Shift Row, each row perform circular left shift. Second Row a 1-byte circular left shift is performed. Third Row a 2-byte circular left shift is performed. For the	C401.2	BTL 1

	Fourth Row a 3-byte circular left shift is performed. In Inverse Shift Row, each row perform circular right shift.		
24	**How the key is expanded in AES** AES (Rijndael) uses a key schedule to expand a short key into a number of separate round keys. This is known as the Rijndael key schedule. The three AES variants have a different number of rounds. Each variant requires a separate 128-bit round key for each round plus one more.	C401.2	BTL 1
25	**What primitive operations are used in RC5** • Key expansion • Encryption • Decryption	C401.2	BTL 1
27	**User A & B exchange the key using Diffie Hellman alg. Assume á=5 q=11 XA=2 XB=3. Find YA, YB, K.** Soln: $Y_A = á^{XA}$ mod q $= 5^2$ mod 11 = 3 $Y_B = á^{XB}$ mod q = 5^3 mod 11 = 4 $K_A = Y_B^{XA}$ mod q = 4^2 mod 11 = 5 $K_B = Y_A^{XB}$ mod q= 33 mod 11= 5	C401.2	BTL 4
28	**Whether the Diffie Hellman key exchange protocol is vulnerable?** Yes, the key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates	C401.2	BTL 1
29	**Write about elliptic curve cryptography.** Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic	C401.2	BTL 1

	curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization		
30	**List the parameters for the three AES version?** (**APR/MAY 2018**) Block size – 128 bits Key size – 128 , 192, 256 bits No. of rounds – 10 , 12 or 14	C401.2	BTL 1

PART B

1	**Explain in detail about DES and Triple DES. (APR2012, NOV2009, NOV2008 , APR 2017) Williams Stalling P.No: 73**	C401.2	BTL 1
2	**Explain about AES in detail. (NOV2009, MAY2009, NOV2008,NOV2007,DEC2016, , NOV 2017, APRIL 2018) Williams Stalling P.No: 134**	C401.2	BTL 1
3	**Explain about RC4 Algorithm. (APR 2012) Williams Stalling P.No: 191-194**	C401.2	BTL 1
4	**Explain the RSA algorithm and explain the RSA with p=7,q=11,e=17,M=8. Discuss its merit. (APR2011, NOV2011, NOV2012, NOV2010, DEC2016) Williams Stalling P.No: 268-280**	C401.2	BTL 1
5	**Discuss the discrete logarithm and explain Diffie-Hellman Key Exchange algorithm with its merits and demerits. (APR2011, NOV2012, NOV2010, DEC2016, APR 2017) Williams Stalling P.No: 298-301**	C401.2	BTL 4
6	**Explain in detail about elliptic curve cryptography(APRIL 2018). Williams Stalling P.No: 310-313**	C401.2	BTL 1
7	**User Alice & Bob exchange the key using Diffie Hellman alg. Assume α=5 q=83 X$_A$=6 X$_B$=10. Find Y$_A$, Y$_B$, K. (NOV /DEC 2017). - Notes**	C401.2	BTL 5

UNIT III HASH FUNCTIONS AND DIGITAL SIGNATURES

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 - SHA - HMAC – CMAC - Digital signature and authentication protocols – DSS – EI Gamal – Schnorr.

S. No.	Question	Course Outcome	Blooms Taxanomy Le
1	**1. What is the difference between public key and private key cryptosystem?(APR2012, NOV2011)** <table><tr><td>**Conventional(privatekey) Encryption**</td><td>**Public key Encryption**</td></tr><tr><td>1. Same algorithm with same key used for encryption and decryption.</td><td>1. Same algorithm is used used for encryption & decryption with a pair of keys.</td></tr><tr><td>2. Sender & receiver must share the algorithm and key</td><td>2. Sender & re ceiver have one of. the matched pair keys</td></tr><tr><td>3. Key must be kept secret.</td><td>3. Any one of the key must bekept secret.</td></tr></table>	C401.3	BTL 1
2	**What is meant by Message Authentication?** Message Authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.	C401.3	BTL 1
3	**List out the attacks during the communication across the network.** • Disclosure • Traffic analysis • Masquerade • Content modification • Sequence modification • Timing modification • Source repudiation • Destination repudiation	C401.3	BTL 1

