CAIAS
CHRIST ACADEMY
INSTITUTE FOR ADVANCED STUDIES
AFFILIATED TO BANGALORE UNIVERSITY

III Semester MCA Course Book – Cryptography and Network Security

3MCA3E3: Cryptography and Network Security

Course Book

II Semester MCA

Prepared by: -

Dr.C.Umarani

Head- Department of Computer Science and Applications

Christ Academy Institiue for Advanced studies,

III Semester MCA Course Book – Cryptography and Network Security

3MCA3E3: Cryptography and Network Security

Name of the Course: Cryptography and Network Security

Course Code: 3MCA3E3:

Course Credits: 4 Number of Hours per Week: 4

Total No. of Teaching Hours: 53

PEDAGOGY

Classrooms lecture, Subject related exercises, student seminar/presentation.

COURSE OBJECTIVE:

 To understand basics of cryptography and network security by symmetric encryption techniques for given

applications

 To apply block, stream ciphers to secure messages over insecure channels

 To analyze methods for message authentication and access control

 To evaluate how to encrypt application layer data to identify users and protect information

 To examine various protocols for intrusion detection and prevention against network threats

Course Outcomes:

After completing this course, students will be able to:

1. **Understand Cryptography Basics:** Explain the fundamentals of cryptography and network security, focusing on symmetric encryption.
2. **Apply Encryption Techniques:** Use block and stream ciphers to secure messages over insecure channels.

III Semester MCA Course Book – Cryptography and Network Security

3. **Analyze Authentication Methods:** Identify methods for message authentication and access control.
4. **Encrypt Application Data:** Apply encryption to secure application data, identify users, and protect information.
5. **Examine Security Protocols:** Understand and evaluate protocols for intrusion detection and prevention against network threats.

Unit I:

Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security

Mechanisms, A Model for Network Security, Symmetric Ciphers, Classical Encryption Techniques, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography

Unit II:

Block Cipher Principles, The Data Encryption Standard, The Strength of DES, Differential and Linear

Cryptanalysis, Block Cipher Design The AES Polynomials with Coefficients in GF(28), Simplified AES, Multiple Encryption and Triple DES, Block Cipher Modes of Operation, Stream Ciphers and RC4

Unit III

Fermat's and Euler's Theorem, The Chinese Remainder Theorem, The RSA Algorithm, Key

Management, Diffie-Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography, Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash

Functions, Security of Hash Functions and Macs

Unit IV [10 Hours]

Digital Signatures, Authentication Protocols, Digital Signature Standard, Kerberos, X.509

Authentication Service, Public-Key Infrastructure, IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key

Management

Unit V [10 Hours]

CAIAS
CHRIST ACADEMY
INSTITUTE FOR ADVANCED STUDIES
AFFILIATED TO BANGALORE UNIVERSITY

III Semester MCA Course Book – Cryptography and Network Security

Web Security, Secure Socket Layer and Transport Layer Security, Intruders, Intrusion Detection, Password Management, Malicious Software, Firewalls

References

1. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson

Internal Marks Matrix:

S.No	CRITERIA	MARKS
1	IE (Internal Examination)	15
2	ASSIGNMENTS	5
3	PRESENTATION	5
4	ATTENDANCE	5
TOTAL		30

Attendance Marks:

Attendance Percentage	Marks
76-80%	02 Marks
81-85%	03 Marks
86-90%	04 Marks
91-100%	05 Marks

III Semester MCA Course Book – Cryptography and Network Security

University Sample Question Paper:

CAIAS
CHRIST ACADEMY
INSTITUTE FOR ADVANCED STUDIES
AFFILIATED TO BANGALORE UNIVERSITY

III Semester MCA Course Book – Cryptography and Network Security

JP – 773

III Semester M.C.A./M.Sc. (Two Years Course) Examination, May/June 2023
(CBCS – 2021 – 22)
COMPUTER SCIENCE
MCA 3E3/MSC 3E3 : Cryptography and Network Security (Elective)

