# MAHATMA GANDHI UNIVERSITY

**Kottayam, Kerala**

**Undergraduate Programmes (HONOURS)**
**2025 Admission Onwards**

| SYLLABUS | | | |
|---|---|---|---|
| **SIGNATURE COURSE** | | | |
| **Name of the College** | Bishop Abraham Memorial College, Thuruthicaud | | |
| **Faculty/ Discipline** | Mathematics | | |
| **Programme** | BSc (Hons) Mathematics | | |
| **Course Coordinator** | Tijy Mathew | | |
| **Contributors** | Megha Rose Manoj | | |
| **Course Name** | Mathematical Foundations of Data Science and Cryptography | | |
| **Type of Course** | DSE | | |
| **Specialization title** | Data Science and Cryptography | | |
| **Course Code** | MG3DSEMATA12 | | |
| **Course Level** | 200 | | |
| **Course Summary** | To introduce students to the mathematical foundations required for data science and cryptography, including linear algebra, probability, and number theory. | | |
| **Semester** | 3 | **Credits** | 4 |

**Course Details**

| Learning Approach | Lecture | Total Hours |
|---|---|---|
| Credits | 4 | 60 |

| **Pre-requisites, if any** | |
|---|---|

**Course Outcomes (CO)**

| **Number of COs** | | **4** | |
|---|---|---|---|
| **CO No.** | **Expected Course Outcome** | **Learning Domains *** | **PO No** |
| 1 | Understand the foundations of linear algebra. | U | PO1, PO2, PO4, PO10 |
| 2 | Understand the basic concepts of statistics. | U | PO1, PO2, PO3, PO10 |
| 3 | Understand number theoretic foundations of cryptography. | U | PO1, PO2 |
| 4 | Understand and apply the classical encryption techniques. | A | PO1, PO2 |

**Remember (K), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C), Skill (S), Interest (I) and Appreciation (Ap)*

**CO-PO Articulation Matrix**

| CO/PO | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| CO 1 | 1 | 2 | - | 3 | - | - | - | - | - | 3 |
| CO 2 | 2 | 3 | 2 | - | - | - | - | - | - | 3 |

| CO/PO | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| CO 3 | 3 | 2 | - | - | - | - | - | - | - | - |
| CO 4 | 2 | 2 | - | - | - | - | - | - | - | - |

*'0' is No Correlation, '1' is Slight Correlation (Low level), '2' is Moderate Correlation (Medium level) and '3' is Substantial Correlation (High level).*

**Course Content**

Content for Classroom transaction (Units)

| Module | Units | Course Description | Hrs | CO No. |
|---|---|---|---|---|
| 1 | Linear Algebra for Data Science | | | |
| | 1.1 | Vectors and matrices: Vectors, Vector operations, Matrices and matrix operations, Representation of data using vectors and matrices. | 4 | ["1"] |
| | 1.2 | Vector Spaces: Vector spaces, Subspaces, Linear independence, Basis and dimensions (concept only). | 6 | ["1"] |
| | 1.3 | Eigen values, Eigen vectors. | 5 | ["1"] |
| 2 | Probability for Data Science | | | |
| | 2.1 | Probability: Basic definitions, Probability, Bayesian v/s frequentist, Frequentist approach, The law of large numbers. | 3 | ["2"] |
| | 2.2 | Conditional probability: Compound events, Conditional probability, Addition rule, Mutual exclusively, Multiplication rule, Independence, Complementary events. | 4 | ["2"] |
| | 2.3 | Bayes' theorem: Bayesian ideas revisited, Bayes' theorem, More applications of Bayes' theorem. | 4 | ["2"] |
| | 2.4 | Random variables: Discrete random variables, Continuous random variables. | 4 | ["2"] |
| 3 | Number Theory for Cryptography | | | |
| | 3.1 | Divisibility and division algorithm: Divisibility, Division algorithm, Euclidean algorithm. | 5 | ["3"] |
| | 3.2 | Modular arithmetic, Prime numbers. | 5 | ["3"] |
| | 3.3 | Fermat's and Euler's theorem: Fermat's theorem (without proof), Euler's totient function, Euler theorem (without proof). | 5 | ["3"] |
| 4 | Introduction to Cryptography and Classical Encryption Techniques | | | |
| | 4.1 | Symmetric cipher model: Basic terminology, Cryptography, Symmetric cryptosystem, Cryptanalysis and brute force attack. | 5 | ["4"] |
| | 4.2 | Substitution techniques: Caesar cipher, Mono alphabetic ciphers, Playfair cipher, Hill cipher. | 5 | ["4"] |
| | 4.3 | Poly alphabetic ciphers and Transposition techniques: Poly alphabetic ciphers-Vigenere ciphers and Vernam ciphers, One-time pad, Transposition techniques. | 5 | ["4"] |

