DEPARTMENT OF MATHEMATICS

SYLLABUS
FOR
VALUE ADDED COURSE
(UG LEVEL)

CRYPTOGRAPHY

Course Co-ordinator
Mathematics
R.D. Women's University
Bhubaneswar

Controller of Examinations
R.D. Women's University
Bhubaneswar

RAMA DEVI WOMEN'S UNIVERSITY
Vidya Vihar, Bhubaneswar-751022

CRYPTOGRAPHY
Course Code- MATH-VAC-II-CG

COURSE OUTCOME:

At the end of the course, the students will be able to

CO1: Able to analyze basic cryptographic protocols even customize them for (uncomplicated) practical scenarios.

CO2: A solid understanding of the use of fundamental crypto primitives in security in computing, especially in networking.

CO3: classify the symmetric encryption techniques and illustrate various Public key cryptographic techniques.

CO4: Summarize the intrusion detection and its solutions to overcome the attacks and discuss authentication applications and Basic concepts of system level security.

UNIT-I

Cryptography: Classical cryptosystem and their vulnerability public key cryptography, RSA scheme.

UNIT-II

Primality testing and factoring, Primitive roots, ElGamal Cryptosystem, Quadratic congruences and applications.

UNIT-III

Discrete Logarithms, Algorithm for Discrete Logarithm Problem, Security of ElGamal System, Schnorr signature scheme, The ElGamal signature scheme, The digital signature algorithm, Provable secure signature schemes.

REFERENCES

1. Neal Koblitz : A course of Number Theory and Cryptography, Second Edition, Springer Verlag, New York, 1987.

2. Douglas R. Stinson: Cryptography: Theory and Practice (3rd Edn.), Chapman Hall/CRC, 2006.

DEPARTMENT OF MATHEMATICS

SYLLABUS
FOR
VALUE ADDED COURSE
(UG LEVEL)

TYPE SETTING IN LATEX

Course Co-ordinator
Mathematics
R.D. Women's University
Bhubaneswar

RAMA DEVI WOMEN'S UNIVERSITY
Vidya Vihar, Bhubaneswar-751022

Controller of Examinations
R.D. Women's University
Bhubaneswar

TYPE SETTING IN LATEX
Course Code- MATH-VAC-I-TSL

COURSE OUTCOME:

Students will be able to learn:

CO1: Typesetting of complex mathematical formulae using LaTeX and use tabular and array environments within LaTeX.

CO2: Use various methods to either create or import graphics into a LaTeX document.

CO3: Typesetting of journal articles, technical reports, thesis, books, and slide presentations.

CO4: Automatic generation of table of contents, bibliographies and indexes.

UNIT-I

Preparing an input file, sentences and paragraphs, the document class, sectioning, display material, running Latex, Changes the type style, producing mathematical symbols and mathematical formulae, arrays, delimiters, multiline formulae, putting one thing on other, spacing in math mode.

UNIT-II

Defining command and environments, Producing and including graphics in a Latex file, figures and other floating bodies, lining it up in columns, table of content, cross-reference, bibliography and citation, making index and glossary, slides, overlays and notes, letters.

UNIT-III

Design it yourself: document class, page style, title page, customizing the style, line and page breaking, numbering, length, spaces and boxes, formatting with boxes, centering and flushing, list making environments, changing font type size and special symbols. Picture, picture environments, picture objects, text, boxes, straight lines, arrow, stacks, circles, oval, framing, curve, grid, repeat patterns.

REFERENCES

1. Leslie Lamport, A Document Preparation System User's Guide and Reference Manual, Addison-Wesley Publishing Company. Reference Books Stefan Kottwitz, LaTeX Beginner's Guide, Packt Publishing, UK.

OTHER SOURCES FOR READING

1. Till Tantau, User Guide to the Beamer Class, http://latex-beamer.sourceforge.net.
2. Tobias Oetiker, The Not So Short Introduction to LATEX2E, https://tobi.oetiker.ch/lshort/lshort.pdf.