Time : 3 Hours Max. Marks : 70

Instructions : *1) Answer **any five** from Section – **A**.*
*2) Answer **any four** from Section – **B**.*

SECTION – A

Answer **any five** questions. **Each** question carries **six** marks. **(5×6=30)**

1. List and briefly define categories of passive and active security attacks.
2. With a diagram explain different Cipher block modes of operation.
3. Explain DEs Round Function and Key generation in detail.
4. Explain the Diffie-Hellman key exchange algorithm with an example.
5. Write RSA algorithm and perform encryption and decryption on given message p = 17, q = 11, e = 7, m = 88.
6. Explain X.509 certificate format with neat diagram.
7. Use Chinese Remainder Theorem to get value of message X.
   X = 3(mod 5)
   X = 1(mod 7)
   X = 6(mod 8)
8. Explain overview of IP security and its applications.

SECTION – B

Answer **any four** questions. **Each** question carries **ten** marks. **(4×10=40)**

9. Explain AES algorithm with neat diagrams.
10. Write short note on :
    a) Substitution techniques with its methods and example. 5
    b) Transposition techniques with its methods and example. 5

P.T.O.

CAIAS
CHRIST ACADEMY
INSTITUTE FOR ADVANCED STUDIES
AFFILIATED TO BANGALORE UNIVERSITY

III Semester MCA Course Book – Cryptography and Network Security

JP – 773

11. With neat diagram explain Kerberos application.

12. Write a note on :
    a) Digital signature. 5
    b) Hash functions. 5

13. Explain the following :
    a) Authentication Header. 5
    b) Encapsulating security payload. 5

14. Explain the security services and mechanisms mentioned in X.800 in detail.

CAIAS
CHRIST ACADEMY
INSTITUTE FOR ADVANCED STUDIES
AFFILIATED TO BANGALORE UNIVERSITY

III Semester MCA Course Book – Cryptography and Network Security

Assignment – Infosys Springboard- MOOC Course for 10 hours:

Sl.No.	Reg. No.	Student Name
1	P03BV23S126036	A SHIRLEY IRIS
2	P03BV23S126001	AAKARSH KUMAR
3	P03BV23S126003	NAMBIAR ANGITHA SHYLENDRAN
4	P03BV23S126053	ASHWINI. G
5	P03BV23S126002	ATHUL A JOE
6	P03BV23S126004	DEEPAK BLESSON ROSE C S
7	P03BV23S126031	GOWTHAM K B
8	P03BV23S126032	H K PREMANANDA
9	P03BV23S126005	JASTIN M B
10	P03BV23S126018	MANJUNATHA B S
11	P03BV23S126020	MANOJ C
12	P03BV23S126006	MONIKA G
13	P03BV23S126040	NAVEEN KUMAR N
14	P03BV23S126007	PUNITH KUMAR B
15	P03BV23S126055	RAJESH R
16	P03BV23S126019	ROHIT H
17	P03BV23S126021	SALMA SATHEESH
18	P03BV23S126054	SANGAVI B
19	P03BV23S126008	SANJITH M P
20	P03BV23S126009	SAPNA KUMARI
21	P03BV23S126010	SPANDANA P
22	P03BV23S126011	SRI HARIHARAN M
23	P03BV23S126012	USHA M L
24	P03BV23S126013	USHASHREE LV
25	P03BV23S126046	V KAVYA SREE
26	P03BV23S126014	MANASA S
27	P03BV23S126015	HEMANTH V
28	P03BV23S126033	MEGHANA M
29	P03BV23S126016	ALBIN JOSHI
30	P03BV23S126017	DIVYA S