| Teaching and Learning Approach | **Classroom Procedure (Mode of transaction)**<br>Lecture, Interactive instructions, Assignment, Library work, Seminar. |
|---|---|

| | |
|---|---|
| **Assessment Types** | **MODE OF ASSESSMENT**<br>Mode of Assessment: Theory<br><br>**A. Continuous Comprehensive Assessment (CCA)**<br>**• Theory – 30 Marks**<br>Test Paper, Viva, Seminar, Assignment, Quiz<br><br>**B. End Semester Evaluation (ESE)**<br>**• Theory – 70 Marks**<br>Assessment Methods – examination<br>Duration of Examination – 2.00 Hrs<br>Pattern of examination for Theory – Non-MCQ<br>Different parts of written examination – Part - A , B , C<br>Answer Type:<br>◦ PART - A<br>◦ Short answer - (5 out of 8 ) – 5 × 2 = 10<br>◦ PART - B<br>◦ Short Essays - (5 out of 8 ) – 5 × 6 = 30<br>◦ PART - C<br>◦ Essays - (3 out of 6 ) – 3 × 10 = 30 |

## References


- Gilbert Strang, Introduction to Linear Algebra (5th Edition), Cambridge Press, 2016. (Chapter 1: Sections- 1.1-1.3, Chapter 2: Section- 2.1, Chapter 3: Sections- 3.1, 3.4, Chapter 6: Section- 6.1).
- Sinan Ozdemir, Principles of Data Science (3rd Edition), Packt Publishing, 2024. (Relevant sections from Chapter 5 and 6).
- William Stallings, Cryptography and Network security: Principles and Practices (5th Edition), Prentice Hall, 2011. (Chapter 2: Sections- 2.1-2.3, Chapter 4: Sections- 4.1-4.3, Chapter 8: Sections-8.1, 8.2).
- Behrouz A. Forouzan, Data Communications and Networking (4th edition), Mc Graw Hill, 2007(Chapter 30: Sections-30.1, 30.2(relevant parts)).


## Suggested Readings


- Gilbert Strang, Linear Algebra and its applications (4th Edition), Cengage Learning, 2005.
- S. C. Gupta, V.K. Kapoor, Fundamentals of Mathematical Statistics (10th Revised Edition), Sultan Chand & Sons, 2000.
- David M. Burton, Elementary Number Theory (7th Edition), Mc Graw Hill, 2010.




## Affidavit

- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, retain the copyright of this syllabus and expressly prohibit its distribution in complete form to any institution outside our own.
- We, Bishop Abraham Memorial College, Thuruthicaud, agree to appoint a new course coordinator for the proposed Data Science and Cryptography in the event of the unavailability of the currently nominated coordinator. This appointment will ensure the continued coordination of course delivery, assessments, and all related academic responsibilities necessary for the successful implementation of the specialization, for as long as the college offers this programme.
- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, declare that no part of this signature course submitted here for approval has been taken from the course content developed by, or from any of the course titles prepared by, the BoS/expert committee in the same discipline under our University.

