

**INFORMATION AND NETWORK SECURITY**  
**[As per Choice Based Credit System (CBCS) scheme]**  
**(Effective from the academic year 2017 - 2018)**  
**SEMESTER – VII**

Subject Code	17CS743	IA Marks	40
Number of Lecture Hours/Week	3	Exam Marks	60
Total Number of Lecture Hours	40	Exam Hours	03

**CREDITS – 03**

<b>Module – 1</b>	<b>Teaching Hours</b>
-------------------	-----------------------

Introduction. How to Speak Crypto. Classic Crypto. Simple Substitution Cipher. Cryptanalysis of a Simple Substitution. Definition of Secure. Double Transposition Cipher. One-time Pad. Project VENONA. Codebook Cipher. Ciphers of the Election of 1876. Modern Crypto History. Taxonomy of Cryptography. Taxonomy of Cryptanalysis.

**8 Hours**

**Module – 2.**

What is a Hash Function? The Birthday Problem. Non-cryptographic Hashes. Tiger Hash. HMAC. Uses of Hash Functions. Online Bids. Spam Reduction. Other Crypto-Related Topics. Secret Sharing. Key Escrow. Random Numbers. Texas Hold 'em Poker. Generating Random Bits. Information Hiding.

**8 Hours**

**Module – 3**

Random number generation Providing freshness Fundamentals of entity authentication Passwords Dynamic password schemes Zero-knowledge mechanisms Further reading Cryptographic Protocols Protocol basics From objectives to a protocol Analysing a simple protocol Authentication and key establishment protocols

**8 Hours**

**Module – 4**

Key management fundamentals Key lengths and lifetimes Key generation Key establishment Key storage Key usage Governing key management Public-Key Management Certification of public keys The certificate lifecycle Public-key management models Alternative approaches

**8 Hours**

**Module – 5**

Cryptographic Applications Cryptography on the Internet Cryptography for wireless local area networks Cryptography for mobile telecommunications Cryptography for secure payment card transactions Cryptography for video broadcasting Cryptography for identity cards Cryptography for home users

**8 Hours**

**Course outcomes:** The students should be able to:

- Analyze the Digital security lapses
- Illustrate the need of key management

**Question paper pattern:**

The question paper will have ten questions.

There will be 2 questions from each module.

Each question will have questions covering all the topics under a module.

The students will have to answer 5 full questions, selecting one full question from each module.

**Text Books:**

1. Information Security: Principles and Practice, 2nd Edition by Mark Stamp Wiley
2. Everyday Cryptography: Fundamental Principles and Applications Keith M. Martin Oxford Scholarship Online: December 2013

**Reference Books:**

1. Applied Cryptography Protocols, Algorithms, and Source Code in C by Bruce Schneier



**H. O. D.**

Dept. Of Information Science & Engineering  
Alva's Institute of Engg. & Technology  
Mijar, MOODBIDRI - 574 225