			B.Tech.,(Semest	er- VI)	
			Section A		
		Date : Duration :	March 07, 2018 45 mt	Assignment lest : Maximum Marks :	10
Ι					(5,5 Marks)
	(a)	What are the char	acteristics of Cryptographic hash f	functions?	
	(b)	Describe the gene	eral structure of a Cryptographic ha	ash function.	
П					(10 Marks)
		D			(101/10/10)
	(a)	Describe SHA512	2 hash function.		
III					(5,5 Marks)
	(a)	What are the vari	ous ways in which message auther	ntication service is offered?	
	(b)	What are the requ	irements of Message Authentication	on Code?	
IV					(10 Marks)
	(\cdot)				()
	(a)	write about HMA	AC.		
V					(5,5 Marks)
	(a)	Describe essentia	l components of a Digital Signatur	e process.	
	(b)	Write about Elgar	mal Digital Signature scheme		
VI					(10 Marks)
• •		11 X 500			(10 1/14/18)
	(a)	How X.509 certif	icates are useful for Public key dis	stribution.	

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI)

BAPATLA ENGINEERING COLLEGE (Autonomous) Department of Information Technology I Mid Term Examinations

Subject	:	Introduction to Cyber Security (14IT603)	Class	:	VI Sem. Sec. B
Max. Marks	:	30	Duration	:	1 hr. 30 mts.
Date	:	January 11, 2018	A.Y.	:	2017-18

PART-A

Answer all questions Each question carries equal marks

(6 Marks)

- (a) What is confusion in the context of encryption?
- (b) What is a product cipher?
- (c) What is a nonce?
- (d) What is a one-way function?
- (e) Why it is difficult to attack RSA public-key cryptosystem?
- (f) What is a digital signature?

PART-B

Answer any one question

Π

Ι

2

- (a) Describe the three characteristics of a Cryptographic systems.
- (b) Write about DES algorithm.

OR

III

- (a) Describe the modes of operation used to convert a block cipher algorithm to stream cipher algorithm.
- (b) How a Double DES algorithm is subjected to meet-in-the middle attack?

PART-C

Answer any one question

IV

- (a) Write about RSA public-key cryptosystem.
- (b) What requirements must a public-key cryptosystem fulfill to be a secure algorithm?

OR

V

- (a) Write about Diffie-Hellman key exchange algorithm.
- (b) Describe the man-in-the-middle attack on the Diffie-Hellman key exchange algorithm.

(3,9 Marks)

(9,3 Marks)

(6,6 Marks)

(6,6 Marks)

Introduction to Cyber Security 14IT605 B.Tech(Semester- VI) Section A								
Da	ate	:	December 26, 2018	Alternate	Assessment Test	:		Ι
D	uration	:	45 mts.	1	Maximum Marks	:	3	0
Se	et-I (Rno mod 3 == 0)							
I	What is the OSI security	⁷ are	chitecture?			(3	M)	
II	What is steganography?					(3	M)	
III	Briefly describe the Play	/fai	r cipher.			(3	M)	
IV	Briefly describe the Hill	cip	her.			(3	M)	
V	Briefly define types of c	ryp	tanalytic attacks based or	what is known to the attack	er.	(3	M)	
VI	What are two problems	witl	h the one-time pad?			(3	M)	
VII	What is the difference be	etw	een diffusion and confusi	on?		(3	M)	
VIII	What is a product cipher	r?				(3	M)	
IX	What is the purpose of the	he S	S-boxes in DES?			(3	M)	
Х	Explain the avalanche et	ffec	t.			(3	M)	

			B.Tech., (Semester- VI) Section	n A		
Da	ite	:	December 26, 2018	Alternate Assessment Test	:	Ι
Dı	uration	:	45 mts.	Maximum Marks	:	30
Se	t-II (Rno mod 3 == 1)					
Ι	What is the difference be	etw	een passive and active security threats?		(3 N	1)
II	Briefly define categories	of	security services.		(3 N	1)
III	What is the difference be M)	etw	een an unconditionally secure cipher and	d a computationally secure cipl	ner?	(3
IV	Briefly describe the Caes	sar	cipher.		(3 N	1)
V	Briefly describe the mon	loal	phabetic cipher.		(3 N	1)
VI	What is the difference be	etw	een a monoalphabetic cipher and a polya	alphabetic cipher?	(3 N	(1)
VII	Why is it important to st	udy	the Feistel cipher?		(3 N	1)
VIII	What is the difference be	etw	een a block cipher and a stream cipher?		(3 N	1)
IX	Which parameters and de	esi	gn choices determine the actual algorithm	n of a Feistel cipher?	(3 N	1)
Х	What is a singular transf	orn	nation? Give one example.		(3 N	1)