4	**Define Disclosure.** Release of message contents to any person or process not possessing the appropriate cryptographic key.	C401.3	BTL 1
5	**Define Traffic analysis** Traffic analysis is the Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined	C401.3	BTL 1
6	**Define Masquerade**. Masquerade is the insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient	C401.3	BTL 1
7	**Define Timing modification.** Timing modification is the Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.	C401.3	BTL 1
8	**Define Source repudiation and Destination repudiation** Source repudiation is the Denial of transmission of message by source. Destination repudiation is the Denial of receipt of message by destination..	C401.3	BTL 1
9	**Define the classes of message authentication function.** • Hash function • Message encryption • Message authentication code (MAC	C401.3	BTL 1
10	**Define Hash function (<u>APRIL/ MAY 2018)</u>** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator	C401.3	BTL 1
11	**Differentiate Message Authentication Code and Hash function. (<u>DEC 2016)</u>** In MAC, a public function of the message and a secret key are used to produce a fixed length authenticator. A hash function accepts a variable size	C401.3	BTL 1

	message as input and produces a fixed size output (hash code) which is similar to MAC. But hash code does not use a key.		
12	**What you meant by MAC?** MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC. **T=MAC(K,M)** where M is a variable-length message, K is a secret key shared only by sender and receiver, and MAC(K,M) is the fixed-length authenticator.	C401.3	BTL 1
13	**List out the attack on MAC.** • Brute-force attacks • Cryptanalysis.	C401.3	BTL 1
14	**What do you mean by one way property in hash function? (APR2011, NOV2012)** An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.	C401.3	BTL 1
15	**Define Replay Attack. (NOV2011)** Replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IPpacket substitution	C401.3	BTL 1
16	**Define Digital signature.** A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message	C401.3	BTL 1
17	**What are the properties of Digital Signature?** The digital signature must have the following properties: It must verify the author and the date and time of the signature. It must authenticate the contents at the time of the signature. It must be verifiable by third parties, to resolve disputes	C401.3	BTL 1

18	**List out the attacks related to Digital Signature.** Key-only attack: - Known message attack - Generic chosen message attack - Directed chosen message attack - Adaptive chosen message attack	C401.3	BTL 1
19	**Mention the signature function in DSS ? (NOV/DEC2017)** The hash **function** used in the **DSS** standard is specified in the Secure Hash Standard (SHS), which are the specifications for the Secure Hash Algorithm (SHA).	C401.3	BTL 1
20	**Define Generic chosen message attack** If A is the sender and C is the attacker. Then C chooses a list of messages before attempting to breaks A's signature scheme, independent of A's public key. C then obtains from A valid signatures for the chosen messages. The attack is generic, because it does not depend on A's public key; the same attack is used against everyone.	C401.3	BTL 1
21	**Define Universal forgery** If A is the sender and C is the attacker. Then C finds an efficient signing algorithm that provides an equivalent way of constructing signatures on arbitrary messages.	C401.3	BTL 1
22	**Define Existential forgery** If A is the sender and C is the attacker. Then C forges a signature for at least one message. C has no control over the message. Consequently, this forgery may only be a minor nuisance to A.	C401.3	BTL 1
23	**What are the two approaches of Digital Signature? (NOV2012)** - RSA Approach - DSS Approach	C401.3	BTL 1

(a) RSA approach

(b) DSS approach

24	**Specify the various types of authentication protocols? (APR 2017)** • One –way authentication • Mutual authentication	C401.3	BTL 1
25	**How is the security of MAC expressed? (NOV /DEC 2017)** MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is public-key cryptography. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation	C401.3	BTL 1
26	**How Digital signature differs from authentication protocols? (APR/ MAY 2018)** A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit. An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax	C401.3	BTL 1
27	**List out some hash algorithm.** • MD5 (Message Digest version 5) algorithm. • SHA_1 (Secure Hash Algorithm). • RIPEMD_160 algorithm	C401.3	BTL 1

