Cryptography and Encryption Assignment

TITTLE: Exploring and Implementing Modern Trends in Cryptography
Submission Deadline: 8th April, 2025
Group Size: 5

1. OBJECTIVE

This assignment requires students to explore, analyze, and implement modern cryptographic trends. Each group will:

1. Research and discuss a selected cryptographic trend.
2. Attempt an implementation (where applicable) by developing a prototype, simulation, or proof-of-concept.
3. Select and analyze a research paper (published within the last five years) from a reputable journal or conference.
4. Write a structured technical report detailing their findings, implementation, and analysis.

2. ASSIGNMENT SCOPE & TOPICS

Each group must select one of the following areas for their discussion, implementation, and research paper selection:

1. Post-Quantum Cryptography (PQC) – Exploring quantum-resistant algorithms (e.g., CRYSTALS-Kyber, NTRU).
2. Homomorphic Encryption – Implementing basic operations on encrypted data without decryption.
3. Zero-Knowledge Proofs (ZKPs) & Blockchain Security – Applying zk-SNARKs or zk-Rollups in privacy-focused transactions.
4. Secure Multi-Party Computation (SMPC) – Investigating protocols for secure data sharing.
5. AI and Cryptography – Examining how AI enhances cryptanalysis and cryptographic security.
6. Lightweight Cryptography for IoT – Implementing a lightweight encryption algorithm for constrained devices.
7. Passwordless Authentication & Biometric Cryptography – Investigating FIDO2, WebAuthn, or biometric-based authentication.

8. Attribute-Based Encryption (ABE) – Exploring fine-grained access control in cloud environments.
9. DNA Cryptography & Confidential Computing – Exploring ultra-secure encryption techniques or TEEs.
10. Signcryption – Implementing combined digital signature and encryption techniques for efficient security in communication.

3. REPORT FORMAT (UMaT STANDARD)

- The final report must be prepared according to UMaT's technical report format
- The report must be 10–12 pages (excluding references and appendices).
- Use UMaT technical report guidelines and referencing style
- Plagiarism will not be tolerated. All submissions must include a plagiarism report (Turnitin or similar).

4. SUBMISSION GUIDELINES

- Submission of technical report.
- PPT presentations and demonstration where applicable

CONCLUSION

This assignment enables students to explore, analyze, and implement modern cryptographic trends. By researching recent papers, evaluating cryptographic techniques, and attempting practical implementations, students will gain hands-on experience in encryption, privacy, and security. The structured report will enhance their technical writing and analytical skills, preparing them for real-world cybersecurity challenges