# MAHATMA GANDHI UNIVERSITY

**Kottayam, Kerala**

**Undergraduate Programmes (HONOURS)**
**2025 Admission Onwards**

| SYLLABUS | | | |
|---|---|---|---|
| **SIGNATURE COURSE** | | | |
| **Name of the College** | Bishop Abraham Memorial College, Thuruthicaud | | |
| **Faculty/ Discipline** | Mathematics | | |
| **Programme** | BSc (Hons) Mathematics | | |
| **Course Coordinator** | Tijy Mathew | | |
| **Contributors** | Megha Rose Manoj | | |
| **Course Name** | Introduction to Data Science and Cryptography | | |
| **Type of Course** | DSE | | |
| **Specialization title** | Data Science and Cryptography | | |
| **Course Code** | MG4DSEMATA12 | | |
| **Course Level** | 200 | | |
| **Course Summary** | This course provides an introductory overview of data science and the principles of modern symmetric ciphers. | | |
| **Semester** | 4 | **Credits** | 4 |

**Course Details**

| Learning Approach | Lecture | Total Hours |
|---|---|---|
| Credits | 4 | 60 |

| **Pre-requisites, if any** | |
|---|---|

**Course Outcomes (CO)**

| Number of COs | | 4 | |
|---|---|---|---|
| **CO No.** | **Expected Course Outcome** | **Learning Domains *** | **PO No** |
| 1 | Understand the basic terminologies in data science and data types. | U | PO2, PO3, PO9, PO10 |
| 2 | Understand the basic concepts of data analysis. and visualization. | U, I | PO1, PO2 |
| 3 | Understand the most widely used symmetric cipher: the Data Encryption Standard (DES) and the general principles of symmetric block ciphers for secure communication. | U | PO1, PO2, PO3, PO10 |
| 4 | Explain the block cipher Advanced Encryption Standard (AES). | U, I | PO2, PO3, PO9 |

**Remember (K), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C), Skill (S), Interest (I) and Appreciation (Ap)*

**CO-PO Articulation Matrix**

| CO/PO | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| CO 1 | - | 2 | 2 | - | - | - | - | - | 2 | 1 |
| CO 2 | 2 | 3 | - | - | - | - | - | - | - | - |
| CO 3 | 3 | 3 | 2 | - | - | - | - | - | - | 2 |
| CO 4 | - | 2 | 2 | - | - | - | - | - | 2 | - |

*'0' is No Correlation, '1' is Slight Correlation (Low level), '2' is Moderate Correlation (Medium level) and '3' is Substantial Correlation (High level).*

**Course Content**

Content for Classroom transaction (Units)

| Module | Units | Course Description | Hrs | CO No. |
|---|---|---|---|---|
| 1 | Introduction to Data Science | | | |
| | 1.1 | Data science terminologies: What is data science? Basic data science terminologies; Why data science? Examples and case studies; Some more technologies. | 5 | ["1"] |
| | 1.2 | Types of data: Structured v/s unstructured data; Quantitative v/s qualitative data; Discrete v/s continuous data; The 4 levels of data- nominal level, ordinal level, Interval level and ratio level. | 5 | ["1"] |
| | 1.3 | Steps of Data Science: Overview of the 5 steps; Exploring the data; Guiding questions for data exploration; Data frames; Series. | 5 | ["1"] |
| 2 | Data Collection, Analysis and visualization | | | |
| | 2.1 | Data collection: Obtaining data -Observational and experimental sampling data. | 5 | ["2"] |
| | 2.2 | Data analysis: Measure of center; Measure of variation; Correlations in data; The empirical rule; Point estimate, Sampling distribution; Confidence interval; Hypothesis test- t-test, Chi-square test; Type I and Type II errors. | 5 | ["2"] |
| | 2.3 | Data visualization: Communicating data; Effective visualizations- Scatter plots, Line graphs, bar charts, histograms and box plots; Correlation v/s causation; Simpson's paradox; Verbal communication. | 5 | ["2"] |
| 3 | Block ciphers and Data Encryption Standard (DES) | | | |
| | 3.1 | Block cipher principles: Stream ciphers and block ciphers, Feistel cipher (concept only). | 5 | ["3"] |
| | 3.2 | The Data Encryption Standard (DES); The strength of DES. | 5 | ["3"] |
| | 3.3 | Block cipher design principles. | 5 | ["3"] |
| 4 | Advanced Encryption Standard (AES) | | | |
| | 4.1 | The origin of Advanced Encryption Standard (AES). | 5 | ["4"] |
| | 4.2 | AES Structure. | 5 | ["4"] |
| | 4.3 | Block cipher modes of operation. | 5 | ["4"] |

| Teaching and Learning Approach | Classroom Procedure (Mode of transaction)<br>Lecture, Interactive instructions, Assignment, Library Work, Seminar |
|---|---|

