

**(Established under the Presidency University Act, 2013 of the Karnataka Act 41 of 2013)**

**[2022-23 EVEN SEMESTER]**

**COURSE HAND OUT [Revision 02-Jan 2023]**

**SCHOOL:** School of CSE & IS **DEPT**.: **CSE-Allied DATE OF ISSUE:** 16-02-2023

**NAME OF THE PROGRAM : B.Tech**

**P.R.C. APPROVAL REF. : PU/AC18.8/CSE16/CSE/2021-25**

**SEMESTER/YEAR : IV Semester / II Year**

**COURSE TITLE & CODE : Cryptography and Network Security & CSE 3078**

**COURSE CREDIT STRUCTURE : 3-0-3**

**CONTACT HOURS : 3 SESSIONS PER WEEK**

**COURSE IC : Ms. B Prema Sindhuri, Mr. Gnanakumar G**

**COURSE INSTRUCTOR(S) : Dr. Anandaraj S P, Ms. Bhavana A, Mr. Prakash B Metre, Ms.Vani Ashok Hiremani, Mr. Shine V J, Dr. Vijaya Kumar A, Ms. Yashashwini D K, Dr. Robin Rohit, Dr. K Marimuthu.**

**COURSE URL :** [**https://camu.in/index#/TeachingPlan**](https://camu.in/index#/TeachingPlan)

**PROGRAM OUTCOMES:**

**PO-1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.**

**PO-2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.**

**PO-3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.**

PO-4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

**PO-5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations**

PO-6: **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO-7: **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of and need for sustainable development.

**PO-8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.**

PO-9: **Individual and teamwork:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO-10**: Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO-11: **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

**PO-12:Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.**

**COURSE PREREQUISITES:** Data Communications and Computer Networks

**COURSE DESCRIPTION:**

The Course covers the principles and practice of cryptography and network security, focusing in particular on the security aspects of the web and Internet.

**COURSE OUTCOMES: On successful completion of the course the students shall be able to:**

|  |  |  |
| --- | --- | --- |
| **TABLE 1: COURSE OUTCOMES** | | |
| **CO Number** | **CO** | **Expected BLOOMS LEVEL** |
| 1 | Identifies the basic concept of Cryptography | **Knowledge** |
| 2 | Apply the concepts of cryptographic algorithms | **Application** |
| 3 | Describe the Public key Cryptographic Techniques for various applications. | **Comprehension** |
| 4 | Explain the network security concepts during their implementation of different applications | **Comprehension** |

**MAPPING OF C.O. WITH P.O. [H-HIGH, M- MODERATE, L-LOW]**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TABLE 2: CO PO Mapping ARTICULATION MATRIX** | | | | | | | | | | | | |
| **CO. No** | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** |
| CO1 | H | M |  |  |  |  |  |  |  |  |  |  |
| CO2 | M | H |  |  | L |  |  | L |  |  |  |  |
| CO3 | L | M | L |  | M |  |  | L |  |  |  | L |
| CO4 |  | L | L |  |  |  |  | L |  |  |  | L |

**COURSE CONTENT (SYLLABUS):**

**Module 1: Introduction to Cryptography and types of Ciphers [8 Sessions] [Knowledge]**

Introduction to Cryptography, Model of Network Security, OSI Security architecture, Security Attacks: active attacks, passive attacks, services: Authentication, Access Control, Data Confidentiality, Data Integrity, Nonrepudiation, Substitution Ciphers : Caesar, Monoalphabetic, Polyalphabetic, Play-fair and Hill Cipher, Introduction to Block Cipher and Stream Cipher, Feistel Structure

**Module 2: Private Key Cryptography and Number Theory [13 Sessions] [Application]**

Symmetric Encryption Algorithms : Data Encryption Standard, Introduction to Galois Field, Advanced Encryption Standard, Modular Arithmetic, Prime numbers, Fermat’s little theorem, brief about primality testing and factorization, Discrete Logarithmic Problem, Euclidean and Extended Euclidean Algorithm, Euler Totient Function, Chinese Remainder Theorem

