Subject Description Form

Subject Code	COMP5576
Subject Title	Modern Cryptography
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	This course aims to provide students with a solid understanding of modern cryptographic concepts and their application in securing digital systems and internet traffic. Students will learn about fundamental and advanced cryptographic primitives, formal security models, and practical protocols. The course also explores cybersecurity principles, real-world threats, secure communication, and attack detection. By doing so, we are going to equip students with the technical depth required to analyse and develop secure systems and preparing students for research or industry roles where they can apply cryptographic techniques to real-world cybersecurity problems.
Intended Learning Outcomes	Upon completion of the subject, students will be equipped with Professional / Academic Knowledge and Skills: (a) **Identify and explain major cryptographic primitives and protocols** (e.g., encryption, digital signatures, key exchange), and evaluate their strengths and limitations under formal security models. (b) **Understand common security threats** to data, systems, and communication networks, and apply cryptographic techniques as countermeasures. (c) **Design and implement secure cryptographic protocols by** integrating symmetric and public-key techniques. (d) **Apply a combination of cryptographic tools and system-level security measures** to meet confidentiality, integrity, authenticity, and non-repudiation requirements in realistic scenarios. (e) **Critically assess emerging cybersecurity risks and privacy challenges**, and reflect on the potential of modern technologies (e.g., post-quantum cryptography, zero-knowledge proofs) to address them.
Subject Synopsis/ Indicative Syllabus	Topic 1: Cryptography • Cryptographic primitives: symmetric and public key encryption, hash functions, message authentication codes, digital signatures. • Security models and provable security. • Cryptographic protocols: Key establishment protocols.

<table>
<tr><td></td><td>

Advanced topics: zero-knowledge proofs, homomorphic encryption, post-quantum cryptography.

Topic 2: Cybersecurity

Types of attacks, threat models, and the role of cryptography in network security.
Secure Sockets Layer (SSL), Transport Layer Security (TLS), and TCP-level security extensions.
Web security and major threats to web applications: XSS, CSRF, session hijacking, cookie manipulation
Network Security Tools and Practices. Penetration testing and vulnerability scanning methodologies.

Topic 3: Case Study

Real-world analysis of security breaches and cryptographic failures.
Application of learned techniques to evaluate and strengthen a system’s security posture.
Policy and compliance considerations in practical settings.

</td></tr>
<tr><td>Teaching/Learning Methodology</td><td>The course uses a combination of lectures, case-based discussions, assignments, and labs. Students will engage in both analytical reasoning and practical system design, culminating in individual and group-based assessments.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Learning Outcomes</td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="5">Intended subject learning outcomes to be assessed (Please tick as appropriate)</td></tr>
<tr><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td></tr>
<tr><td>1. Assignment(s)</td><td>5%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td></tr>
<tr><td>2. Project</td><td>10%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td></tr>
<tr><td>3. Midterm</td><td>15%</td><td>√</td><td>√</td><td>√</td><td>√</td><td>√</td></tr>
<tr><td>4. Final Examination</td><td>70 %</td><td>√</td><td>√</td><td>√</td><td>√</td><td></td></tr>
<tr><td>Total</td><td>100 %</td><td colspan="5"></td></tr>
</table>
Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:
Continuous assessment consists of assignments, projects, and midterm to facilitate students to achieve the intended learning outcomes.

Assignments are designed to evaluate students’ technical understanding of cryptographic primitives, protocol implementation, and the ability to analyse security threats and countermeasures in practice. They promote hands-on application of theoretical concepts and foster analytical thinking.
</td></tr>
</table>

<table>
<tr><td></td><td colspan="2">Project is designed to encourage teamwork or individual initiative to solve open-ended problems or evaluate the security of a system/application using the full range of course knowledge.

Midterm aims to reinforce theoretical understanding through focused assessments, ensuring retention of core concepts and definitions.

The final examination assesses students' comprehensive grasp of core principles in cryptography and cybersecurity, and their ability to reason formally about security goals, threats, and protocol design.</td></tr>
<tr><td rowspan="6">Student Study Effort Expected</td><td>Class contact:</td><td></td></tr>
<tr><td>▪ Lecture</td><td>26 Hrs.</td></tr>
<tr><td>▪ Lab & Tutorial</td><td>13 Hrs.</td></tr>
<tr><td>Other student study effort:</td><td></td></tr>
<tr><td>• Assignment & Projects</td><td>66 Hrs.</td></tr>
<tr><td>Total student study effort</td><td>105 Hrs.</td></tr>
<tr><td>Reading List and References</td><td colspan="2">Boneh, D., & Shoup, V. (2020). A graduate course in applied cryptography. Draft 0.6.

Katz, J., & Lindell, Y. (2007). Introduction to modern cryptography: principles and protocols. Chapman and hall/CRC.

Stallings, W. (1995). Network and internetwork security: principles and practice. Prentice-Hall, Inc..

Du, W. (2022). Computer & internet security: a hands-on approach. Independently published.</td></tr>
</table>