| | |
|---|---|
| **Assessment Types** | **MODE OF ASSESSMENT**<br>Mode of Assessment: Theory<br><br>**A. Continuous Comprehensive Assessment (CCA)**<br>**• Theory – 30 Marks**<br>Test Paper, Viva, Seminar, Assignment, Quiz, problem solving method<br><br>**B. End Semester Evaluation (ESE)**<br>**• Theory – 70 Marks**<br>Assessment Methods – examination<br>Duration of Examination – 2.00 Hrs<br>Pattern of examination for Theory – Non-MCQ<br>Different parts of written examination – Part - A , B , C<br>Answer Type:<br>∘ PART - A<br>∘ Short answer - (5 out of 8 ) – 5 × 2 = 10<br>∘ PART - B<br>∘ Short Essays - (5 out of 8 ) – 5 × 6 = 30<br>∘ PART - C<br>∘ Essays - (3 out of 6 ) – 3 × 10 = 30 |

## References


- Sinan Ozdemir: Principles of Data Science (3rd Edition), Packt Publishing, 2024 (Relevant sections from chapters 1,2 ,3 7, 8 and 9).
- William Stalings, Cryptography and Network Security, Principles and Practices (5th Edition), Prentice Hall, 2011(Chapter 3: Sections- 3.1, 3.2, 3.4, 3.6, Chapter 5: Sections- 5.1, 5.2, Chapter 6: Section- 6.2 (Table 6.1).
- Behrouz A. Forouzan, Data Communications and Networking (4th edition), Mc Graw Hill, 2007(Chapter 30: Section-30.2(relevant parts)).


## Suggested Readings


- Atul Kahate, Cryptography and Network Security (3rd Edition), Mc Graw Hill, 2013.
- Joel Grus, Data Science from Scratch: First Principles with Python, O'Reilly, 2015.


## Affidavit

- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, retain the copyright of this syllabus and expressly prohibit its distribution in complete form to any institution outside our own.
- We, Bishop Abraham Memorial College, Thuruthicaud, agree to appoint a new course coordinator for the proposed Data Science and Cryptography in the event of the unavailability of the currently nominated coordinator. This appointment will ensure the continued coordination of course delivery, assessments, and all related academic responsibilities necessary for the successful implementation of the specialization, for as long as the college offers this programme.
- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, declare that no part of this signature course submitted here for approval has been taken from the course content developed by, or from any of the course titles prepared by, the BoS/expert committee in the same discipline under our University.

# MAHATMA GANDHI UNIVERSITY
**Kottayam, Kerala**

**Undergraduate Programmes (HONOURS)**
**2025 Admission Onwards**

| SYLLABUS | | | |
|---|---|---|---|
| **SIGNATURE COURSE** | | | |
| **Name of the College** | Bishop Abraham Memorial College, Thuruthicaud | | |
| **Faculty/ Discipline** | Mathematics | | |
| **Programme** | BSc (Hons) Mathematics | | |
| **Course Coordinator** | Tijy Mathew | | |
| **Contributors** | Megha Rose Manoj | | |
| **Course Name** | Introduction to Python Programming and Modern Cryptography | | |
| **Type of Course** | DSE | | |
| **Specialization title** | Data Science and Cryptography | | |
| **Course Code** | MG5DSEMATA12 | | |
| **Course Level** | 300 | | |
| **Course Summary** | To introduce Python programming and modern cryptographic systems with mathematical foundations. | | |
| **Semester** | 5 | **Credits** | 4 |
| **Course Details** | **Learning Approach** / **Lecture** / **Total Hours**<br>Credits / 4 / 60 | | |
| **Pre-requisites, if any** | | | |

**Course Outcomes (CO)**

| **Number of COs** | | **4** | |
|---|---|---|---|
| **CO No.** | **Expected Course Outcome** | **Learning Domains *** | **PO No** |
| 1 | Understand the basics of Python and to write basic Python programs. | A | PO1, PO2, PO3, PO4, PO10 |
| 2 | Handling and analyzing data using NumPy. | An | PO1, PO2, PO3, PO4 |
| 3 | Understanding the fundamentals of data analysis using pandas. | U | PO1, PO2, PO3, PO4 |
| 4 | Understand the fundamental concepts of public key cryptography, encryption, and key exchange mechanisms. | U | PO1, PO2 |