28	**What is the role of compression function in hash function? (APR 2017)** The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value usually b>n; hence the term compression	C401.3	BTL 1
29	**What is MAC based on DES** One of the most widely used MACs, referred to as Data Authentication Algorithm (DAA) is based on DES. The algorithm can be defined as using cipher block chaining (CBC) mode of operation of DES with an initialization vector of zero. The data to be authenticated are grouped into contiguous 64-bit blocks: D1, D2 …Dn. if necessary, the final block is padded on the right with zeros to form a full 64-bit block. Using the DES encryption algorithm and a secret key, a data authentication code	C401.3	BTL 1
30	**State three requirements for authentication? (APR 2017)** Disclosure release of message content. Traffic analysis discovery of pattern of traffic between parties. Content modification changes to the contents of a message.	C401.3	BTL 1

PART B

1	**Explain about MD5 in detail. (APR2011, APR2012, DEC 2016, APRIL 2018) Williams Stalling P.No: 210**	C401.3	BTL 1
2	**Illustrate about the SHA algorithm and explain. (NOV 2017 ,NOV2011, NOV2010, NOV2009, MAY2009, MAY2007) Williams Stalling P.No: 353-358**	C401.3	BTL 1
3	**Write a detailed note on Digital signatures. (NOV2011, NOV2010, DEC 2016, APR 2017) Williams Stalling P.No: 377-397**	C401.3	BTL 1
4	**Write notes on Birthday Attack. (APR 2012) Williams Stalling P.No: 338-339**	C401.3	BTL 1
5	**Compare the performance of RIPEMD-160 algorithm and SHA-1 algorithm? (APR 2017) Williams Stalling P.No: 352-358**	C401.3	BTL 1
6	**Describe about Hash Function. How its algorithm is designed? Explain its features & properties? (NOV 2012, NOV2008, APRIL 2018) Williams Stalling P.No: 328-331**	C401.3	BTL 1
7	**Write down the steps involved in Elgamal DSS & Schnorr DSS ? (NOV/DEC 2017) – NOTEs**	C401.3	BTL 1

UNIT IV   SECURITY PRACTICE & SYSTEM SECURITY

Authentication applications – Kerberos – X.509 Authentication services - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security.

S. No.	Question	Course Outcome	Blooms Taxanomy Level
1	**List out the Requirements of Kerberos. (APR2011)** • Secure • Reliable • Transparent • Scalable	C401.4	BTL 1
2	**What is dual signature? What it is purpose?** The purpose of the dual signature is to link two messages that intended for two different recipients to avoid misplacement of orders	C401.4	BTL 1
3	**Define Kerberos.** Kerberos is an authentication service developed as part of project Athena atMIT.The problem that Kerberos address is, assume an open distributed environment in which users at work stations wish to access services on servers distributed throughout the network	C401.4	BTL 1
4	**In the content of Kerberos, what is realm?** A full service Kerberos environment consisting of a Kerberos server, a no. Ofclients, no.of application server requires the following: The Kerberos server must have user ID and hashed password of all participating users in its database. The Kerberos server must share a secret key with each server. Such anenvironment is referred to as "Realm".	C401.4	BTL 1

5	**Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved? Write the authentication dialogue? (NOV /DEC 2017)** a) C ->AS: [IDC|| PC || IDV] b) AS ->C: Ticket c) C ->V: [IDC || ADC || IDV] Ticket = EKV [IDC ||ADC || IDV]	C401.4	BTL 4
6	**Define Intruder. Name three different classes of intruder. (APR2011 , DEC 2016)** Intruder is a person who can access the network or system without proper permission or rights. • Classes of Intruders • Masquerader • Misfeasor • Clandestine user	C401.4	BTL 1
7	**What do you mean by Trojan horse? (APR 2011)** A **Trojan Horse** is a malicious security-breaking program that appears to be a benign and legitimate program, but it is designed to have destructive effects on a computer and may open a backdoor. Unlike a virus, a Trojan Horse does not replicate itself. One example is a free game that someone could download, but it actually is a Trojan Horse that holds viruses and worms that invade your computer.	C401.4	BTL 1
8	**Define: Malicious software. (NOV 2011)** Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs	C401.4	BTL 1

