Information Security and Cryptography (CS302)
B.Tech. III (CSE) - Semester 6
Academic year 2023-24
Lecture Plan

Course Outcomes:

After successful completion of this course, student will be able to

1. Understand the concepts related to Information Security and Cryptography
2. Apply the concept of security services and mechanisms from the application developers and network administrator's perspective.
3. Analyze the security schemes for their use in different application scenarios.
4. Evaluate and asses the computer and network systems for associated risks.
5. Design the security schemes depending on the organization requirements.

Lecture Plan

WEEK NUMBER	TOPIC	FACULTY MEMBER
Week 1	• Introduction to the course, scheme and syllabus • Security Goals, CIA Traid, Security Attacks, Active and Passive Attacks • Security Services, Security Mechanisms, Model of Network Security	S J Patel
	• Information Security in current context, attack vectors, threat landscape	D R Patel
Week 2	• Number theory: Modular arithmetic, congruence, divisibility, Euclidean algorithm, Inverses • Algebraic structures, Groups – Properties, subgroups, Lagrange's theorem	S J Patel
	• Substitution Techniques, Ceaser and Monoalphabetic Ciphers	D R Patel
Week 3	• Number theory (cont.), permutation group, cyclic groups, Rings, Finite Fields- GF(p) and GF(2^n) • Shannon's theory	S J Patel
	• Polyalphabetic Ciphers, One-time pad	D R Patel
Week 4	• Euler's phi function, Euler's theorem, Fermat's little theorem, Chinese remainder theorem • Integer factorization, Discrete logarithm and related hard problems	S J Patel
	• Transposition techniques and related ciphers	D R Patel
Week 5	• Principles of Public Key Cryptography (PKC), RSA • Security analysis and attacks on RSA	S J Patel
	• Digital Watermarking and Steganography	D R Patel
Week 6	• Diffie-Hellman Key Exchange • El-gamal Cryptosystem	S J Patel
	• Modern symmetric cipher building blocks, block cipher design principles	D R Patel
Week 7	• Elliptic Curves, prime and binary curves, Point addition and scaler multiplication, • Properties of elliptic curve points	S J Patel

	• Fiestel cipher, Diffusion and Confusion, Avalanche effect	D R Patel
Week 8	• Elliptic curve discrete logarithm problem • Elliptic curve based encryption algorithms	S J Patel
	• Data Encryption Standard (DES), Cryptanalysis of DES	D R Patel
MID SEMESTER EXAMINATION		
Week 9	• Hash Functions and Data Integrity, Properties of cryptographic hash functions, • Security of Hash Functions-The Random Oracle Model	S J Patel
	• Advanced Encryption Standard (AES) and cryptanalysis	D R Patel
Week 10	• Iterated Hash Functions- Merkel Damgard Construction • Secure Hash Algorithm (SHA).	S J Patel
	• Block cipher modes of operation	D R Patel
Week 11	• Message authentication requirements, security • Message authentication codes (MAC) based on hash functions-HMAC • MACs based on block ciphers- CMAC	S J Patel
	• Random Bit Generation and Stream Ciphers	D R Patel
Week 12	• Authenticated Encryption • Digital Signatures: Security requirements, RSA Digital Signatures,	S J Patel
	• Advanced topics: Tweakable ciphers	D R Patel
Week 13	• NIST Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), RSA-PSS Digital Signature Algorithm	S J Patel
	• Advanced topics: Format preserving ciphers	D R Patel
Week 14	• Entity Authentication: Challenge-response protocol • Password based authentications, Zero-knowledge Proofs	S J Patel
	• Advanced topics	D R Patel
END SEMESTER EXAMINATION		

Sankita Patel, Course Co-ordinator