Introduction to Cyber Security

14IT605

B.Tech.,(Semester- VI)

Section A

Date	:	March 07, 2018	Assignment Test	:	II
Duration	:	45 mt.	Maximum Marks	:	10

I **(5,5 Marks)**

(a) What are the characteristics of Cryptographic hash functions?

(b) Describe the general structure of a Cryptographic hash function.

II **(10 Marks)**

(a) Describe SHA512 hash function.

III **(5,5 Marks)**

(a) What are the various ways in which message authentication service is offered?

(b) What are the requirements of Message Authentication Code?

IV **(10 Marks)**

(a) Write about HMAC.

V **(5,5 Marks)**

(a) Describe essential components of a Digital Signature process.

(b) Write about Elgamal Digital Signature scheme

VI **(10 Marks)**

(a) How X.509 certificates are useful for Public key distribution.

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

I **(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 **(3,9 Marks)**

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

OR

III **(9,3 Marks)**

(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 **(6,6 Marks)**

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

OR

V **(6,6 Marks)**

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

Introduction to Cyber Security 14IT605

B.Tech.,(Semester- VI) Section A

Date	:	December 26, 2018	Alternate Assessment Test	:	I
Duration	:	45 mts.	Maximum Marks	:	30

Set-I (Rno mod 3 == 0)

I	What is the OSI security architecture?	**(3 M)**
II	What is steganography?	**(3 M)**
III	Briefly describe the Playfair cipher.	**(3 M)**
IV	Briefly describe the Hill cipher.	**(3 M)**
V	Briefly define types of cryptanalytic attacks based on what is known to the attacker.	**(3 M)**
VI	What are two problems with the one-time pad?	**(3 M)**
VII	What is the difference between diffusion and confusion?	**(3 M)**
VIII	What is a product cipher?	**(3 M)**
IX	What is the purpose of the S-boxes in DES?	**(3 M)**
X	Explain the avalanche effect.	**(3 M)**

Introduction to Cyber Security 14IT605

B.Tech.,(Semester- VI) Section A

Date	:	December 26, 2018	Alternate Assessment Test	:	I
Duration	:	45 mts.	Maximum Marks	:	30

Set-II (Rno mod 3 == 1)

I	What is the difference between passive and active security threats?	**(3 M)**
II	Briefly define categories of security services.	**(3 M)**
III	What is the difference between an unconditionally secure cipher and a computationally secure cipher?	**(3 M)**
IV	Briefly describe the Caesar cipher.	**(3 M)**
V	Briefly describe the monoalphabetic cipher.	**(3 M)**
VI	What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?	**(3 M)**
VII	Why is it important to study the Feistel cipher?	**(3 M)**
VIII	What is the difference between a block cipher and a stream cipher?	**(3 M)**
IX	Which parameters and design choices determine the actual algorithm of a Feistel cipher?	**(3 M)**
X	What is a singular transformation? Give one example.	**(3 M)**

Introduction to Cyber Security 14IT605

B.Tech.,(Semester- VI) Section A

Date	:	December 26, 2018	Alternate Assessment Test	:	I
Duration	:	45 mts.	Maximum Marks	:	30

Set-III (Rno mod 3 == 2)

I	Briefly define categories of passive and active security attacks.	**(3 M)**
II	Briefly define categories of security mechanisms.	**(3 M)**
III	What are the essential ingredients of a symmetric cipher?	**(3 M)**
IV	What are the two basic functions used in encryption algorithms?	**(3 M)**
V	How many keys are required for two people to communicate via a cipher?	**(3 M)**
VI	What is the difference between a block cipher and a stream cipher?	**(3 M)**
VII	What are the two general approaches to attacking a cipher?	**(3 M)**
VIII	What is a transposition cipher?	**(3 M)**
IX	Why is it important to study the Feistel cipher?	**(3 M)**
X	What is the difference between a block cipher and a stream cipher?	**(3 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-I (Rno mod 5 == 0)

I	Describe Cipher Block Chaining mode of operation along with its merits and demirits	**(5 M)**
II	Describe Output Feedback mode of operation along with 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 multiple encryption? **(3 M)**

II Describe Electronic Code Book mode of operation along with its merits and demirits **(5 M)**

III 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	:	January 05, 2019	Alternate Assessment Test	:	II
Duration	:	45 mts.	Maximum Marks	:	30

Set-III (Rno mod 5 == 2)

I What is a meet-in-the-middle attack? **(5 M)**

II Describe Cipher Feedback mode of operation along with 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-III (Rno mod 5 == 3)

I How assymmetric encryption provides confidentiality service? **(5 M)**

II How assymmetric encryption provides authentication service? **(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-III (Rno mod 5 == 4)

I Describe Counter mode of operation along with its merits and demirits **(4 M)**

II Describe RSA cryptosystem **(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

I **(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 **(3,9 Marks)**

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

OR

III **(9,3 Marks)**

(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 **(6,6 Marks)**

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

OR

V **(6,6 Marks)**

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

Introduction to Cyber Security

14IT605

B.Tech.,(Semester- VI)

Section A

Date	:	March 07, 2018	Assignment Test	:	II
Duration	:	45 mt.	Maximum Marks	:	10

I **(5,5 Marks)**

(a) What are the characteristics of Cryptographic hash functions?

(b) Describe the general structure of a Cryptographic hash function.

II **(10 Marks)**

(a) Describe SHA512 hash function.

III **(5,5 Marks)**

(a) What are the various ways in which message authentication service is offered?

(b) What are the requirements of Message Authentication Code?

IV **(10 Marks)**

(a) Write about HMAC.

V **(5,5 Marks)**

(a) Describe essential components of a Digital Signature process.

(b) Write about Elgamal Digital Signature scheme

VI **(10 Marks)**

(a) How X.509 certificates are useful for Public key distribution.

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

I **(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 **(3,9 Marks)**

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

OR

III **(9,3 Marks)**

(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 **(6,6 Marks)**

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

OR

V **(6,6 Marks)**

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

Introduction to Cyber Security

14IT605

B.Tech.,(Semester- VI)

Section A

Date	:	March 07, 2018	Assignment Test	:	II
Duration	:	45 mt.	Maximum Marks	:	10

I **(5,5 Marks)**

(a) What are the characteristics of Cryptographic hash functions?

(b) Describe the general structure of a Cryptographic hash function.

II **(10 Marks)**

(a) Describe SHA512 hash function.

III **(5,5 Marks)**

(a) What are the various ways in which message authentication service is offered?

(b) What are the requirements of Message Authentication Code?

IV **(10 Marks)**

(a) Write about HMAC.

V **(5,5 Marks)**

(a) Describe essential components of a Digital Signature process.

(b) Write about Elgamal Digital Signature scheme

VI **(10 Marks)**

(a) How X.509 certificates are useful for Public key distribution.