University of Rajshahi
Department of Computer Science and Engineering
B. Sc. Engg. Part-4 Even Semester, Examination-2022
CSE-4231 (Cryptography and Network Security)

Time: 3 Hours **Full Marks: 52.5**

[Answer any **six** questions taking at least **three** from each Section]

Section-A

1.	(a) What is restricted algorithm? What are the drawbacks of restricted algorithm?	2.75
	(b) The famous Caesar Cipher replace each character by the character three to the right modulo 26. Perform Caesar cipher then transposition cipher (width=5) on the plaintext m=" COMPUTER SCIENCE AND ENGINEERING". Leave the space as it is.	4
	(c) Differentiate between symmetric and asymmetric encryption.	2
2.	(a) What is birthday attack? Discuss the birthday attack against one-way hash function.	3
	(b) Mr. Bob uses 6byte alphanumeric characters to encrypt using DES. Calculate in detail the time required to break the password using a 1 billion attempts/s machine.	4
	(c) Discuss prime numbers generation technique in real world.	1.75
3.	a) If someone creates a database of all primes, won't he be able to use that database to break public key?	2
	b) How is S-box substitutions used to convert a 48-bit input to 32-bit output. Discuss with necessary figure and data.	4
	c) Briefly discuss the variants of DES.	2.75
4.	a) What is digital signature? Explain hash functions and digital signatures.	2.5
	b) Write down the properties of digital signature.	2.25
	c) Suppose n=3337, e=79 and d=1019. Encrypt the message m=1010567890987 using RSA public key algorithm and hence decrypt the encrypted message and show that it is equal to the original message m.	4

Section-B

5.	a) What is Kerberos? Briefly discuss Kerberos's credentials.	3
	b) Briefly discuss public-key authority technique to distribute public key.	2.75
	c) Suppose q=353, primitive root α =3, A's secret key X_A=97 and B's secret X_B=233. Use Diffie-Hellman key exchange algorithm to calculate the key.	3
6.	a) What is PGP?	1
	b) With a neat diagram explain how to get both the confidentiality and authentication service of PGP.	4.75
	c) What are the applications of IPSec?	3
7.	a) Compare between Message Digest (MD5) and Secure Hash Algorithm (SHA).	2.75
	b) What is firewall? Explain the limitations of firewalls?	3
	c) What is IP security? Explain the role of IPSec in the routing architecture	3
8.	a) To make sure your system is protected there are some actionable guides in 11 simple steps. Explain these steps.	3
	b) Data protection is very important. Discuss some encryption software tools available to protect your data.	3
	c) Differentiate among Trap doors, Logic bomb and Trojan horse.	2.75

University of Rajshahi

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

B.Sc. Engineering Part IV Even Semester Exam-2021

Course Code: CSE4231 **Course Title:** Cryptography and Network Security

Time: 3 Hours Full Marks: 52.50

[ANSWER ANY SIX QUESTIONS TAKING AT LEAST THREE FROM EACH SECTION]

SECTION A

1.(a) What is meant by Authentication, Integrity and Nonrepudiation? [2.00]

(b) Discuss in brief the following cryptanalytic attacks. [4.75]

i. Ciphertext-only attack
ii. Adaptive-Chosen-plaintext attack and
iii. Rubber-hose attacks.

(c) Suppose the key sequence from the pad is "ARPFUTHSNH". Encrypt "BANGLADESH" using one time pad and hence decrypt the encrypted message. [2.00]

2.(a) Compare among symmetric, public-key and hybrid cryptography. [3.00]

(b) a) Briefly discuss the terms. [4.00]

(i) Poor key choice (ii) Random keys (iii) Pass phrases and (iv) Updating keys

(c) Write the importance to update keys. Also write the effect of poor key choice. [1.75]

3.(a) RC5 is a symmetric-key block cipher algorithm designed by Ronald Rivest in 1994. Discuss RC5 for 64-bit data block. [5.00]

(b) How can you generate a longer hash value than a given hash function produces? [2.00]

(c) What is RSA? [1.75]

4.(a) Briefly discuss DES S-box substitution and P-box permutation with example. [4.00]

(b) In RSA algorithm suppose p=5, q=7 and e=11; find out the decryption key. [2.00]

(c) Discuss prime number test algorithm by Lehmann. [2.75]

SECTION B

5.(a) Kerberos is a trusted third-party authentication protocol designed for TCP/IP network. Briefly discuss the procedure [3+2]

(i) to get initial ticket (ii) to get a service.