**Module 3: Public Key Cryptography and its Applications [10 Sessions] [Comprehension]**

Overview of Public Key Cryptography, RSA, Diffie - Helman Key exchange, Man in the middle attack, Cryptographic Hash functions, Secure Hash Algorithm, Message Authentication Codes – HMAC, Digital Signature, Discussion on real time practices of Cryptography

**Module 4: Network Security [7 Sessions] [Comprehension]**

Network Security fundamentals, Network Security applications: Authentication: Kerberos, PKI, Network Security applications: e-mail security: PGP, MIME, Network Security applications: IP Security: IP Sec architecture, Network Security applications: Web Security.

**DELIVERY PROCEDURE (PEDAGOGY):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 3: SPECIAL DELIVERY METHOD/ PEDAGOGY PLANNED WITH TOPICS** | | | | |
| **S. No** | **Lecture Number** | **Subtopic as per lesson Plan** | **Pedagogy title/ short explanation of adopted pedagogy** | **\*\* At end of semester please update whether activity was done** |
| **1** | **L22** | **Man in Middle Attack** | **Self learning** |  |
| **2** | **L34** | **Network Security Applications** | **Self learning** |  |
| **3** | **L6** | **Playfair Cipher** | **Participative learning** |  |
| **4** | **L7** | **Hill Cipher** | **Participative learning** |  |
| **5** |  | **Student Seminar** | **Technology based Learning** |  |

**REFERENCE MATERIALS:**

**Text Books:**

T1. William Stallings, *"Cryptography and Network Security - Principles and Practices"*, Prentice

Hall, 8th Edition, 2019

T2. Wade Trappe and Lawrence C Washington, *“Introduction to Cryptography with Coding*

*Theory”*, Pearson, 2020

**Reference Books:**

R1. Behrouz A Forouzan, Debdeep Mukhopadhyay, “*Cryptography and Network Security*”, McGraw Hill, third edition, 2010

R2. R.Rajaram, “*Network Security and Cryptography*” SciTech Publication.3rd Edition, 2014

R3. AtulKahate, "*Cryptography and Network Security*", Tata McGraw-Hill, 2nd Edition, 2019

R4. BruceSchneier, “*Applied Cryptography*", John Wiley and Sons Inc. Second Edition, 2015.

**Online Resources:**

1. <https://onlinecourses.nptel.ac.in/noc22_cs90/preview>

(Cryptography and network Security)

1. e-pgpathshala UGC lecture series : E-Series and Self learning Materials.

<https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=fBYckQKJvP3a/8Vd3L08tQ>==

Web Resources:-

1. <http://182.72.188.195/cgi-bin/koha/opac-detail.pl?biblionumber=10133&query_desc=kw%2Cwrdl%3A%20Cryptography%20and%20Network%20Security>
2. <http://182.72.188.195/cgi-bin/koha/opac-detail.pl?biblionumber=5875&query_desc=kw%2Cwrdl%3A%20Cryptography%20and%20Network%20Security>
3. <https://presiuniv.knimbus.com/user#/home?loggedInUsing=msteams>

**GUIDELINES TO STUDENTS:**

Students are required to strictly adhere to assignment deadlines.

1. Students are required to actively participate in classroom discussions and other activities which is planned in and out of the classroom.
2. Make-up will be granted for genuine reasons, only when prior-permission is obtained from Instructor-in-charge and approving the permission is at the discretion of Instructor- in-charge
3. All course related information and notices will be uploaded in CAMU and also communicated during class hours through Microsoft –TEAM.
4. NPTEL or any MOOC course will be encouraged