III Semester MCA Course Book – Cryptography and Network Security

31	P03BV23S126022	ABHIRAMI S
32	P03BV23S126029	LAKSHMI M
33	P03BV23S126023	SUMA JARAGALA
34	P03BV23S126028	C YASWANTH
35	P03BV23S126039	PAVAN R
36	P03BV23S126050	MONICA A
37	P03BV23S126052	ASHWINI B
38	P03BV23S126024	M N DIVYASHREE
39	P03BV23S126025	ANUP V
40	P03BV23S126044	DHANUSHREE K S
41	P03BV23S126047	YASHWANTH KUMAR
42	P03BV23S126038	CHANDANA K
43	P03BV23S126030	ROHAN RAVI KELASKAR
44	P03BV23S126026	AMIT RAJENDRA BADIGER
45	P03BV23S126042	ABDUL NABI
46	P03BV23S126027	ADARSH K
47	P03BV23S126043	PRAVEEN
48	P03BV23S126037	NANDITHA K M
49	P03BV23S126049	PRAJWAL J
50	P03BV23S126051	SUDEEP N N
51	P03BV23S126045	LIKITHA SHETTY B R
52	P03BV23S126041	FARDEEN KHAN
53	P03BV23S126048	GANESHA A M
54	P03BV23S126034	LAVANYA N
55	P03BV23S126035	BHAGYA SHREE C K

Presentation – Unit 1 :

Sl.No.	Reg. No.	Student Name
1	P03BV23S126036	A SHIRLEY IRIS
2	P03BV23S126001	AAKARSH KUMAR
3	P03BV23S126003	NAMBIAR ANGITHA SHYLENDRAN
4	P03BV23S126053	ASHWINI. G
5	P03BV23S126002	ATHUL A JOE

III Semester MCA Course Book – Cryptography and Network Security

6	P03BV23S126004	DEEPAK BLESSON ROSE C S
7	P03BV23S126031	GOWTHAM K B
8	P03BV23S126032	H K PREMANANDA
9	P03BV23S126005	JASTIN M B
10	P03BV23S126018	MANJUNATHA B S
11	P03BV23S126020	MANOJ C
12	P03BV23S126006	MONIKA G
13	P03BV23S126040	NAVEEN KUMAR N
14	P03BV23S126007	PUNITH KUMAR B
15	P03BV23S126055	RAJESH R
16	P03BV23S126019	ROHIT H
17	P03BV23S126021	SALMA SATHEESH
18	P03BV23S126054	SANGAVI B
19	P03BV23S126008	SANJITH M P
20	P03BV23S126009	SAPNA KUMARI
21	P03BV23S126010	SPANDANA P
22	P03BV23S126011	SRI HARIHARAN M
23	P03BV23S126012	USHA M L
24	P03BV23S126013	USHASHREE LV
25	P03BV23S126046	V KAVYA SREE
26	P03BV23S126014	MANASA S
27	P03BV23S126015	HEMANTH V
28	P03BV23S126033	MEGHANA M
29	P03BV23S126016	ALBIN JOSHI
30	P03BV23S126017	DIVYA S
31	P03BV23S126022	ABHIRAMI S
32	P03BV23S126029	LAKSHMI M
33	P03BV23S126023	SUMA JARAGALA
34	P03BV23S126028	C YASWANTH
35	P03BV23S126039	PAVAN R
36	P03BV23S126050	MONICA A
37	P03BV23S126052	ASHWINI B
38	P03BV23S126024	M N DIVYASHREE
39	P03BV23S126025	ANUP V
40	P03BV23S126044	DHANUSHREE K S

III Semester MCA Course Book – Cryptography and Network Security

41	P03BV23S126047	YASHWANTH KUMAR
42	P03BV23S126038	CHANDANA K
43	P03BV23S126030	ROHAN RAVI KELASKAR
44	P03BV23S126026	AMIT RAJENDRA BADIGER
45	P03BV23S126042	ABDUL NABI
46	P03BV23S126027	ADARSH K
47	P03BV23S126043	PRAVEEN
48	P03BV23S126037	NANDITHA K M
49	P03BV23S126049	PRAJWAL J
50	P03BV23S126051	SUDEEP N N
51	P03BV23S126045	LIKITHA SHETTY B R
52	P03BV23S126041	FARDEEN KHAN
53	P03BV23S126048	GANESHA A M
54	P03BV23S126034	LAVANYA N
55	P03BV23S126035	BHAGYA SHREE C K