BMS COLLEGE OF ENGINEERING, BANGALORE-19

(Autonomous College under VTU Belagavi)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Semester	**5**		
Course Title:	**Cryptography**		
Course Code:	**22CS5PCCRP**		
L-T-P:	**3-1-0 Total Credits:**		**4**

Unit No.	**Topics**	**Hrs.**
1	**Introduction:** Security Goals, Cryptographic Attacks **Mathematics of Cryptography:** Integer Arithmetic, Modular Arithmetic, Linear Congruence **Traditional symmetric-Key Ciphers:** Introduction, Substitution Ciphers, Transposition Ciphers, **Mathematics of Symmetric-key cryptography:** Algebraic Structures, GF (2n) Fields	**8**
2	**Introduction to Modern Symmetric Key Ciphers:** Modern Block Ciphers, Modern Stream Ciphers. **Data Encryption Standard (DES):** Introduction, DES Structure, DES Analysis, Security of DES, Multiple DES **Advanced Encryption Standard (AES):** Introduction, Transformations, Key Expansion, AES Ciphers, analysis of AES	**8**
3	**Encipherment using Modern Symmetric-Key Ciphers:** Use of Modern Block Ciphers, Use of Stream Ciphers. **Mathematics of Asymmetric-Key Cryptography:** Primes, Primality Testing, Chinese Remainder Theorem, Quadratic Congruence, Legendre Symbol.	**8**
4	**Asymmetric -Key Cryptography:** Introduction, RSA cryptosystem, ElGamal Cryptosystem, Elliptic Curve cryptosystems. Cryptographic hash functions, Secure hash algorithm,	**8**
5	**Message Integrity and Message Authentication:** Message authentication, Digital Signature, RSA digital signature. **Key Management:** KERBEROS , Diffie-Hellman Key Agreement, X.509	**8**

Course Outcomes (Co):

CO1	**Apply** cryptographic techniques to ensure data confidentiality, integrity, and authentication.
CO2	**Analyze** various symmetric and asymmetric cryptosystems and types of attacks on these cryptosystems.
CO3	**Demonstrate** cryptographic encryption and decryption techniques.

CO-PO-PSO Mapping:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3														3
CO2	3				3					1 1					
CO3	2														

Tool	Remarks	Marks
Internals	Best 2 out of 3	40
Quiz	--	--
Lab Component	--	--
Self-Study Component	--	--
AAT	ONE	10
Total		50

Prescribed Text Book:

Sl. No.	Book Title	Authors	Edition	Publisher	Year
1	“Cryptography and Network Security”	Behrouz A. Forouzan and Debdeep Mukhopadhyay	2nd edition	Tata McGraw Hill	2013

Reference Text Book:

Sl. No.	Book Title	Authors	Edition	Publisher	Year
1	“Cryptography: Theory and Practice”	Stinson. D.	3rd edition	Chapman & Hall/CRC	2012
2	“Cryptography and Network Security”	Atul Kahate		Tata McGraw-Hill	2003
3	”Cryptography and Network Security Principles and practice”	W. Stallings	5th edition	Pearson Education Asia	2013

E-Book:

Sl. No.	Book Title	Authors	Edition	Publisher	Year	URL
1	Cryptography and Network Security. Principles and Practice	William Stallings	3rd edition	Pearson Education	2007	http://williamstallings.com /Crypto3e.html
2	Handbook of Applied Cryptography	Menez, van Oorschot, Vanstone	ISBN: 0-8493-8523-7	CRC Press	2001	http://www.cacr.math.uwa terloo.ca/hac/

Mooc Course:

Sl. No.	Course name	Course Offered By	Year	URL
1	Cryptography and Network Security	NPTEL	2017	http://nptel.ac.in/courses/106105031/
2	Cryptography 1	Coursera	2019	https://www.coursera.org/course/crypto

Alternate Assessment Tool Plan:

PLAN:

Students are supposed to develop a Cryptographic algorithm/Digital Signature (using C/C++ preferably) without using libraries or built-in functions. Code demonstration along with a report has to be submitted.

Example: Implement of RSA Digital Signature, Elgamal Digital Signature, Diffie Hellman Signature, and Modified RSA algorithm for practical purpose, Hybrid encryption schemes.

