Ambedkar University Delhi

Course Outline

Monsoon Semester (Jan-May 2018)

School:			Undergraduate Studies
Programme with title:			BA (Honours)
Semester to which offered:			VI semester
Course Title:			Number Theory and Cryptography
Credits:			4 Credits
Course Code (new):			SUS1MA515
Course Code (old):			M14 and M16 (iv)
Type of Course:	Elective	no	Cohort BA (H) Mathematics
	Elective	yes	Cohort BA (H) other than Mathematics

For SUS only (Mark an X for as many as appropriate):

1. Foundation (Compulsory)
2. Foundation (Elective)
3. Discipline (Compulsory) x
4. Discipline (Elective)
5. Elective

Course Coordinator and Team: Dr. Ramneek Khassa

Email of course coordinator: **ramneek@aud.ac.in**

Pre-requisites: Mathematics of the 12th level

Aim: The main objective of this course is to prepare students who either wish to pursue Mathematics as career or need to use it from application point of view. Cryptography and Crypto analysis is a field where even non-mathematicians who are familiar with Elementary Number

theory have flourished and this course will easily feed in their needs to familiarize them with rudiments of Cryptography.

BRIEF DESCRIPTION OF MODULES/ MAIN MODULES:

1. **Euclidean Algorithm and Applications**
2. **Linear Congruences**
3. **Factorization methods**
4. **Arithmetic Functions**
5. **Primitive Roots**
6. **Quadratic Reciprocity and Elementary Cryptosystems**
7. **Lab work using MATHEMATICA**

ASSESSMENT DETAILS WITH WEIGHTS:

1. Class test 10% (First week of February)
2. Lab Work assessments 15% (Throughout semester)
3. Mid semester 25% (as per AUD academic calendar)
4. End semester 35% (as per AUD academic calendar)
5. Group Presentations 15% (early April)

Reading List:

MAIN REFERENCES:

1. George E Andrews, *Number Theory*, Hindustan Publishing House, Indian Edition.
2. David M Burton, *Elementary Number Theory (6th Edition)*, Tata McGraw-Hill Edition, Indian reprint, 2007.
3. Neville Robins, *Beginning Number Theory (2nd Edition)*, Narosa Publishing House Pvt. Ltd., 2007.

ADDITIONAL REFERENCES:

Klima, Sigmon & Stitzinger, *Applications of Abstract Algebra with MAPLE* (*Kindle Edition*), CRC Press, 1999.

Niven, Zuckerman & Montgomery*, An introduction to the Theory of Numbers* (*5th Edition*), Wiley, 1991.