Nadar Saraswathi College of Engineering and Technology, **Vadapudupatti, Theni - 625 531** (Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)	Format No.	NAC/TLP-07a.12
	Rev. No.	01
	Date	14-11-2017
	Total Pages	01

Question Bank for the Units – I to V

SEM-	**VII Semester – B.E.**
BR-	**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**
	CS6701 – Cryptography & Network Security
	Part-A (10 x 2 = 20 Marks)
	UNIT – I

No	Question	Level	Competence	Mark
1.1	**List** the four categories of security threats.	L2	Comprehension	2
1.2	**Calculate** GCD of 1070 and 1066 using Euclid algorithm.	L3	Application	2
1.3	**Define** primitive root.	L2	Comprehension	2
1.4	**Give** examples for substitution cipher.	L1	Knowledge	2
1.5	**Define** cryptography8	L2	Comprehension	2
1.6	**Explain** why Modular arithmetic has been used in cryptography.	L5	Evaluation	2
1.7	**Compare** Block cipher and Stream cipher.	L4	Analysis	2
2.1	**Classify** the basic functions used in encryption algorithms.	L3	Application	2
2.2	**Describe** security mechanism.	L1	Knowledge	2

2.3	**Assess** the following cipher text using brute force attack: CMTMROOEOORW (Hint: Algorithm-Rail fence).	L5	Evaluation	2
2.4	**Generalize** why network need security.	L6	Synthesis	2
2.5	**Give** examples for transposition cipher.	L1	Knowledge	2
2.6	**Show** how to convert the given text "VALLIAMMAI" in to cipher text using Rail fence Technique.	L3	Application	2
2.7	**Plan** how many keys are required by two people to communicate via a cipher.	L6	Synthesis	2
	UNIT – II			
3.1	**Define** RC5.	L2	Comprehension	2
3.2	**List** the five modes of operation of block cipher.	L2	Comprehension	2
3.3	**Summarize** the purpose of S-boxes in DES.	L1	Knowledge	2
3.4	**Formulate** few applications of RC5 algorithm.	L6	Synthesis	2
3.5	**Give** the strengths of Triple DES.	L1	Knowledge	2
3.6	**Criticise** why the middle portion of triple DES a decryption rather than encryption?	L4	Analysis	2
3.7	**List** the function of state array.	L2	Comprehension	2
4.1	**Point out** is it possible to use the DES algorithm to generate message authentication code.	L4	Analysis	2
4.2	**Discover** the difference between sub bytes and sub words.	L3	Application	2
4.3	**Describe** the triple encryption. How many keys are used in triple encryption?	L1	Knowledge	2

4.4	**Give** the applications of the public key crypto systems.	L1	Knowledge	2
4.5	**Explain** any one attacking technique in RSA.	L5	Evaluation	2
4.6	**Discover** the Difference between public key and conventional encryption.	L3	Application	2
4.7	**Analysis** the purpose of Diffie Hellman key exchange.	L4	Analysis	2
	UNIT – III			
5.1	**Define** digital signature.	L2	Comprehension	2
5.2	**Compare** MD5 and SHA algorithm.	L4	Analysis	2
5.3	**Illustrate** the design objectives of HMAC.	L3	Application	2
5.4	**Define** digital signature.	L2	Comprehension	2
5.5	**Distinguish** DSA and ElGamal algorithm.	L6	Synthesis	2
5.6	**Define** MAC.	L2	Comprehension	2
5.7	**List** the requirements of hash function.	L5	Evaluation	2
6.1	**Estimate** the block size of MD5.	L1	Knowledge	2
6.2	**Differentiate** MAC and hash function.	L2	Comprehension	2
6.3	**Discriminate** message authentication code and one way hash function.	L2	Comprehension	2
6.4	**Show** how SHA is more secure than MD5.	L1	Knowledge	2
6.5	**List** any three hash algorithm.	L4	Analysis	2
6.6	**Formulate** how digital signature is different from conventional.Give any two.	L5	Evaluation	2