**Remember (K), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C), Skill (S), Interest (I) and Appreciation (Ap)*

**CO-PO Articulation Matrix**

| CO/PO | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| CO 1 | 1 | 2 | 3 | 2 | - | - | - | - | - | 3 |

| CO/PO | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| CO 2 | 2 | 2 | 3 | 3 | - | - | - | - | - | - |
| CO 3 | 1 | 2 | 3 | 3 | - | - | - | - | - | - |
| CO 4 | 2 | 2 | - | - | - | - | - | - | - | - |

*'0' is No Correlation, '1' is Slight Correlation (Low level), '2' is Moderate Correlation (Medium level) and '3' is Substantial Correlation (High level).*

**Course Content**

Content for Classroom transaction (Units)

| Module | Units | Course Description | Hrs | CO No. |
|---|---|---|---|---|
| 1 | Python Programming fundamentals | | | |
| | 1.1 | Basics: Language Semantics; Scalar Types; Control flow. | 3 | ["1"] |
| | 1.2 | Data structures and sequences: Tuples; List; Dictionary; Set; Built-in sequence functions; List, set and dictionary comprehensions. | 4 | ["1"] |
| | 1.3 | Functions: Namespaces, scope, and local functions; Returning multiple values; Functions are objects; Anonymous functions; Generators; Errors and exception handling. | 4 | ["1"] |
| | 1.4 | Files and operating system: Bytes and Unicode with files. | 4 | ["1"] |
| 2 | Data Handling using NumPy | | | |
| | 2.1 | The NumPy ndarray: Creating ndarrays; Data types for ndarrays; Arithmetic with NumPy arrays; Basic indexing and slicing; Boolean indexing; Fancy indexing; Transposing arrays and swapping axes. | 7 | ["2"] |
| | 2.2 | Array oriented programming: Pseudorandom number generation; Fast element-wise array functions; Array-oriented programming with arrays; Expressing conditional logic as array operations; Mathematical and statistical methods; Methods for Boolean arrays; Sorting; Unique and other set logic; File input and output with arrays; Linear algebra. | 8 | ["2"] |
| 3 | Getting Started with pandas | | | |
| | 3.1 | Introduction to pandas data structures: Series; Data frame; Index objects. | 7 | ["3"] |
| | 3.2 | Essential functionality: Reindexing; Dropping entries from an axis; Indexing, selection, and filtering; Arithmetic and data alignment. | 8 | ["3"] |
| 4 | Public Key Cryptography | | | |
| | 4.1 | Principles of public key cryptosystems. | 5 | ["4"] |
| | 4.2 | RSA. | 5 | ["4"] |
| | 4.3 | Diffie-Hellman key exchange. | 5 | ["4"] |

| Teaching and Learning Approach | **Classroom Procedure (Mode of transaction)**<br>Lectures, Tutorials, Interactive instructions, ICT tools, Seminars, Hands on training. |
|---|---|

| | |
|---|---|
| **Assessment Types** | **MODE OF ASSESSMENT**<br>Mode of Assessment: Theory<br><br>**A. Continuous Comprehensive Assessment (CCA)**<br>**• Theory – 30 Marks**<br>Test Paper, Viva, Seminar, Practical assessment<br><br>**B. End Semester Evaluation (ESE)**<br>**• Theory – 70 Marks**<br>Assessment Methods – Examination<br>Duration of Examination – 2.00 Hrs<br>Pattern of examination for Theory – Non-MCQ<br>Different parts of written examination – Part - A , B , C<br>Answer Type:<br>◦ PART - A<br>◦ MCQ - (15 out of 18 ) – 15 × 2 = 30<br>◦ PART - B<br>◦ Short answer - (5 out of 8 ) – 5 × 6 = 30<br>◦ PART - C<br>◦ Short Essays - (1 out of 2 ) – 1 × 10 = 10 |

## References


- Wes McKinney, Python for Data Analysis: Data Wrangling with pandas, NumPy, and Jupyter (Third edition), O'Reilly Publications, 2022. (Chapter 2: Sections- 2.3, Chapter 3: Sections- 3.1-3.3, Chapter 4: Sections- 4.1-4.6, Chapter 5: Relevant parts from Sections-5.1 & 5.2).
- William Stallings, Cryptography and Network Security: Principles and Practice (Fifth edition), Prentice Hall, 2011. (Chapter 9: Relevant parts from Sections-9.1, 9.2, Chapter 10: Relevant parts fromSection-10.1).
- Behrouz A. Forouzan, Data Communications and Networking (4th Edition), Mc Graw Hill,2007 (Chapter 30: Section 30.3).