(b) What is meant by key distribution? Explain the public-key certificate technique to distribute public key. [3.75]

6.(a) Why is PGP now widely used? [2.00]

(b) Write shortly the following services of PGP. [4.75]

i. Compression
ii. E-mail Compatibility and
iii. Segmentation and Reassembly.

(c) What are the applications of IPSec? [2.00]

7.(a) What is web security? [1.00]

(b) Compare the different threats on the web. [4.00]

(c) What is intruder? How can you protect password file? [3.75]

8.(a) What is digital signature? Describe direct digital signature. [3.75]

(b) Briefly discuss MD5 algorithm for message authentication. [3.00]

(c) Differentiate between Trap doors and Logic bombs. [2.00]

University of Rajshahi

Department of Computer Science and Engineering

B.Sc. (Engg.), Part-IV, Even Semester Examination, 2020

CSE-4231 (Cryptography and Network Security)

Time: 3 Hours | Full Marks: 52.5

[Answer any six questions taking any three from each section]

Section-A

1. (a) What is cryptanalytic attack? Differentiate between Known-plaintext attack and Chosen-ciphertext attack. 3
   (b) The famous Caesar Cipher replaces each character by the character three to the right modulo 26. Perform Caesar cipher and then transposition cipher (width=5) on the plaintext m=I LOVE MY COUNTRY. Leave the space as it is. 3
   (c) In fact one-time pad is unbreakable given infinite resources. Discuss one-time pad with example. 2.75

2. a) What is digital signature? Discuss signing technique with: 4
      i. Symmetric cryptosystems and an arbitrator.
      ii. Public-key cryptography.
   b) Mr. Bob uses 6 byte alphanumeric characters to encrypt using DES. Calculate in detail the time required to break the password using a 1 billion attempts/s machine. 3
   c) What is key crunching? Why pass phrase is important? 1.75

3. a) Define prime numbers, primitive root of a prime number, and Inverse modulo a number. 2.75
   b) DES has a 16 rounds of identical operations. Briefly discuss the operations in a round. 3
   c) Suppose (1010 0101 1100 0011 1001 1001 0111 0111) is the 32-bit input to an expansion permutation. What will be the equivalent 48-bit output? 3

4. a) What is one way hash function? Briefly discuss Message Digest 5 (MD5). 5
   b) Suppose n=3337, e=79 and d=1019. Encrypt the message m=010567890987 using RSA public key algorithm and hence decrypt the encrypted message and show that it is equal to the original message m. 3.75

Section-B

5. a) Explain the criticisms against Digital Signature Algorithm (DSA). 2
   b) What is Kerberos? How does Kerberos work? 4
   c) Briefly discuss Kerberos's credentials. 2.75

6. (a) 'Public-key authority' is a public key distribution technique. How does it work? 2
   (b) Prime number q=353, primitive root α =3, A's secret key X_A=97 and B's secret key X_B=233. Use Diffie-Hellman key exchange algorithm to calculate the key. 3
   (c) What is Pretty Good Privacy (PGP)? With a neat diagram explain the 'confidentiality and authentication' service of PGP. 3.75

7. a) What is IP security? Explain the role of IPSec in the routing architecture. 3
   b) Explain different types of intruders with example. 3
   c) How to learn passwords? Explain. 2.75

8. a) Briefly explain the followings terms: 3.75
      i. Trap doors.
      ii. Logic bomb.
      iii. Trojan horse.
   b) What is firewall? Briefly discuss Application-level gateway firewall. 3
   c) What are the techniques to control access and to enforce site's security policy? 2

University of Rajshahi
Department of Computer Science and Engineering
B. Sc. Engg. Part-4 Even Semester, Examination-2019
CSE-4231 (Cryptography and Network Security)

Time: 3 Hours | Full Marks: 52.5

[Answer any **six** questions taking at least **three** from each Section]

Section-A

1. (a) What do you mean by authentication, integrity and nonrepudiation? 3
   (b) Briefly discuss (i) ciphertext-only attack, (ii) adaptive-chosen-plaintext attack and rubber-hose cryptanalysis. 3
   (c) Differentiate between substitution cipher and transposition cipher with example. 2.75

2. (a) What is protocol? Discuss the communication using Symmetric cryptography. 2.75
   (b) Briefly discuss the following terms: one-way function, trapdoor one-way function, hash function, one-way hash function with example. 4
   (c) Explain birthday attack. 2

3. (a) How can you store, update, distribute and verify key? Explain. 4
   (b) No encryption key should be used for an indefinite period. Why? 2
   (c) What is the role of prime number in public key cryptography? Discuss prime numbers generation technique in real world. 2.75

