GANPAT UNIVERSITY									
FACULTY OF TECHNOLOGY									
Programme	Bachelor of Technology					Branch/Spec.	Computer Science & Engineering (BDA)		
Semester	VI					Version	1.0.0.0		
Effective from Academic Year			2017– 18			Effective for the batch Admitted in			June 2015
Subject code	**2CSE602**		Subject Name			**Information Security**			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	0	1	0	4	Theory	40	60	100
Hours	3	0	2	0	5	Practical	30	20	50

Pre-requisites:

Computer Network, Programming Language

Learning Outcome:

After learning the course the students should be able to

- Understand the principles and practices of cryptographic techniques.
- Understand a variety of generic security threats and vulnerabilities, and identify & analyse particular security problems for given application.
- Appreciate the application of security techniques and technologies in solving real-life security problems in practical systems.
- Apply appropriate security techniques to solve security problem.

Theory syllabus

Unit	Content	Hrs
1	**Introduction** Information Security understanding,Security goals, Security attacks, Security services, security mechanisms	**4**
2	**Cryptographic Mathematics** Modular arithmetic, linear congruence, Algebraic structure, checking of primeness, quadratic congruence	**3**
3	**Classical Ciphers** Symmetric cipher model, substitution ciphers, transposition ciphers, steganography	**4**
4	**Modern symmetric key ciphers** Modern block ciphers, modern stream ciphers, Data Encryption standard, advanced encryption standard, Electronic code book mode, CBC, cipher feedback mode, output feedback mode	**7**
5	**Public key cryptography** RSA, RSA proof, RSA attacks, Rabin cryptosystem, Key management: Diffie Hellman	**6**
6	**Message Authentication and Hash functions** Authentication requirements, functions, Message authentication codes (MAC), Hash functions, security of Hash functions	**4**
7	**Hash algorithms, Digital Signatures** SHA- 512, Basics, digital signature standards	**7**
8	**Network and System Security** Understanding of Worms, Virus, Trojan Horse, Malwares, IP and Network Security ,Web security Email Security, System Security, tools	**7**

9	**Case Studies (Self Study topics)** Cyber Security, Laws, Cyber security amendments, Block Chain ,Security compliances	**1**

Practical content

- Test various vulnerabilities using bWAPP.
- Implement SQL Injection and DOS Attack.
- Implement Caesar Cipher Encryption – Decryption
- Implement Monoalphabetic Cipher Encryption – Decryption
- Implement Playfiar Cipher Encryption – Decryption
- Implement transposition Cipher Encryption – Decryption
- Implement RSA Cipher Encryption – Decryption
- Implement Key Exchange Algorithm
- Implement Digital Signature Algorithm
- Demonstration of working of Block Chain
- Study SNORT Intrusion Detection System and list the operations available in it.
- Hands on Block chain

Text Books

1	William Stallings: “Cryptography and Network Security – Principles and Practice”, 4/E, Pearson Education, 2005.

Reference Books

1	Bruce Scheneir: “Applied Cryptography”, 2/E, John Wiley, 1996
2	Behrouz Forouzan: “Cryptography & Network Security”, 1/E, TMH, 2007.