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI) Section A

Date	:	December 26, 2018	Alternate Assessment	Test :
Duration	:	45 mts.	Maximum M	larks : 30
Set-III (Rno mod .	3 == 2)			
I Briefly define c	ategories of	passive and active security attac	ks.	(3 M)
II Briefly define c	ategories of	security mechanisms.		(3 M)
III What are the est	sential ingre	edients of a symmetric cipher?		(3 M)
IV What are the tw	o basic fun	ctions used in encryption algorith	ıms?	(3 M)
V How many keys	are require	ed for two people to communicate	e via a cipher?	(3 M)
VI What is the diff	erence betw	een a block cipher and a stream	cipher?	(3 M)
VII What are the tw	o general aj	pproaches to attacking a cipher?		(3 M)
III What is a transp	osition cipl	ner?		(3 M)
IX Why is it impor	tant to stud	y the Feistel cipher?		(3 M)
X What is the diff	erence betw	een a block cipher and a stream	cipher?	(3 M)
	Ir	troduction to Cyber Se B.Tech.,(Semester- VI)	curity 14IT605 Section A	
Date	:	January 05, 2019	Alternate Assessment	Test : II
Duration Set-I (Rno mod 5	: ==0)	45 mts.	Maximum Ma	arks : 30
I Describe Cipher	Block Cha	ining mode of operation along w	vith its merits and demirits	(5 M)
-				

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI) Section A						
Date	: January 05, 2019	Alternate Assessment Test : II				
Duration	: 45 mts.	Maximum Marks : 30				
Set-II (Rno mod .	5 == 1)					
I What is multip	le encryption?	(3 M)				
II Describe Electronic Code Book mode of operation along with its merits and demirits						

Ш	Why is the middle portion of 3DES a decryption rather than an encryption?	(2 M)

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI) Section A					
Date Duration Set-III (Rno mod 5 == 2)	:	January 05, 2019 45 mts.	Alternate Assessment Test Maximum Marks	:	II 30
I What is a meet-in-the-middle attack?			(5 M	[)	

II	Describe Cipher	Feedback mode of	operation along with i	its merits and demirits	(5 M)
	1		1 0		

B.Tech.,(Semester- VI) Section A						
Date	: January 05, 2019	Alternate Assessment Tes	t :	II		
Duration	: 45 mts.	Maximum Mark	s :	30		
Set-III (Rno mod 5 ==	= 3)					
I How assymmetric	encryption provides confidentia	ality service?	(5 N	1)		
II How assymmetric	encryption provides authenticat	tion service?	(5 N	1)		

Introduction to Cyber Security 14IT605

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI) Section A						
Date	: January 05, 2019	Alternate Assessment Test : II				
Duration	: 45 mts.	Maximum Marks : 30				
Set-III (Rno mod S	5 == 4)					
I Describe Count	er mode of operation along with its merit	s and demirits (4 M)				
II Describe RSA c	ryptosystem	(6 M)				

BAPATLA ENGINEERING COLLEGE (Autonomous) Department of Information Technology I Mid Term Examinations

Subject	:	Introduction to Cyber Security (14IT605)	Class	:	VII Sem. Sec. B
Max. Marks	:	30	Duration	:	1 hr. 30 mts.
Date	:	January 11, 2018	A.Y.	:	2017-18

PART-A

Answer all questions Each question carries equal marks

	(6 Marks)
(a) What is confusion in the context of encryption?	
(b) What is a product cipher?	
(c) What is a nonce?	

(d) What is a one-way function?

(e) Why it is difficult to attack RSA public-key cryptosystem?

(f) What is a digital signature?