9	**Write down the system security standards? (APR2012, NOV2011)** • National Institute of Standards and Technology(NIST) • The International Organization for Standardization (ISO) • The International Telecommunication Union (ITU) • Internet Society (ISOC)	C401.4	BTL 1
10	**What are two common techniques used to protect a password file?** **One-way function**: The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. **Access control**: Access to the password file is limited to one or a very few accounts	C401.4	BTL 1
11	**Define Intrusion. (APR2012,NOV2012)** The process of accessing a network or system without proper permission or rights.	C401.4	BTL 1
12	**Give few examples for worms. (NOV2012)** A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function. An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.	C401.4	BTL 1
13	**Define virus. Specify the types of viruses?** A virus is a program that can infect other program by modifying them the modification includes a copy of the virus program, which can then go on to infect other program, **Types:** 1) Parasitic virus 2) Memory-resident virus 3) Boot sector virus 4) Stealth virus 5) Polymorphic virus	C401.4	BTL 1

14	**List any two applications of X.509 Certificate? (NOV/DEC 2017)** Various code-signing schemes, such as signed Java ARchives, and Microsoft Authenticode. Various secure E-Mail standards, such as PEM and S/MIME. E-Commerce protocols, such as SET.	C401.4	BTL 1
15	**List the design goals of firewalls?** 1. All traffic from inside to outside, and vice versa, must pass through the firewall. 2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. 3. The firewall itself is immune to penetration.	C401.4	BTL 1
16	**What are the different phases a virus go through his lifetime?** 1. Dormant phase 2. Propagation phase 3. Triggering Phase 4. Execution phase	C401.4	BTL 1
17	**Define the roles / functions of firewall? (APR 2017, APRIL 2018)** A **firewall** acts as a barrier between a trusted network and and an untrusted network. A **firewall** controls access to the resources of a network through a positive control model.	C401.4	BTL 1
18	**State the difference between threats and attack? (APR 2017)** **Threat**: object, person, or other entity representing a constant danger to an asset. This can take any form and can be malevolent, accidental, or simply an act of nature. **Attack:** a deliberate act that exploits vulnerability. It can be either active or passive attack.	C401.4	BTL 1
19	**Define password selection strategy?** • The technique used to give password is:	C401.4	BTL 1

	• User education		
	• Computer generated password		
	• Reactive password checking		
	• Proactive password checking		
20	**What are the types of firewalls?** The three types of firewalls are • Packet Filtering Router • Application Level gateway • Circuit level gateway	C401.4	BTL 1
21	**Define trusted system?** One way to increase the security of a system against intruders and malicious program is toimplement trusted system	C401.4	BTL 1
22	**What is a threat? List its types? (APRIL/MAY 2018)** **Threat**: object, person, or other entity representing a constant danger to an asset. This can take any form and can be malevolent, accidental, or simply an act of nature. Worms, virus, Trojan, spyware, riskware, phishing, spam.	C401.4	BTL 1
23	**What is circuit level gateway?** Circuit level gateway does not permit an end to end TCP connection rather the gatewaysets up two TCP connections one between itself and a TCP user on an inner side and one between itself and a TCP user on an outside.	C401.4	BTL 1
24	**What is Bastion host?** A Bastion host is a system identified by the firewall administrator as a critical strongpoint in the network security.	C401.4	BTL 1
25	**What properties are required of a reference monitor?** The reference monitor enforces the following properties: • Complete mediation	C401.4	BTL 1