## Suggested Readings


- Ajith Kumar B P., Python for Education, Inter University Accelerator Center- New Delhi, 2010.
- Allen Downey, Think Python: How to Think Like a Computer Scientist, Green Tea Press, 2012.
- Behrouz A. Forouzan, Cryptography and Network Security, Mc Graw Hill Company, 2007.


## Affidavit

- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, retain the copyright of this syllabus and expressly prohibit its distribution in complete form to any institution outside our own.
- We, Bishop Abraham Memorial College, Thuruthicaud, agree to appoint a new course coordinator for the proposed Data Science and Cryptography in the event of the unavailability of the currently nominated coordinator. This appointment will ensure the continued coordination of course delivery, assessments, and all related academic responsibilities necessary for the successful implementation of the specialization, for as long as the college offers this programme.
- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, declare that no part of this signature course submitted here for approval has been taken from the course content developed by, or from any of the course titles prepared by, the BoS/expert committee in the same discipline under our University.

# MAHATMA GANDHI UNIVERSITY

**Kottayam, Kerala**

**Undergraduate Programmes (HONOURS)**
**2025 Admission Onwards**

| SYLLABUS | | | |
|---|---|---|---|
| **SIGNATURE COURSE** | | | |
| **Name of the College** | Bishop Abraham Memorial College, Thuruthicaud | | |
| **Faculty/ Discipline** | Mathematics | | |
| **Programme** | BSc (Hons) Mathematics | | |
| **Course Coordinator** | Tijy Mathew | | |
| **Contributors** | Megha Rose Manoj | | |
| **Course Name** | Secure Data Systems and Emerging Technologies | | |
| **Type of Course** | DSE | | |
| **Specialization title** | Data Science and Cryptography | | |
| **Course Code** | MG6DSEMATA12 | | |
| **Course Level** | 300 | | |
| **Course Summary** | To expose students to secure data handling, privacy concepts, and emerging technologies. | | |
| **Semester** | 6 | **Credits** | 4 |
| **Course Details** | **Learning Approach** / Credits: **Lecture** 4; **Total Hours** 60 | | |
| **Pre-requisites, if any** | | | |

**Course Outcomes (CO)**

| **Number of COs** | | **4** | |
|---|---|---|---|
| **CO No.** | **Expected Course Outcome** | **Learning Domains *** | **PO No** |
| 1 | Understand the fundamentals of data security | U | PO1, PO2, PO9 |
| 2 | Understand and analyze cryptographic hash functions, message authentication codes (MACs), and digital signatures to guarantee data integrity, source authentication, and non-repudiation in secure communication systems. | An | PO2, PO3 |
| 3 | Understand and apply secure key management and distribution architectures using both symmetric Key Distribution Centers and public-key infrastructures to ensure secure key generation, exchange, storage, and revocation. | A | PO2, PO3 |
| 4 | Understand the network and transport-layer security protocols (IPsec, SSL/TLS) and application-layer email security (PGP). | U | PO2 |

**Remember (K), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C), Skill (S), Interest (I) and Appreciation (Ap)*

**CO-PO Articulation Matrix**

| CO/PO | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 | PO 8 | PO 9 | PO 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| CO 1 | - | - | - | - | - | - | - | - | 1 | - |
| CO 2 | - | 2 | 2 | - | - | - | - | - | - | - |
| CO 3 | - | 2 | 2 | - | - | - | - | - | - | - |
| CO 4 | - | 2 | - | - | - | - | - | - | - | - |

*'0' is No Correlation, '1' is Slight Correlation (Low level), '2' is Moderate Correlation (Medium level) and '3' is Substantial Correlation (High level).*