4. (a) Why is it important to update the keys? Discuss the process of destroying the old keys. 3
   (b) Discuss the effect of reduced key space. 3
   (c) What do you mean by dictionary attack? Write the effect of poor key choice. 2.75

Section-B

5. (a) Explain the key features of Rivest Cipher (RC5) block cipher algorithm. 1.75
   (b) What is Rivest Shamir Adleman (RSA)? 1
   (c) Briefly discuss RSA algorithm. Suppose p=5, q=7, and e=11; find out the decryption key, then encrypt the message m=123456789 and finally decrypt. 6

6. (a) How can you generate a longer hash value than a given hash function produces? 2
   (b) Compare Message digest (MD5) and Secure Hash Algorithm (SHA). 2.75
   (c) Briefly discuss Kerberos's credentials. 4

7. (a) Explain the following public key distribution techniques: 4
      (i) Publicly Available Directory.
      (ii) Public-key certificates.
   (b) With neat diagram explain the confidentiality service of Pretty Good Privacy (PGP). 3
   (c) What is Internet Protocol (IP) security? 1.75

8. (a) What is a firewall? Write the strength and weakness of a firewall. 3
   (b) Mention different threats on the web. 2.75
   (c) What is R64 conversion? Explain why is R64 conversion is useful for e-mail application. 3

University of Rajshahi

Department of Computer Science and Engineering

B. Sc. (Engg.) Part-4 Even Semester Examination-2018

Course: CSE4231 (Cryptography and Network Security)

Full Marks: 52.5 Time: 3 Hours

[N.B. Answer **Six** questions taking at least **Three** from each Section]

Section-A

1.	(a)	Define the terms: Ciphertext, Encryption, Cryptography, and Cryptologist.	4
	(b)	Write some drawbacks of restricted algorithm?	2
	(c)	What is one-time pad? Discuss with example.	2.75
2.	(a)	Discuss the communication using hybrid cryptography.	2
	(b)	What is timestamps? Why it is important in some applications like digital checking? Explain.	4
	(c)	Briefly explain the time and cost estimates for Brute-force attack.	2.75
3.	(a)	What do you meant by key space? Discuss the effect of reduced key space.	4
	(b)	Define the terms: (i) Key crunching (ii) Greatest common divisor (iii) inverse modulo a number	3 1.75
	(c)	If someone creates a database of all primes, won't he be able to use that database to break public key?	2.5
4.	(a)	Explain the Lehmann's prime number test algorithm.	3.5
	(b)	Discuss DES initial permutation and final permutation in short.	2.75
	(c)	What do you mean by triple-DES? Explain in brief.	

Section-B

5.	(a)	What are the design goals of MD4 hash function?	1.75
	(b)	Briefly discuss secure hash algorithm (SHA).	3.5
	(c)	What RSA? Explain it with an example.	3.5
6.	(a)	What is Kerberos?	1
	(b)	Compare the message format of Kerberos V.4 and V.5.	2.75
	(c)	Discuss Diffie-Hellman key exchange with an example.	5
7.	(a)	What is PGP? Why is PGP now widely used?	2.75
	(b)	Briefly discuss confidentiality and authentication service of PGP with necessary diagram.	4
	(c)	Explain different types of intruders.	2
8.	(a)	Differentiate among Trap doors, Logic bomb and Trojan horse.	3
	(b)	What is virus? Explain the lifetime of virus.	3
	(c)	Briefly discuss the design goals and limitation of firewall.	2.75

University of Rajshahi
Department of Computer Science and Engineering
B. Sc. (Engg.) Part-4 Even Semester Examination-2016
CSE-4231 (Cryptography and Network Security)
Full Marks: 52.5 Time: 3:00 Hours

[Answer any SIX questions taking THREE from each section]

Section-A

1. a) Briefly define the play fair cipher. And encrypt the plain text "BANGLADESH" using the key "DHAKA". 5
   b) What is Feistel cipher and its importance? 3
   c) What is MIME? 0.75

2. a) Define the trapdoor one-way function and one-way hash function. 2
   b) How can you sign a document? Explain. 4
   c) What is timestamps? Why it is important in some applications like digital checking? Explain. 2.75

3. a) What is birthday attack? Explain. 1.75
   b) Briefly discuss the effect of reduced key space. 4
   c) Why is it necessary to update the key? How can you destroy old keys? 3

4. a) What is prime number? Explain prime number test algorithm by Lehmann. 3
   b) Briefly discuss DES initial permutation and final permutation. 3
   c) What is triple-DES? Discuss. 2.75

Section-B

5. a) How can you generate a longer hash value than a given hash function produces? 1.75
   b) Briefly discuss Secure Hash Algorithm (SHA). 3.5
   c) What is RSA? Briefly discuss RSA algorithm with example. 3.5