	• Isolation • Verifiability		
26	**What are the two rules that a reference monitor enforces?** The two rules are: • No read up • No write down.	C401.4	BTL 1
27	**What is an access right?** An access right describes the way in which a subject may access an object. Eg. read, write, execute, delete.	C401.4	BTL 1
28	**In the context of access control, what is the difference between a subject and an object?** A subject is an entity capable of accessing objects (eg. user, application, process). An object is resource to which access is controlled. An object is an entity used to contain information (eg. records, files, directories, processors, communication ports	C401.4	BTL 1
29	**What is honey pot?** Honey pots are decoy system that is designed to lure a potential attacker away from critical systems. Honey pots are designed to Divert an attacker from accessing critical systems Collect information about the attacker's activity Encourage the attacker to stay on the system long enough for administrators to respond.	C401.4	BTL 1
30	**Define ZOMBIE? (APR 2017)** This program secretly over another internet takes attached computer and the uses that computer launch attacks that are difficult to trace zombie's creator	C401.4	BTL 1

	PART B		
1	Explain kerberos authentication mechanism with suitable diagram?(DEC2016, APRIL 2018) Williams Stalling P.No: 403-417	C401.4	BTL 1
2	Explain in detail about firewalls. (APR2011, NOV2011, APR 2012, NOV2012, NOV2010, DEC2016, NOV 2017). Williams Stalling P.No: 621-646	C401.4	BTL 1
3	How does screened host architecture for firewalls differ from screened subnet firewall architecture? Which offers more security for information assets on trusted network? Explain with neat sketch? (APRIL 2018) Williams Stalling P.No: 621-646	C401.4	BTL 4
4	Explain about viruses in detail. (APR2011, NOV2012, APR 2017) Williams Stalling P.No: 602-607	C401.4	BTL 1
5	Explain the types of Intrusion Detection Systems. (NOV2011, NOV2010, APR 2017) Williams Stalling P.No: 570-581	C401.4	BTL 1
6	Explain about Malicious Software. (APR2012) Williams Stalling P.No: 598-620	C401.4	BTL 1
7	Explain in detail about SET for E-Commerce Transaction. (NOV/ DEC 2017) Williams Stalling P.No: 549-560	C401.4	BTL 1

UNIT V   E-MAIL, IP & WEB SECURITY

E-mail Security: Security Services for E-mail-attacks possible through E-mail - establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME. IPSecurity: Overview of IPSec - IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3-Exportability-Encoding-Secure Electronic Transaction (SET).

S. No.	Question	Course Outcome	Blooms Taxanomy Level
1	**Mention four SSL protocols. (APR 2011)** • SSL Record Protocol • Handshake Protocol. • Change Cipher Spec Protocol. • Alert Protocol.	C401.5	BTL 1
2	**Define TLS. (APR 2012)** TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. TLS is defined as a Proposed Internet Standard in RFC 5246. RFC 5246 is very similar to SSLv3	C401.5	BTL 1
3	**What do you mean by S/MIME? (APR 2012)** S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public keyencryption and signing of MIME data. S/MIME is on an IETFstandards track and defined in a number of documents, most importantly RFCs (3369,3370,3850,3851). S/MIME was originally developed by RSA Data Security Inc.S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption)	C401.5	BTL 1
4	**What is the purpose of S/MIME?** Abbreviated as : Secure/Multipurpose Internet Mail ExtensionSpecified as a standard way of encoding arbitrary data in email such as pictures, rich text,video clips ,binary files etc., along with adding signed and encrypted data	C401.5	BTL 1

| 5 | **What are the types of MIME? (<u>NOV 2012</u>)**

• **Text** **Plain** **Enriched** • **Multipart** **Mixed** **Parallel** **Alternative** **Digest** • **Message** **rfc822** **Partial** **External-body** • **Image** **jpeg** **gif** • **Video** **mpeg** • **Audio** **Basic** • **Application** **PostScript** **octet-stream** | C401.5 | BTL 1 |
| 6 | **What protocol compromise SSL? (<u>NOV 2012</u>)**