**Course Content**

Content for Classroom transaction (Units)

| Module | Units | Course Description | Hrs | CO No. |
|---|---|---|---|---|
| 1 | Data Security Fundamentals | | | |
| | 1.1 | Computer Security Concepts: Definition of computer security; Examples; Confidentiality; Integrity; Availability; The challenges of computer security. | 4 | ["1"] |
| | 1.2 | Security Threats and Attacks: Active attacks; Passive attacks. | 4 | ["1"] |
| | 1.3 | Security Services: Authentication; Access control; Data confidentiality; Data integrity; Non-repudiation. | 4 | ["1"] |
| | 1.4 | Security Mechanism: Specific security mechanism; Pervasive security mechanism. | 4 | ["1"] |
| 2 | Cryptographic Data Integrity | | | |
| | 2.1 | Cryptographic Hash Functions; Applications; Security requirements. | 5 | ["2"] |
| | 2.2 | Message authentication-requirements; Message authentication functions; Message authentication code (concept only). | 5 | ["2"] |
| | 2.3 | Digital signatures. | 6 | ["2"] |
| 3 | Key Management and Distribution | | | |
| | 3.1 | Symmetric key distribution. | 6 | ["3"] |
| | 3.2 | Public key distribution. | 7 | ["3"] |
| 4 | Security on the Internet | | | |
| | 4.1 | IP security. | 4 | ["4"] |
| | 4.2 | Secure sockets layer (SSL) | 3 | ["4"] |
| | 4.3 | Transport layer security | 4 | ["4"] |
| | 4.4 | Pretty good privacy (PGP) | 4 | ["4"] |

| Teaching and Learning Approach | **Classroom Procedure (Mode of transaction)**<br>Lectures, Interactive Sessions, Assignments, Seminars. |
|---|---|

| | |
|---|---|
| **Assessment Types** | **MODE OF ASSESSMENT**<br>Mode of Assessment: Theory<br><br>**A. Continuous Comprehensive Assessment (CCA)**<br>**• Theory – 30 Marks**<br>Test Paper, Viva, Seminar, Assignment, Quiz<br><br>**B. End Semester Evaluation (ESE)**<br>**• Theory – 70 Marks**<br>Assessment Methods – examination<br>Duration of Examination – 2.00 Hrs<br>Pattern of examination for Theory – Non-MCQ<br>Different parts of written examination – Part - A , B , C<br>Answer Type:<br>◦ PART - A<br>◦ MCQ - (15 out of 18 ) – 15 × 2 = 30<br>◦ PART - B<br>◦ Short answer - (5 out of 8 ) – 5 × 6 = 30<br>◦ PART - C<br>◦ Short Essays - (1 out of 2 ) – 1 × 10 = 10 |

## References


- William Stalings, Cryptography and Network security, Principles and Practices (5th Edition), Prentice Hall, 2011 (Chapter 1: Sections- 1.1- 1.5 (relevant parts) Chapter 11: Sections- 11.1, 11.3 (Table 11.1 & 11.2), Chapter 12: Sections- 12.1, 12.2 (relevant parts)).
- Behrouz A Forouzan, Data Communications and Networking (4th edition), Mc Graw Hill, 2007 (Chapter 31: Sections- 31.4 (relevant parts), 31.5, 31.7, Chapter 32: Sections- 32.1, 32.2, 32.3)


## Suggested Readings


- Behrouz A. Forouzan, Cryptography and Network Security, Mc Graw Hill Company, 2007.
- Atul Kahate, Cryptography and Network Security (3rd Edition), Mc Graw Hill, 2013.


## Affidavit

- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, retain the copyright of this syllabus and expressly prohibit its distribution in complete form to any institution outside our own.
- We, Bishop Abraham Memorial College, Thuruthicaud, agree to appoint a new course coordinator for the proposed Data Science and Cryptography in the event of the unavailability of the currently nominated coordinator. This appointment will ensure the continued coordination of course delivery, assessments, and all related academic responsibilities necessary for the successful implementation of the specialization, for as long as the college offers this programme.
- We, Bishop Abraham Memorial College, Thuruthicaud and Tijy Mathew, declare that no part of this signature course submitted here for approval has been taken from the course content developed by, or from any of the course titles prepared by, the BoS/expert committee in the same discipline under our University.