6. a) What is meant by key distribution? Discuss Diffie-Hellman key exchange with an example. 4
   b) Discuss different types of intruders. 3
   c) How can you protect password file? 1.75

7. a) What is logic Bomb? 2
   b) What is R64 conversion? Why R64 conversion useful for an e-mail application? 4.75
   c) What do you mean by Password management? 2

8. a) Explain how an IP packet is encrypted and authenticated using ESP of IP Sec. 4.75
   b) What characteristics are needed in a secure hash function? 4

University of Rajshahi
Department of Computer Science and Engineering
B. Sc. Engg. Part-4 Even Semester, Examination-2015
CSE-4231 (Cryptography and Network Security)

Time: 3 Hours | Full Marks: 52.5

[Answer any six taking at least three from each part.]

Part-A

1.	a) Define the following terms: Encryption, Cryptography, Cryptanalysis and Cryptologist.	3
	b) What are the differences between symmetric algorithm and public-key algorithm?	2.75
	c) Briefly discuss chosen-key attack, rubber-hose cryptanalysis.	3
2.	a) Describe the Caesar cipher method.	3
	b) Write down the encryption process with Playfair cipher method using proper example.	3
	c) Write down the algorithm structure of Feistel cipher method.	2.75
3.	a) What is key crunching? Why pass phrase is important?	2.75
	b) Discuss prime numbers generation technique in real world.	2
	c) Discuss different key storing techniques.	2
	d) No encryption key should be used for an indefinite period. Why?	2
4.	a) What is one way hash function?	0.75
	b) Briefly discuss DES S-box substitution and P-box permutation with example.	4
	c) Write down the design criteria for S-boxes in DES.	3
	d) What is the difference between Sub Bytes and Sub Word	1

Part-B

5.	a) What is digital signature? Why do need digital signature?	2
	b) Write the properties of digital signature.	1.75
	c) Describe about direct digital signature.	3
	d) Differentiate between MAC and hash function.	2
6.	a) What are the problems of symmetric encryption? How does public key encryption provide secrecy and authentication?	3
	b) What are the techniques for distribution of public keys? Explain one of them.	2.75
	c) Explain the usage of IPsec.	1
	d) Discuss the security and speed of RSA.	2
7.	a) What are the services provided by PGP?	1
	b) Explain the reasons for using PGP.	4
	c) Name any encryption keys used in PGP.	1
	d) Why E-mail compatibility function in PGP needed?	2.75
8.	a) What is web security? Compare the different threats on the web.	4
	b) Discuss the techniques to learn passwords.	2.75
	c) What are the limitations of firewalls?	2

University of Rajshahi
Department of Computer Science and Engineering
B. Sc. Engg. Part-4 Even Semester, Examination-2014
CSE-4231 (Cryptography and Network Security)

Time: 3 Hours | Full Marks: 52.5

[N.B: Answer any six taking at least three from each part.]

Part-A

1.	a)	What do you mean by Authentication, Integrity and Nonrepudiation?	3
	b)	Briefly discuss chosen-plaintext attack and chosen-ciphertext attack.	3
	c)	What is double transposition cipher? Explain with explain.	2.75
2.	a)	What are the problems of symmetric cryptosystems?	2.75
	b)	Briefly discuss signing document with public-key cryptography.	2
	c)	What is birthday attack? Discuss the birthday attacks against one-way hash function.	4
3.	a)	Define the following terms: Prime numbers, Greatest Common Divisor, and Inverse modulo a number.	3
	b)	Discuss the effect of reduced key space.	3.75
	c)	How can you destroy old keys?	2
4.	a)	Briefly discuss the features of Data Encryption Standard (DES)	3
	b)	Briefly discuss DES initial permutation and final permutation.	2.75
	c)	Discuss RC5 block cipher algorithm.	3

Part-B

5.	a)	What are the design goals of MD4?	1.75
	b)	Discuss MD5.	3.5
	c)	Discuss RSA algorithm with example.	3.5
6.	a)	What is DSA?	1
	b)	Briefly discuss Kerberos model.	2.75
	c)	What is the security of Kerberos?	2
	d)	Discuss Kerberos v.4	3
7.	a)	What is meant by key distribution?	1
	b)	Shortly discuss different techniques to distribute public key.	5.75
	c)	Briefly discuss the way to get a service.	2
8.	a)	What is intruder?	1
	b)	How can you protect password file?	2
	c)	Briefly discuss different types of viruses.	2.75
	d)	What is a firewall? What are the design goals of a firewall?	3