**COURSE SCHEDULE:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 4: COURSE BROAD SCHEDULE** | | | | |
| **Sl. No.** | **ACTIVITY** | **PLANNED STARTING DATE** | **PLANNED CONCLUDING DATE** | **TOTAL NUMBER OF PERIODS** |
| **01** | Overview of the course | 09-02-2023 | 09-02-2023 | 1 |
| **02** | Module : 01 | 10-02-2023 | 27-02-2023 | 8 |
| **03** | Assignment | 25-02-2023 | 26-02-2023 | - |
| **04** | Module: 02 | 28-02-2023 | 27-03-2023 | 13 |
| **05** | Quiz | 25-03-2023 | 25-03-2023 | - |
| **06** | Mid-term Exam | As per COE schedule | As per COE schedule | 1.5 hrs |
| **07** | Module: 03 | 28-03-2023 | 17-04-2023 | 9 |
| **08** | Module: 04 | 17-04-2023 | 03-05-2023 | 7 |
| **09** | Group Seminar | 04-05-2023 | 06-05-2023 | 2 |
| **10** | Revision and Conclusion of the Course |  |  | 4 |
| **11** | End term Exam | As per COE schedule | As per COE schedule | 3 hrs |

**DETAILED SCHEDULE OF INSTRUCTION:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 5: DETAILED COURSE SCHEDULE/ LESSON PLAN** | | | | |
| **Session no** | **TOPIC** | **SUBTOPIC** | **CO Number** | **Reference** |
| **1** | Introduction | Introduction to Cryptography |  | **T1 1.1** |
| **2** | Security Architecture, | **CO1** | T1 1.2, T2 |
| **3** | Model of Network Security | **CO1** | T1 1.3, T2 |
| **4** | Security attacks and services | Active and passive attacks, Authentication, confidentiality, access control, integrity and non-repudiation | **CO1** | T1 1.3, T2 |
| **5** | Classical Encryption Techniques | Caesar, Monoalphabetic, Polyalphabetic Ciphers | **CO1** | T1 2.1, T2 |
| **6** | Playfair Cipher | **CO1** | T2 3.2 |
| **7** | Hill Cipher | **CO1** | T2 3.2 |
| **8** | Block and Stream Ciphers | Definition and Feistel Structure | **CO1** | T1 3.1, T2 |
| Module 1 Completed | | | | |
| **9** | Symmetric Key Cryptography | Introduction, Data Encryption Standard (DES) | **CO2** | T1 3.2 ,T2,R1 |
| **10** | DES (Contd...) | **CO2** | T1 3.2 ,T2,R1 |
| **11** | Introduction to Galois Field | **CO2** | T1 4.7,T2,R1 |
| **12** | Advanced Encryption Standard (AES) | **CO2** | T1 5.1 ,T2,R1 |
| **13** | AES (Contd...) | **CO2** | T1,T2,R1 |
| **14** | Introduction to Number Theory | Congruence and Divisibility | **CO2** | T1 4.1, T2,R1 |
| **15** | Prime Numbers, Fermat’s little theorem | **CO2** | T1 8.1,T2,R1 |
| **16** | Euler totient function, Euclidean Algorithm | **CO2** | T1 4.2, R1,R3 |
| **17** | Extended Euclidean Algorithm | **CO2** | T1 4.2,R1,R3 |
| **18** | Chinese Remainder Theorem | **CO2** | T1 8.4, R1,R3 |
| Module 2 Completed | | | | |
| **19** | Introduction to Public Key Cryptography (PKC) | Introduction, RSA algorithm | **CO3** | T1 9.2, T2,R1,R3 |
| **20** | RSA (Contd...) | **CO3** | T1,T2,R1,R3 |
| **21** | Diffie-Hellman key exchange | **CO3** | T1 10.1, T2,R1,R3 |
| **22** | Man in Middle Attack | Man in Middle Attack | **CO3** | T1,T2,R1,R3 |
| **23** | Applications of PKC | Hash function, Properties, MD5 | **CO3** | T1,T2,R1,R3 |
| **24** | SHA 256 | **CO3** | T1 11.5, T2,R1,R3 |
| **25** | Introduction to Digital Signature | **CO3** | T1 13.1, T2,R1,R3 |
| **26** | Digital Signature Algorithm | **CO3** | T1 13.2, T2,R1,R3 |
| **27** | Message Authentication Codes (MAC) | **CO3** | T1 12.1, T2,R1,R3 |
| **28** | MAC (Contd...) | **CO3** | T1,T2,R1,R3 |
| **29** | Some discussion on real world applications of Cryptography | Applications like whatsapp, banking and other secure applications | **CO3** | T1,T2,R1,R3 |
| Module 3 Completed | | | | |
| **31** | Network Security | Fundamentals, | **CO4** | T1 16.1, R1,R3,R4 |
| **32** | Authentication : Kerberos | **CO4** | T1 15.3, R1,R3,R4 |
| **33** | e-mail security : PGP and MIME | **CO4** | T1 18.1. 18.2, R1,R3,R4 |
| **34** | IP Security : IPSec architecture | **CO4** | T1 19.1, R1,R3,R4 |
| **35** | Web Security | **CO4** | T1 16.1 ,R1,R3,R4 |
| **36** | Seminar | Group Seminar | **CO4** | T1,R1,R3,R4 |
| **37** | Group Seminar (Contd) | **CO4** | T1,R1,R3,R4 |
| **38** | Revision | | | |
| Module 4 Completed | | | | |