Sl. No	Week	Activity
1	1st and 2nd	Formation of groups. Note: Student groups of size 2 members only
2	3rd	AAT topic selection by each group
3	4th	Presentation: Student team and topic introduction by each group
4	5th, 6th	Design the workflow along with Front-end Design
5	7th	Presentation on Front-end Design of the application
6	8th, 9th, 10th	Design and Development of the actual algorithm and testing it for various test cases.
7	11th	Complete code demonstration
8	12th	AAT Report Preparation

Rubrics Used For Evaluation (AAT):

Criteria	Exemplary Proficient		Partially Proficient	Points
User Interface / Front End Design OR Tool Usage	(1) The designed application has an exceptional design, attractive and usable interface. It is easy to locate all important elements.	(0.75) The designed application has an attractive design and usable interface. It is easy to locate all important elements.	(0.5) The designed application has a usable design interface, but may appear busy or boring. It is easy to locate most of the important elements.	___ / 1
Implementation of the Algorithm OR Implementation done in the Tool	(4) Implementation of the algorithm has been done accurately without the usage of any library functions.	(2.5) Implementation of the algorithm has been done appropriately without the usage of any library functions.	(1.5) Implementation of the algorithm has been done with usage of few library functions.	___ /4
Testing for various cases	(1) The implemented algorithm works for any given valid input.	(0.75) The implemented algorithm works for almost all valid inputs.	(0.5) The implemented algorithm works for any some valid inputs.	___ /1
Application/Relevance	(1) The designed algorithm has several applications and is relevant in the area of cryptography.	(0.75) The designed algorithm has few applications and is relevant in the area of cryptography.	(0.5) The designed algorithm has few applications and is not very relevant in the area of cryptography.	___ /1
Report	(1) Clear and Effective writing and adherence to appropriate style guidelines	(0.75) Writing that is clear and effective for the most part and minor errors in adherence to appropriate style guidelines	(0.5) Unclear and ineffective writing and multiple errors in adherence to appropriate style guidelines	___/1
Oral communication (presentation)	(1) Clear and effective communication	(0.75) Communication is clear	(0.5) Unclear communication	___/1
Participation in Discussions	(1) Provided many good ideas; inspired others; clearly communicated ideas, needs, and feelings.	(0.75) Participated in discussions; on some occasions, made suggestions.	(0.5) Listened mainly; Rarely spoke up, and ideas were off the mark.	___/1
Total				__/ **10**

Tutorial Plan :

Tutorial #	Topic
1	**Open SSL Library Features and Application in Cryptography** **https://www.openssl.org/docs/**
2	**Introduction to CrypTool and Installation** **Demonstration of basic features available in CrypTool**
3	**Demonstration of Caesar cipher** In the message to decode, any punctuation is left unchanged in the encoded message, as too are any numbers. To change this **Options > Text Options** and from here you can select what attributes of a message the cipher will alter and which it will leave unchanged. Experiment encrypting the same message with the Caesar cipher with different settings selected from the text options. Decipher each message after doing so and see if the deciphered message still has the same punctuation, spacing etc.
4	**Demonstration of Vigenere cipher** Animal is a tool within the CrypTool that displays the concepts behind a cipher in a user friendly fashion, by the means of an animation. Demonstrate the use of animal tool for the above cipher.
5	**Demonstration of DES** Open a new file and type a plaintext message. Next click from the menu **Crypt/Decrypt > Symmetric (modern) > DES (ECB)…** This presents a key selection window, this key must be 64 bits long, which equates to 16 hexadecimal figures. For simplicity use the default key of: 00 00 00 00 00 00 00 00 Select **Encrypt** and there should be presented a window showing the data encrypted in hexadecimal form and its corresponding ASCII representation. To decrypt the message again select **Crypt/Decrypt > Symmetric (modern) > DES (ECB)…** Use the same key and select **Decrypt**, and the original message will be displayed in hexadecimal representation. Selecting **View > Show as text** displays it in ASCII; you may also notice some of the formatting is lost in the process or some padding is added. Encrypt the same message using the same process as above only selecting **Crypt/Decrypt > Symmetric (modern) > DES (CBC)…** instead. Compare the two encrypted messages.
6	**Compare ECB versus CBC mode of operation for the following applications: a) An online bank statement** b) **An encrypted VoIP session** c) **Viewing of a website using TCP/IP** **Demonstrate DES encryption and decryption using Animal.**
7	**Demonstration of RSA**
8	Now, encrypt a message of your choice using the values: p = 59, q = 71, e = 13 Observe the results. Encrypt the same message with the values: p = 673, q = 619, e = 13 **Demonstrate RSA encryption and decryption using Animal.**
9	**Demonstrate RSA implementation using PKI.**
10	

11	**1963497163 is the product of two prime numbers, use tools within the CrypTool to find these two prime numbers. Mention what tools you used to do this.**
12	**Demonstrate hybrid encryption** Combine aspects of AES and RSA algorithm and demonstrate encryption of different plaintext.
13	**Demonstration of** OWASP vulnerabilities

SEE Exam Question Paper Format:

Unit-1	Internal Choice	Two Questions to be asked for 20 Marks each
Unit-2	Mandatory	One Question to be asked for 20 Marks
Unit-3	Mandatory	One Question to be asked for 20 Marks
Unit-4	Internal Choice	Two Questions to be asked for 20 Marks each
Unit-5	Mandatory	One Question to be asked for 20 Marks

Bloom's Level	**Percentage of Questions to be Covered**
Remember / Understand	35%
Apply / Analyze	40%
Create / Evaluate	25%