6.7	**Define** CMAC.	L2	Comprehension	2
	UNIT-IV			
7.1	**Define** Worm and Zombie.	L2	Comprehension	2
7.2	**Differentiate** spyware and virus.	L3	Application	2
7.3	**What** are the advantages of intrusion detection system over firewall?	L2	Comprehension	2
7.4	**Define**: SET	L2	Comprehension	2
7.5	**Define** virus. Specify the types of viruses?	L1	Knowledge	2
7.6	**Give** the uses of application level gateway?	L1	Knowledge	2
7.7	**Define** firewall.	L2	Comprehension	2
8.1	**What** is Kerberos? What are the uses?	L1	Knowledge	2
8.2	**What** do you mean by trusted systems?	L1	Knowledge	2
8.3	**List** 4 requirements were defined by Kerberos.	L2	Comprehension	2
8.4	**List** the classes of Intruders.	L2	Comprehension	2
8.5	**Mention** the limitations of firewalls.	L5	Evaluation	2
8.6	**Generalize** the role of Ticket Granting Server in inter realm operations of Kerberos?	L6	Synthesis	2
8.7	**Summarize** the purpose of X.509 standard?	L1	Knowledge	2
	UNIT- V			
9.1	**Define** S/MIME.	L2	Comprehension	2

9.2	**Quote** the applications of IP Security.	L2	Comprehension	2
9.3	What is meant by SET? What are the features of SET?	L1	Knowledge	2
9.4	**List** the steps involved in SET Transactions.	L2	Comprehension	2
9.5	**Define** the email compatibility function in PGP.	L2	Comprehension	2
9.6	**List** the elements of MIME.	L2	Comprehension	2
9.7	Why does PGP generate a signature before Applicationing compression?	L6	Synthesis	2
10.1	**Illustrate** services are provided by IPSec?	L3	Application	2
10.2	**Give** the expansion of SPI and describe its features.	L1	Knowledge	2
10.3	**Define** replay attack?	L2	Comprehension	2
10.4	**Compare** transport mode and tunnel mode.	L5	Evaluation	2
10.5	I**dentify** the purposes of SSL alert protocol.	L2	Comprehension	2
10.6	Why does ESP **Application** a padding field?	L3	Application	2
10.7	**Give** the reason for using PGP.	L1	Knowledge	2
	Part – B (5 x 16 = 80 Marks) or Part – B (5 x 13 = 65 Marks)			
	UNIT- I			
11.a-1	State and **Describe** (i) Fermat's theorem. (ii) Euler's theorem.	L2	Comprehension	8 5
11.a-2	(i) **Evalute** 3^{21} mod 11 using Fermat's theorem. (ii) State Chinese Remainder theorem and find X for the	L5	Evaluation	7 6

	given set of congruent equations using CRT. X=2(mod3) X=3(mod5) X=2(mod7)			
11.a-3	(i) **Discuss** the following a) Message Integrity (1) b) Denial of Service (1) c) Availability (1) d)Authentication(1) (ii) **Estimate** 11^{13} mod 53 using modular exponentiation. (9)	L1	Knowledge	1 1 1 1 9
11.a-4	**Summarize** the following in detail. (i) Modular Exponentiation. (ii) Finite fields.	L1	Knowledge	7 6
11.b-1	(i) **Application** Caesar cipher and k=5 decrypt the given Cipher text "YMJTYMJWXNIJTKXNQJSHJ". (ii) **Application** Vigenere cipher, encrypt the word "explanation"using the key "leg".	L3	Application	7 6
11.b-2	(i) **Discuss** briefly the Discrete Algorithms. (ii) **Discuss** about the Groups, Rings and Field	L1	Knowledge	6 7
11.b-3	(i) **Solve** using playfair cipher. Encrypt the word "Semester Result" with the keyword "Examination". List the rules used. (ii) **Demonstrate** the encryption of the message "PAY" using hill cipher with the following key matrix and show the decryption. $K=\begin{vmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{vmatrix}$	L3	Application	7 6
11.b-4	(i) **Explain** how to solve $x^2 \equiv 1 \pmod{35}$ using Chinese remainder theorem.	L4	Analysis	6 7

	(ii) **Explain** in detail the Euclid's Algorithm.			
	UNIT – II			
12.a-1	**Describe** in detail, AES algorithm with round functions.	L2	Comprehension	13
12.a-2	**Explain** the following modes of operation in block cipher. (i) Electronic code book and Cipher block chaining. (ii) Cipher feedback mode and output feedback mode	L4	Analysis	7 6
12.a-3	(i) **Formulate** the single round of DES algorithm. (ii)**Design** the key generation process of DES.	L6	Synthesis	7 6
12.a-4	(i) **Describe** the RC5 method used for encryption and decryption. (ii)**Describe** Triple DES and its applications.	L2	Comprehension	6 7
12.b-1	(i) Draw the general structure of DES and **describe** how encryption and decryption are carried out. (ii) **Identify** the strength of DES algorithm.	L2	Comprehension	6 7
12.b-2	(i) How AES is used for encryption/Decryption?**Discuss** with example. (ii) **Discuss** in detail about Blowfish.	L1	Knowledge	7 6
12.b-3	**Evaluation** using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7. (i) If user A has private key XA=3.What is A's public key YA? (ii)If user B has private key XB=6. What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm.	L5	Evaluation	13
12.b-4	(i) **Describe** RSA Algorithm. (ii)**Estimate** the encryption and decryption values for the RSA algorithm parameters. P=7, Q=11, E=17, M=8.	L1	Knowledge	7 6

