GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)

SUBJECT NAME: CRYPTANALYSIS: FUNDAMENTALS AND APPLICATIONS

SUBJECT CODE: 2725906

SEMESTER: II

Type of course: Master of Engineering (Cyber Security)

Prerequisite: Cryptography fundamentals

Rationale: Cryptanalysis is about interpreting cipher text. The cryptanalyst's goal is to discover weaknesses or flaws in cryptosystems and break the security provided by those systems. Professional cryptanalysts play an important role in evaluating and corroborating the strength of cryptosystems.

Teaching and Examination Scheme

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content

Sr. No.	Content	Total Hours	%Weightage
1.	**Fundamentals of cryptosystems, Breaking cryptosystems** Different cryptographic systems, cryptographic primitives for security services, Basic model of the cryptosystem, codes, stegnography, access control, secrecy of the encryption key, key lengths, key spaces, breaking encryption algorithms, exhaustive key searches, classes of attack, academic attack	6	10
2.	**Cryptographic applications** Cryptography for securing the internet, Cryptography for wireless local area network, Cryptography for mobile telecommunications, Cryptography for secure payment card transactions, Cryptography for video broadcasting, Cryptography for identity cards, Cryptography for anonymity, Cryptography for digital currency	12	30
3.	**Cryptography for personal devices** File protection, Email security, Messaging security, platform security	3	10
4.	**General cryptanalytic methods** Brute force, Time-space tradeoffs, Rainbow tables, slide attacks, cryptanalysis of hash functions, cryptanalysis of random number generators	4	10
5.	**Linear cryptanalysis** Matsui's algorithms, Linear expressions for S-boxes, Matsui's piling up Lemma,Easy1 cipher, Linear expressions and key recovery, Linear cryptanalysis of DES, Multiple linear approximations, Finding linear expressions, linear cryptanalysis code	9	20

6.	**Differential cryptanalysis** S-box differentials, Combining S-box characteristics, key derivation, differential cryptanalysis code, differential cryptanalysis of Feistle ciphers, analysis, differential linear cryptanalysis, conditional characteristics, Higher order differentials, truncated differentials, impossible differentials, boomerang attack, interpolation attack, Related key attack	12	20

Suggested Specification table with Marks (Theory)

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	**30**	**30**			

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books

1. Everyday Cryptography: Fundamental principles and applications By Kevith M. Martin, Oxford University Press

2. Modern cryptanalysis techniques for advanced code breaking, Christopher Swenson, WILEY

Course Outcome

After learning this course, the students should able to:

- Apply cryptography for various applications
- Perform linear cryptanalysis
- Perform differential cryptanalysis

List of Experiment

1) Write a program to reconstruct the private key of RSA from public key.

2) Write a program to find easy factorization for given number which is a product of two prime numbers.

3) Write a program to analyze the effect of constant on cryptographic algorithm.

4) Write a program to perform metaheuristic attack on block cipher.

5) Write a program to perform cryptanalysis on Caesar cipher.

6) Write a program to perform fast attack on simple substitution cipher.

7) Write a program to perform known plaintext attack on DES.

8) Write a case study how cryptanalysis can be performed on browsers.

Design based Problems (DP)/Open Ended Problem

1) Develop cryptanalysis for ciphers having nonrandom behavior.

Major Equipment

Computer systems having following minimum technical configurations

Processor:i3 or i5 or higher

RAM: minimum 4 GB

HDD: 1 TB

Internet and Wi-Fi connectivity

License Window/Linux operating system

List of Open Source Software/learning website

1) https://cyberforensics.tech.purdue.edu