PART-B

Answer any one question

II

III

Ι

(a) Describe the three characteristics of a Cryptographic systems.

- (b) Write about DES algorithm.
- OR

(a) Describe the modes of operation used to convert a block cipher algorithm to stream cipher algorithm.

(b) How a Double DES algorithm is subjected to meet-in-the middle attack?

PART-C

Answer any one question

IV

- (a) Write about RSA public-key cryptosystem.
- (b) What requirements must a public-key cryptosystem fulfill to be a secure algorithm?

OR

V

(a) Write about Diffie-Hellman key exchange algorithm.

(b) Describe the man-in-the-middle attack on the Diffie-Hellman key exchange algorithm.

(9,3 Marks)

(3,9 Marks)

(6,6 Marks)

(6,6 Marks)

10

				Section	A			
		Date	:	March 07, 2018	Assignment Test	:	II	
		Duration	:	45 mt.	Maximum Marks	:	10	
Ι							(5,5	Marks)
	(a)	What are the c	har	acteristics of Cryptographic hasl	n functions?			
	(b)	Describe the g	ene	ral structure of a Cryptographic	hash function.			
II							(10	Marks)
	(a)	Describe SHA	512	hash function.				
III							(5,5	Marks)
	(a)	What are the v	ario	ous ways in which message auth	entication service is offered?			
	(b)	What are the re	equ	irements of Message Authentica	tion Code?			
IV							(10	Marks)
	(a)	Write about H	MA	С.				
V							(5,5	Marks)
	(a)	Describe essen	ntia	components of a Digital Signat	ure process.			
	(b)	Write about El	gar	nal Digital Signature scheme				
VI							(10	Marks)
	(a)	How X.509 ce	rtif	cates are useful for Public key d	listribution.			

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI)

BAPATLA ENGINEERING COLLEGE (Autonomous) Department of Information Technology I Mid Term Examinations

Subject	:	Introduction to Cyber Security (14IT605)	Class	:	VII Sem. Sec. B
Max. Marks	:	30	Duration	:	1 hr. 30 mts.
Date	:	January 11, 2018	A.Y.	:	2017-18

PART-A

Answer all questions Each question carries equal marks

	(6 Marks)
(a) What is confusion in the context of encryption?	
(b) What is a product cipher?	
(c) What is a nonce?	

(d) What is a one-way function?

(e) Why it is difficult to attack RSA public-key cryptosystem?

(f) What is a digital signature?

PART-B

Answer any one question

II

III

Ι

- (a) Describe the three characteristics of a Cryptographic systems.
- (b) Write about DES algorithm.
- OR
- (a) Describe the modes of operation used to convert a block cipher algorithm to stream cipher algorithm.
- (b) How a Double DES algorithm is subjected to meet-in-the middle attack?

PART-C

Answer any one question

IV

- (a) Write about RSA public-key cryptosystem.
- (b) What requirements must a public-key cryptosystem fulfill to be a secure algorithm?

OR

V

(a) Write about Diffie-Hellman key exchange algorithm.

(b) Describe the man-in-the-middle attack on the Diffie-Hellman key exchange algorithm.

12

(6,6 Marks)

(3,9 Marks)

(9,3 Marks)

(6,6 Marks)

		D. Iteli, (Semester- VI)		
	Date : March 07, 2	018 Assignment Test	:	II
	Duration : 45 mt.	Maximum Marks	:	10
Ι				(5,5 Marks)
	(a) What are the characteristics of C	Cryptographic hash functions?		
	(b) Describe the general structure o	f a Cryptographic hash function.		
II				(10 Marks)
	(a) Describe SHA512 hash function	1.		
III				(5,5 Marks)
	(a) What are the various ways in wh	hich message authentication service is offered?		
	(b) What are the requirements of M	lessage Authentication Code?		
IV				(10 Marks)
	(a) Write about HMAC.			
V				(5,5 Marks)
	(a) Describe essential components of	of a Digital Signature process.		
	(b) Write about Elgamal Digital Sig	gnature scheme		
VI				(10 Marks)
	(a) How X.509 certificates are usef	ul for Public key distribution.		

Introduction to Cyber Security 14IT605 B.Tech.,(Semester- VI)