Secure Sockets Layer (SSL) protocol, originally developed by Netscape Communications, provides application-independent security and privacy over the Internet. SSL protocol is designed as a "stack" comprised of two separate protocols: the Record protocol and the Handshake protocol. These two protocols work together to ensure the secure encryption, transmission and reception of sensitive data between an authenticated website (server) and user | C401.5 | BTL 1 |

	(client), preventing unwanted interception by untrustworthy companies or persons.		
7	**Write about PGP?** • Secure Mail Protocol • Abbreviated as Pretty Good Privacy • Proposed by Phil Zimmermann • PGP performs encryption and integrity protection on files • PGP uses public key cryptography for personal use • Certificates are optional in PGP	C401.5	BTL 1
8	**What are the services provided by PGP ? (APRIL /MAY 2018)** • Digital signature • Message encryption • Compression • E-mail compatibility • Segmentation	C401.5	BTL 1
9	**Explain the reasons for using PGP?** a) It is available free worldwide in versions that run on a variety of platforms, including DOS/windows, UNIX, Macintosh and many more. b) It is based on algorithms that have survived extensive public review and are considered extremely secure. E.g.) RSA, DSS and Diffie-Hellman for public key encryption, CAST-128, IDEA, 3DES for conventional encryption, SHA-1for hash coding. c) It has a wide range of applicability from corporations that wish to select and enforce a standardized scheme for encrypting files and communication. d) It was not developed by nor is it controlled by any governmental or standards organization.	C401.5	BTL 1
10	**Why E-mail compatibility function in PGP needed?** Electronic mail systems only permit the use of blocks consisting of ASCII text.To accommodate this restriction PGP provides the service converting the row 8-bit	C401.5	BTL 1

	binary stream to a stream of printable ASCII characters. The scheme used forthis purpose is Radix-64 conversion		
11	**Name any cryptographic keys used in PGP?** a) One-time session conventional keys. b) Public keys. c) Private keys. d) Pass phrase based conventional keys	C401.5	BTL 1
12	**Draw the ESP packet format?** Security Parameters Index Sequence number Payload data Padding Pad length Next header Authentication data	C401.5	BTL 1
13	**List the limitations of SMTP/RFC 822? (DEC 2016)** a) SMTP cannot transmit executable files or binary objects. b) It cannot transmit text data containing national language characters. c) SMTP servers may reject mail message over certain size. d) SMTP gateways cause problems while transmitting ASCII and EBCDIC. e) SMTP gateways to X.400 E-mail network cannot handle non textual dataincluded in X.400 messages. What are the key algorithms used in S/MIME? Digital signature standards. Diffi Hellman. RSA algorithm.	C401.5	BTL 1

For question 12, the bit ruler reads (columns 0 through 31):

0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1

14	**Give the steps for preparing envelope data MIME?** Generate Ks. - Encrypt Ks using recipient's public key. - RSA algorithm used for encryption. - Prepare the 'recipient info block'. - Encrypt the message using Ks.	C401.5	BTL 1
15	**What you mean by versioned certificate?** Mostly used issue X.509 certificate with the product name" versioneddigital id". Each digital id contains owner's public key, owner's name and serial number of the digital id.	C401.5	BTL 1
16	**What are the function areas of IP security?** - Authentication - Confidentiality - Key management	C401.5	BTL 1
17	**Give the application of IP security?** - Provide secure communication across private & public LAN. - Secure remote access over the Internet. - Secure communication to other organization	C401.5	BTL 1
18	**Give the benefits of IP security? (<u>APR 2017)</u>** - Provide security when IP security implement in router or firewall. - IP security is below the transport layer is transparent to the application. - IP security transparent to end-user. - IP security can provide security for individual user	C401.5	BTL 4
19	**What are the protocols used to provide IP security?** - Authentication header (AH) protocol. - Encapsulating Security Payload(ESP).	C401.5	BTL 1