	UNIT – III			
13.a-1	(i)**Describe** HMAC algorithm in detail. (ii)**Explain** the classification of authentication function in detail.	L1	Knowledge	7 6
13.a-2	(i)**Compare** the features of SHA and MD5 algorithm (ii)**Discuss** about the objectives of HMAC and its security features.	L6	Synthesis	7 6
13.a-3	**Describe** the MD5 message digest algorithm with necessary block diagrams.	L4	Analysis	13
13.a-4	(i)**Illustrate** simple hash function and birthday attack. (ii) **Compare** HMAC and CMAC.	L3	Application	7 6
13.b-1	**Explain** in detail ElGamal Public key cryptosystems with an example.	L2	Comprehension	13
13.b-2	**Discuss** about Authentication protocols.	L1	Knowledge	13
13.b-3	**Explain** in detail (i) Message authentication code (ii) Requirements of MAC	L1	Knowledge	6 7
13.b-4	(i)**Enumerate** the properties of Hash Function. (ii)**Describe** the authentication protocol and list its limitations, how the limitations overcome.	L4	Analysis	7 6
	UNIT –IV			
14.a-1	(i)What are the requirements of Kerberos? (ii)**Explain** about Kerberos version 4.	L6	Synthesis	7 6
14.a-2	(i) **Explain** the Firewall design principles.	L4	Analysis	7 6

	(ii) **Explain** firewalls and how they prevent intrusions.			
14.a-3	(i)**Explain** viruses? (ii)**Evaluation** the virus related threats and the counter measures.	L5	Evaluation	3 10
14.a-4	**Illustrate** the three common types of firewalls with diagrams.	L2	Comprehension	13
14.b-1	**Explain** Secure Electronic Transaction with neat diagram.	L2	Comprehension	13
14.b-2	**Illustrate** the following (i) statistical anomaly detection (ii) rule based intrusion detection system	L3 L4	Application & Analysis	7 6
14.b-3	Explain how kerberos **Application** the authentication dialog for obtaining services from another realm.	L3	Application	13
14.b-4	(i) **Discover** the participants of SET system, and explain in detail. (ii) **Illustrate** the Trojan Horse Defence in trusted system.	L3	Application	7 6
	UNIT V			
15.a-1	(i) **Summariz**e the services provided by PGP. (ii)**Discuss** the threats faced by an e-mail and explain its security requirements to provide a secure e-mail service.	L1	Knowledge	5 8
15.a-2	(i)**Describe** about the PKI. (ii)**Identify** the fields in ISAKMP and explain it.	L2	Comprehension	7 6
15.a-3	(i)**Discuss** about the authentication header of IP. (ii)S**ummarize** encapsulating security payload of IP	L1	Knowledge	7 6
15.a-4	**Describe** the phases of Internet key exchange in detail.	L2	Comprehension	13

15.b-1	(i)**Analysis** the Cryptographic algorithm used in S/MIME. (ii)**Explain** how PKI is deployed by SSL	L4	Analysis	7 6
15.b-2	(i)What is PGP? **Show** the message format of PGP (ii)**Illustrate** the key rings and its significance in PGP.	L3	Application	6 7
15.b-3	(i)**Label** the fields in IP security authentication header and explain the functions of each field. (ii)**Identify** transport mode and tunnel mode authentication in IP?	L2	Comprehension	5 8
15.b-4	(i)**Demonstrat**e secure Electronic Transaction with neat diagram. (ii)**Discover** how ESP is applied to both transport and tunnel modes in IP?	L3	Application	7 6
	Part – C (1 x 15 = 15 Marks)			
	UNIT-1			
16 .a-1	**Formulate** ceaser cipher for the cipher Text: PHHW PH DIWHU WKH WRJD SDUWB to identify the plain text with the default key K=3 and also give atleast three important characteristics of this problem that is enabled to brute force cryptanalysis.	L6	Synthesis	15
16 .a-2	**Design** the plaintext in rows of width *l* and read it off by columns. Take the columns in a order defined by a key. If you take the columns in their natural order— without using a key—, then the procedure amounts to a path transposition. The Scytale corresponds to such a columnar transposition with a trivial key. **Example:** *l* = 5, Keyword = A P P L E Key = 1 4 5 3 2 Plaintext = T H I S I S A C O L U M N A R	L6	Synthesis	15

