Cryptography Assignment – Topic Analyses

Subject Code: 2CSE50E24

Name: Rahul Rameshbhai Prajapati

Enrollment Number: 23162171020

Course: B.Tech – Cyber Security

Date: 21/10/2025

Selected Topics:

1. Unit 1 – Security Attacks

2. Unit 2 – Modular Arithmetic

3. Unit 3 – Substitution Ciphers

4. Unit 4 – Advanced Encryption Standard (AES)

5. Unit 5 – RSA Algorithm

Unit 1: Security Attacks – Real-World Application & Relevance

*Real-World Application & Relevance*Security attacks encompass all unauthorized attempts to access, alter, disable, or destroy digital systems. They are categorized mainly as *active* and *passive* attacks. Passive attacks include sniffing and eavesdropping, while active attacks involve data modification, phishing, or denial-of-service (DoS). Modern cybersecurity frameworks, such as NIST and ISO 27001, depend on understanding these attack types for efficient defense strategies.

In 2025, the threat landscape has expanded with *AI-enhanced phishing, **deepfake-based social engineering, and **IoT exploitation*. Research in cyber threat intelligence (CTI) and adversarial machine learning (AML) relies on analyzing these attacks to predict and prevent breaches.

Applications:

- Basis for red teaming and penetration testing
- Incident response planning and threat modeling
- Design of firewalls, IDS, and SIEM solutions
- Cybersecurity awareness programs

Advantages / Strengths

- Structured taxonomy for categorizing threats
- Supports creation of layered security architectures
- Enables risk-informed decisions and compliance monitoring

Disadvantages / Limitations

- Rapidly evolving vectors make static models obsolete
- High defense costs compared to attack execution
- Difficulty in attribution and response prioritization

*Differences vs Security Services*Security Attacks represent techniques used by adversaries, while Security Services like *confidentiality, integrity,

authentication, and **non-repudiation* are designed to protect against attacks.

Parameter	**Security Attacks**	**Security Mechanisms**
Role	Offensive	Defensive
Examples	Replay, MitM, DoS, SQLi	AES, RSA, IDS, Firewalls
Effect	Disrupts or exploits systems	Safeguards/protects systems
Objective	Exploitation/destruction	Protection/recovery

Unit 2: Modular Arithmetic – Real-World Application & Relevance

*Real-World Application & Relevance*Modular arithmetic forms the mathematical foundation of most cryptographic algorithms. Operations such as *modular exponentiation* and *inverses* are crucial for algorithms like *RSA, **DH, and **ECC*.

For example, RSA uses (C = M^e mod n) and (M = C^d mod n). DH relies on modular exponentiation for secure key exchange over public channels.

Applications:

- Key generation and exchange protocols
- Digital signatures and authentication
- Blockchain hashing and mining
- Random number generation in cryptographic systems

Advantages / Strengths

- Provides strict, efficient finite field structures
- Enables secure cryptography via hard problems (factoring, DLP)
- Operations support diverse cryptosystems effectively

Disadvantages / Limitations

- Weak modulus/prime choices compromise security
- High computation cost for large keys
- Susceptibility to quantum computing attacks (Shor's algorithm)

*Differences vs Linear Congruence*Modular arithmetic defines the number system under a modulus, while linear congruence focuses on solving equations (ax equiv b mod n).

Parameter	**Modular Arithmetic**	**Quadratic Congruence**
Use	RSA, DH, ECC	Rabin Cryptosystem
Complexity	Moderate	Higher for composite modulus
Hardness Basis	Factoring, DLP	Quadratic Residue Problem

Parameter	Modular Arithmetic	Quadratic Congruence
Operation Type	General modulo	Specialized equation solving

Unit 3: Substitution Ciphers – Real-World Application & Relevance

*Real-World Application & Relevance*Substitution ciphers are among the earliest cryptographic systems, replacing each character or symbol according to a key. Their concept persists in modern cryptosystems, especially as the basis for S-boxes in ciphers like AES.

Applications:

- Educational illustration of classical cryptography
- Simple obfuscation or puzzle systems
- Key concept behind nonlinear transformations in block ciphers

Advantages / Strengths

- Simple, fast for learning and demonstration
- Forms basis of S-box design and nonlinear crypto
- Illustrates fundamental cryptographic concepts

Disadvantages / Limitations

- Easily broken by frequency analysis
- No secure key exchange; weak against modern cryptanalysis

- Not recommended for real-world encryption

*Differences vs Transposition Cipher*Substitution alters symbols, transposition rearranges their order.

Parameter	**Substitution Cipher**	**Steganography**
Purpose	Obfuscate text	Hide existence of message
Visibility	Ciphertext visible	Message hidden
Security Basis	Secret mapping/key	Concealment in cover medium
Example	Caesar, Vigenère	Image/audio embedding

Unit 4: Advanced Encryption Standard (AES) – Real-World Application & Relevance

*Real-World Application & Relevance*AES is the global symmetric encryption standard. It encrypts 128-bit data blocks using keys of 128, 192, or 256 bits. AES is implemented in HTTPS, VPNs, Wi-Fi, disk encryption systems, and more.

It uses a substitution-permutation network (SPN) structure, involving SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations.

Applications:

- Data encryption for TLS/SSL communication

- Secure file/storage/database systems
- Hardware security modules (AES-NI)
- Blockchains and smart contract encryption

Advantages / Strengths

- High performance in hardware and software
- Resistant to most cryptanalysis
- Parallelizable and widely standardized

Disadvantages / Limitations

- Poor mode selection (e.g., ECB) can leak patterns
- Implementation flaws can expose side-channel data
- Quantum computing reduces effective security margins

*Differences vs DES*DES, with 56-bit keys, is obsolete. AES uses bigger keys, more rounds, and greater cryptanalytic resistance.

Parameter	**AES**	**Stream Cipher**
Processing	Block (128-bit)	Continuous (bit/byte)
Typical Uses	Storage, VPN, TLS	Streaming, IoT
Structure	SPN	Keystream generator
Security	High (128–256 bits)	Depends on keystream

Unit 5: RSA Algorithm – Real-World Application & Relevance

*Real-World Application & Relevance*RSA is the leading asymmetric cryptography standard, based on the challenge of factoring large numbers. It enables encryption, digital signatures, and secure key exchange, forming the foundation for Public Key Infrastructure (PKI), SSL/TLS, and X.509 digital certificates.

RSA employs a public/private key pair. Despite the rise of ECC, RSA remains widely implemented for its standardization and interoperability.

Applications:

- Digital signatures for SSL/TLS
- Key distribution in hybrid schemes
- Authentication in VPN, web apps, secure email
- Software/firmware integrity validation

Advantages / Strengths

- Well-established mathematical foundation
- Enables encryption and authentication
- Globally standardized with broad support

Disadvantages / Limitations

- Requires large keys (2048+ bits) for robust security
- Slow compared to symmetric encryption
- Susceptible to side-channel and padding oracle attacks

- Quantum computing threats (Shor's algorithm)

*Differences vs Rabin Cryptosystem*Rabin is based purely on factorization and may yield multiple decryption outputs, unlike RSA with its unique encryption-decryption pair.

Parameter	**RSA**	**Diffie-Hellman**
Operation	Encryption/Signing	Key Exchange
Hardness Basis	Integer Factoring	Discrete Logarithm
Key Type	Public/Private pair	Shared Secret Derivation
Use Cases	PKI, SSL, S/MIME	VPN, TLS session keys