20	**Specify the IP security services?** • Access control. • Connectionless interpretty. • Data origin authentication • Rejection of replayed packet. • Confidentiality. • Limited traffic for Confidentiality	C401.5	BTL 1
21	**What do you mean by Security Association? Specify the parameters that identifies the Security Association?** An association is a one-way relationship between a sender and receiver thataffords security services to the traffic carried on. A key concept that appears in both the authentication and confidentialitymechanism for ip is the security association (SA). A security Association is uniquely identified by 3 parameters: • Security Parameter Index (SPI). • IP Destination Address. • Security Protocol Identifier	C401.5	BTL 1
22	**Steps involved in SSL required protocol?** • SSL record protocol takes application data as input and fragments it. • Apply lossless Compression algorithm. • Compute MAC for compressed data. • MAC and compression message is encrypted using conventional alg.	C401.5	BTL 1
23	**List out the attacks fixed by SSL v3** • Downgrade Attack • Truncation Attack	C401.5	BTL 1
24	**What is mean by SET? What are the features of SET?** Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the internet.	C401.5	BTL 1

	Features are:		
	• Confidentiality of information		
	• Integrity of data		
	• Cardholder account authentication		
	• Merchant authentication		
25	**Define: Truncation Attack** SSLv2 depends on TCP Connection Closing to indicate there is no more data to send. TCP Connection close is not cryptographically protected. Attacker may utilize this to close the connection SSLv3 added a "finished message" to indicate there is no ore data to send.	C401.5	BTL 1
26	**What is the role of IKE?** Internet Key Exchange Is a protocol for mutual authentication and to establish a session key Alternatives to IKE are : Photuris – a signed Diffie-Hellman Key Exchange, using an stateless cookie SKIP (Simple Key –Management for Internet Protocols) – uses long term Diffie-Hellman public keys	C401.5	BTL 1
27	**What are the phases of IKE?** **Phase 1** Does mutual authentication and establish session keys Expensive Phase 1 exchange is also known as ISAKMP SA [Internet Security Association and Key Management Protocol] or IKE SA **Phase 2** Simpler and cheaper Use the session key created out of phase-1 exchange	C401.5	BTL 1
28	**Define BOTNETS? (DEC 2016)**		

	A BOTNET (zombie army) is a number of internet computers that although their owners are unaware of it, have been set up to forward transmission to other on the internal.	C401.5	BTL 1
29	**Purpose of id payload in ISAKMP/IKE encoding? (NOV /DEC 2017)** ID payload contains a vendor-defined constant. This is used to identify and recognize remote instances of vendor's implementations. This could be used to experiment with new features and at the same time maintain backward compatibility	C401.5	BTL 1
30	**What is the difference between TLS and SSL security? (APRIL /MAY 2018)** **Secure Sockets Layer (SSL)** is a cryptographic protocol that enables secure communications over the Internet. SSL works mainly through using public/private key encryption on data. It is commonly used on web browsers, but SSL can also be used with email servers or any kind of client-server transaction. T**ransport Layer Security (TLS)** is the successor to SSL. TLS uses stronger encryption algorithms and has the ability to work on different ports.	C401.5	BTL 1

PART B

1	**Explain in detail about the security services (PGP, S/MIME) for E-mail. Williams Stalling P.No: 479-482 , 457-474**	C401.5	BTL 1
2	**Explain the operation description of PGP.(APR2011, NOV2012, NOV2010, NOV2009, MAY2009,DEC2016, APRIL 2018) Williams Stalling P.No: 479-482**	C401.5	BTL 1
3	**Explain in detail about architecture of IP Security. (APR2011, APR 2012, NOV2010, DEC 2017) Williams Stalling P.No: 443-526**	C401.5	BTL 1
4	**Discuss authentication , header and ESP in detail with their packet format (APR 2017, NOV 2017) Williams Stalling P.No: 489, 498-503**	C401.5	BTL 1
5	**Describe the SSL Architecture in detail. (APR2011, NOV 2011, MAY2009, NOV2007) Williams Stalling P.No: 531-544**	C401.5	BTL 1
6	**Discuss the working of SET & PKI with neat diagram.(APR2011, NOV2011, APR2012, NOV2012, NOV2010,DEC2016, APRIL 2018) Williams Stalling P.No: 549-560**	C401.5	BTL 1
7	**Explain the steps, methodology involved in SSL/TLS protocol? (NOV/DEC 2017)**	C401.5	BTL 1

Reg. No. : ☐☐☐☐☐☐☐☐☐☐☐☐☐

Question Paper Code : 80304

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2016.

