COURSE CODE	COURSE TITLE	L	T	P	C
1152CS309	APPLIED CRYPTOGRAPHY LAB	0	0	4	2

Course Category: Program Elective

A. **Preamble:**

This course describes the cryptography concepts and it will be implemented using gmp library. Also, this helps to support cryptographic algorithms like RSA, Elliptic Curve Cryptography and Diffie Hellman key exchange

B. Pre-requisites:

Sl. No	Course Code	Course Name
1	1152CS101	Cryptography and Network Security

C. Related Courses:

Sl. No	Course Code	Course Name
1	1152CS117	Information Security
2	1156CS601	Minor Project
3	1156CS701	Major Project

D. Course Educational Objectives:

Students undergoing this course are expected to

- Learn fundamentals of cryptography algorithms.
- Understand the GNU MP Language libraries and standards.
- Acquire background on Euclid theorems, Fermat theorems and cryptographic algorithms.

E. Course Outcomes:

Upon the successful completion of the course, students will be able to:

CO Nos	Course Outcomes	Level of learning domain (Based on revised Bloom's taxonomy)
CO1	Implement the cryptographic basic programs	S3
CO2	Implement the Euclid , Fermat and Extended Euclid Theorems	S3
CO3	Implement the RSA, Diffie Hellman key exchange and chat application	S3
CO4	Write the cryptographic protocols program in HLPSL language using AVISPA toolset.	S3

F. Correlation of COs with Program Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	**M**				**M**										
CO2	**M**				**H**								**L**	**M**	
CO3	**M**		**M**		**H**								**L**	**M**	
CO4	**M**		**M**		**H**										

H- High; M-Medium; L-Low

G. Course Contents

List of Experiments

SNO	Experiment Name
1.	Gmp: Basic Programs
2.	Euclid Algorithm
3.	Extended Euclid Algorithm
4.	Extended Euclid Algorithm with time
5.	Inverse using Extended Euclid Algorithm
6.	Fermat theorem
7.	RSA Algorithm
8.	Chat Application: (Client & Server)
9.	Avispa Basic Programs
10.	Diffie Hellman Key Exchange

H. Learning Resources:

i. Text Books:

1. Wade Trappe, Lawrence C Washington, " Introduction to Cryptography with coding theory", 2nd ed, Pearson, 2007.
2. William Stallings, "Cryptography and Network security Principles and Practices", Pearson/PHI, 4th ed, 2006.

ii. Reference Books:

1. W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education, Second Edition, 2007.

iii. Online Resources:

1. https://gmplib.org
2. www.avispa-project.org