**ASSESSMENT SCHEDULE:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **TABLE 6 ASSESSMENT SCHEDULE** | | | | | | | |
| **Sl.no** | **Assessment type** | **Contents** | **Course outcome**  **Number** | **Duration**  **In Hours** | **marks** | **Weightage** | **Venue, DATE &TIME** |
| **1** | Assignment | Module1 | CO1 | 60 mins | 15 | 7.5% | <https://www.camu.in/index#/scheduleAssessment>  25-02-2023-26-02-2023 |
| **2** | Mid Term Exam | Module1, Module2 | CO1,CO2 | 90 mins | 50 | 25% | As per COE schedule |
| **3** | Quiz | Module2 | CO2 | 20 mins | 20 | 10% | <https://www.camu.in/index#/scheduleAssessment>  25-03-2023 |
| **4** | Seminar | Module 3, Module 4 | CO3, CO4 | 30 mins | 15 | 7.5% | Respective Classrooms |
| **6** | End Term Exam | Full Syllabus | CO1,CO2, CO3,C04, CO5 | 3 Hrs. | 100 | 50% | As per COE schedule |

**COURSE CLEARANCE CRITERIA:**

**AS PER ACADEMIC REGULATIONS OF THE UNIVERSITY**

[**https://presidencyuniversity.in/academic-regulations/**](https://presidencyuniversity.in/academic-regulations/)

**MAKEUP EXAM POLICY:**

**AS PER ACADEMIC REGULATIONS OF THE UNIVERSITY**

[**https://presidencyuniversity.in/academic-regulations/**](https://presidencyuniversity.in/academic-regulations/)

**CONTACT TIMINGS IN THE CHAMBER FOR ANY DISCUSSIONS:**

Students are encouraged to come for any discussions on this course during your Library, CCH Period, Saturdays 2 to 4 PM.

SAMPLE THOUGHT PROVOKING QUESTIONS:

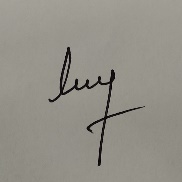
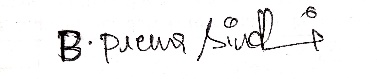
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 7: SAMPLE THOUGHT PROVOKING QUESTIONS** | | | | |
| **SL NO** | **QUESTION** | **MARKS** | **COURSE OUTCOME NO.** | **BLOOM’S LEVEL** |
| 1. | How the information security will be ensured by applying any one of cryptography technique? Brief. | 5 marks | CO 1 | L1 |
| 2. | Is it the Transposition Technique is securable if the information will be send through the networked communication? If.Yes. Explain with Example. | 5 Marks | CO1 | L2 |
| 3. | Write about the Complexity of AES Symmetric Key Encryption Techniques and test it for any of an information security system? | 10 marks | CO2 | L3 |
| 4. | How RSA is Securable and Analyse the Importance of Public key Crypto systems using Public key Cryptography:- | 10 marks | CO2 | L3 |
| 5. | Justify How SHA-512 is Most Secure | 7 marks | CO3 | L3 |
| 6. | Write an Importance of PGP in Email Security | 5marks | CO4 | L2 |