Seventh Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Seventh Semester Information Technology)

(Regulations 2013)

Time : Three hours   Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Compare active and passive attack.

2. Find gcd (1970, 1066) using Euclid's algorithm.

3. Brief the strengths of triple DES.

4. What is an elliptic curve?

5. State any three requirements for authentication.

6. Differentiate MAC and Hash function.

.7. List the three classes of intruders.

8. Define Zombie.

9. List the limitations of SMTP/RFC 822.

10. Define Botnets.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain OSI Security Architecture model with neat diagram.   (8)
        (ii) Describe the various security mechanisms.   (8)

Or

    (b) (i) State Chinese Remainder theorem and find X for the given set of
            congruent equations using CRT.
            X = 2(mod 3)
            X = 3(mod 5)
            X = 2(mod 7).   (8)
        (ii) State and prove Fermat's theorem.   (8)

12. (a) Explain AES algorithm with all its round functions in detail. (16)

Or

(b) Explain RSA algorithm, perform encryption and decryption to the system with $p = 7$; $q = 11$; $e = 17$; $M = 8$. (16)

13. (a) Describe MD5 algorithm in detail. Compare its performance with SHA-1. (16)

Or

(b) Explain digital signature standard with necessary diagrams in detail. (16)

14. (a) Discuss Client Server Mutual authentication, with example flow diagram. (16)

Or

(b) Explain the technical details of firewall and describe any three types of firewall with neat diagram. (16)

15. (a) Discuss the working of SET with neat diagram. (16)

Or

(b) Explain the operational description of PGP. (16)

———————

Reg. No. :

Question Paper Code : 71690

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2017.

Seventh/Eighth Semester

Computer Science and Engineering

CS 6701 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Electronics and Communication Engineering and Information Technology)

(Regulations 2013)

Time : Three hours   Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1.   State Fermat's theorem.

2.   Determine the gcd (24140, 16762) using Euclid's algorithm.

3.   State the difference between private key and public key algorithm.

4.   Give the five modes of operation of block cipher.

5.   What is the role of compression function in hash function?

6.   Specify the various types of authentication protocol.

7.   Define the roles of firewalls.

8.   State the difference between threats and attacks.

9.   Draw the ESP packet format.

10. Specify the benefits of IPSec.

PART B — (5 × 16 = 80 marks)

11. (a)   State Chinese Remainder theorem and find X for the given set of congruent equations using CRT   (16)

$X \equiv 1 \pmod 5$

$X \equiv 2 \pmod 7$

$X \equiv 3 \pmod 9$

$X \equiv 4 \pmod{11}$

Or

(b) Describe :

   (i)   Playfair cipher

   (ii) Railfence cipher

   (iii) Vignere cipher.   (16)

12. (a) Explain Diffie-Hellman Key exchange algorithm in detail.   (16)

                                 Or

   (b) Describe DES algorithm with neat diagram and explain the steps.   (16)

13. (a) Compare the performance of RIPEMD-160 algorithm and SHA-1
        algorithm.   (16)

                                 Or

   (b) Explain the concepts of Digital signature algorithm with key generation
       and verification in detail.   (16)

14. (a) Discuss the different types of virus in detail. Suggest scenarios for
        deploying these types in network scenario.   (16)

                                 Or

   (b) Explain Intrusion Detection System (IDS) in detail with suitable
       diagram.   (16)

15. (a) Explain the architecture of IP security in detail.   (16)

                                 Or

   (b) Discuss authentication header and ESP in detail with their packet
       format.   (16)

                                 ———————