	T R A N S P O S I T I O N			
	(OR)			
16.b-1	**Point out** an example of polynomial arithmetic over GF(2). For f(x) = (x7 + x5 + x4 + x3 + x + 1) and g(x) = (x3 + x + 1), the figure shows f(x) + g(x); f(x)- g(x); f(x) * g(x); and f(x)/g(x). Note that g(x) f(x).	L5	Evaluation	15
16.b-2	**Analyze** how the ITU-T3 Recommendation X.800, Security Architecture for OSI, defines such a systematic approach.	L5	Evaluation	15
	UNIT-2			
16 .a-1	**Compose** the example of using simplified DES Input:1 0 1 0 0 1 0 1 Key:0 0 1 0 0 1 0 1 1 1 with suitable justification	L6	Synthesis	15
16 .a-2	**Assess** the criteria used in the design of DES, as reported in [COPP94], focused on the design of the S-boxes and on the P function that takes the output of the S boxes .	L5	Evaluation	15
	(OR)			
16.b-1	**Deduce** the types of attacks to which information is typically subjected in CNS.	L5	Evaluation	15
16.b-2	**Discuss**: though any size of block is acceptable, following aspects are borne in mind while selecting a size of a block.	L6	Synthesis	15
	UNIT-3			
16 .a-1	**Integrate** the entire MAC process in detail and also explain the (i) Establishment of Shared Secret (ii) Inability to Provide Non-Repudiation	L6	Synthesis	**7** **8**

16 .a-2	**Discriminate** the security of hash functions and MACs	L5	Evaluation	**15**
	(OR)			
16.b-1	**Recommend** any one method of efficient implementation of HMAC.	L5	Evaluation	**15**
16.b-2	With a neat flowchart, **design** MD5 processing of a single 512 bit block.	L6	Synthesis	**15**
	UNIT-4			
16 .a-1	**Prepare** a summary on the significant types of virus categories.	L6	Synthesis	**15**
16 .a-2	**Integrate how** does a screened host architecture for firewalls differ from a screened subnet firewall architecture?	L6	Synthesis	**15**
	(OR)			
16.b-1	**Support** with an example, how a user's certificate is obtained from another certification authority in X.509	L5	Evaluation	**15**
16.b-2	**Assess** the firewall design principle, characteristics and capabilities of firewalls	L5	Evaluation	**15**
	UNIT-5			
16 .a-1	**Compose** how does PGP provide authentication and confidentiality for email services and for file transfer applications?	L6	Synthesis	**15**
16 .a-2	(i)**Formulate** Security Association? (ii)**Invent** the parameters that identify the Security Association.	L6	Synthesis	**7** **8**
	(OR)			
16.b-1	**(i)Assess** the main problem with IPV4 that IPV6 addresses **(ii)Decide** the factors combined to cause the exhaustion of IPV4	L5	Evaluation	**7** **8**

16.b-2	**Deduce** the overall function of TLS/SSL.	L5	Evaluation	**15**

L1: Knowledge, L2: Comprehension, L3: Application, L4: Analysis, L5: Evaluation, L6: Synthesis

QUESTION BANK SUMMARY

S.NO	UNIT	DETAILS	L1	L2	L3	L4	L5	L6	TOTAL
1	Unit-1	PART-A	3	3	3	1	2	2	14
		PART-B	3	1	2	1	1	-	08
		PART-C	-	-	-	-	2	2	04
2	Unit-2	PART-A	4	3	2	3	1	1	14
		PART-B	2	3	-	1	1	1	08
		PART-C	-	-	-	-	2	2	04
3	Unit-3	PART-A	2	6	1	2	2	1	14
		PART-B	3	1	1	2	-	1	08
		PART-C	-	-	-	-	2	2	04
4	Unit-4	PART-A	5	6	1	-	1	1	14
		PART-B	-	2	3	2	1	1	09
		PART-C	-	-	-	-	2	2	04
5	Unit-5	PART-A	3	7	2	-	1	1	14
		PART-B	2	3	2	1	-	-	08
		PART-C	-	-	-	-	2	2	04

Total No of Questions	PART-A	PART-B	PART-C	TOTAL
	70	41	20	131

Prepared By:

Staff Name: Vignesh L.S

STAFF IN CHARGE **HOD** **PRINCIPAL**