**TARGET SET FOR COURSE OUTCOME ATTAINMENT:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TABLE 8: TARGET SET FOR ATTAINMENT OF EACH CO and ATTAINMENT ANALYSIS AFTER RESULTS** | | | | | | |
| **Sl.no** | **C.O. No.** | **Course Outcomes** | **Threshold Set for the CO** | **Target set for attainment in percentage** | Actual C.O. Attainment  In Percentage  \* | Remarks on attainment &Measures to enhance the attainment  \* |
| 01 | CO1 | Describe the basic concept of Cryptography | 60% | 65% |  |  |
| 02 | CO2 | Apply the concepts of cryptographic algorithms | 55% | 60% |  |  |
| 03 | CO3 | Describe the Public key Cryptographic Techniques for various applications. | 55% | 60% |  |  |
| 04 | CO4 | Explain the network security concepts during their implementation of different applications | 55% | 60% |  |  |

**\* LAST TWO COLUMNS ARE TO BE FILLED AFTER END TERM EXAM WITH ACTUAL ATTAINMENT VALUES**

Signature of the course Instructor In-Charge (s)

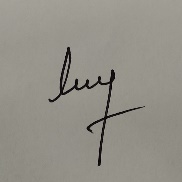
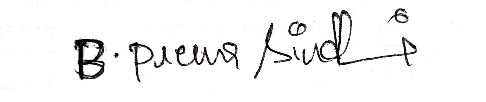


APPROVAL:

This course has been duly verified Approved by the D.A.C.

Signature of the Chairperson D.A.C.

Name and signature of the Instructor In-Charge (s): Ms.B Prema Sindhuri & Mr. Gnana Kumar G



Name and signature of the DAC Chairperson:

**BLOOM'S TAXONOMY SAMPLE VERBS**

Learning Outcomes Verbs at Each Bloom Taxonomy Level to be used for writing the course Outcomes.

|  |  |  |
| --- | --- | --- |
| **TABLE 9: REFERENCE SAMPLES OF BLOOMS TAXONOMY VERBS** | | |
| Cognitive Level | Illustrative Verbs | Definitions |
| Knowledge | arrange, define, describe, duplicate, identify, label, list, match, memorize, name, order, outline, recognize, relate, recall, repeat, reproduce, select, state | remembering previously learned information |
| Comprehension | classify, convert, defend, discuss, distinguish, estimate, explain, express, extend, generalize, give example(s), identify, indicate, infer, locate, paraphrase, predict, recognize, rewrite, report, restate, review, select, summarize, translate | grasping the meaning of information |
| Application | apply, change, choose, compute, demonstrate, discover, dramatize, employ, illustrate, interpret, manipulate, modify, operate, practice, predict, prepare, produce, relate schedule, show, sketch, solve, use write | applying knowledge to actual situations |
| Analysis | analyze, appraise, breakdown, calculate, categorize, classify, compare, contrast, criticize, derive, diagram, differentiate, discriminate, distinguish, examine, experiment, identify, illustrate, infer, interpret, model, outline, point out, question, relate, select, separate, subdivide, test | breaking down objects or ideas into simpler parts and seeing how the parts relate and are organized |
| Synthesis | arrange, assemble, categorize, collect, combine, comply, compose, construct, create, design, develop, devise, explain, formulate, generate, plan, prepare, propose, rearrange, reconstruct, relate, reorganize, revise, rewrite, set up, summarize, synthesize, tell, write | rearranging component ideas into a new whole |
| Evaluation | appraise, argue, assess, attach, choose, compare, conclude, contrast, defend, describe, discriminate, estimate, evaluate, explain, judge, justify, interpret, relate, predict, rate, select, summarize, support, value | making judgments based on internal evidence or external criteria |