INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «___» _____

Programme	**LEVEL 5 EXTENDED DIPLOMA IN CYBERSECURITY**		
Unit Number/ Unit Title	**UNIT 6 CRYPTOGRAPHY**		
Cohort Code:	L04CRP-U6		
Unit Level	Level 4		
Total GLH	Total qualification time 200/ Total Guided learning hours 90/ Self-guided learning hours 110		
Credits	20 CATS/ 10 ECTS		
Lecturer			
Start Date		**End Date**	

Unit Aims	This module provides an introduction to the principles and practices of cryptography. Learners will gain an understanding of the fundamental concepts, algorithms, and applications of cryptographic techniques, which are essential for securing information in various digital and communication systems.
Differentiation Strategies *(e.g. planned activities or support for individual learners according to their needs)*	The total number of students to be in the lesson is approximately 20. This is a multicultural group of students predominantly between the ages of 24 – 45, with numerous ethnic, gender, and creed background. These are UK academic level 5 students; hence it is assumed that they have practical, theoretical, or technological knowledge and understanding of a subject or field of work to find ways forward in broadly defined, complex contexts. These students must be able to generate information, evaluate, synthesise the use information from a variety of sources. Various approaches to addressing the various identified students needs will be adopted throughout the lesson. Such will include:- 1. Progressive tasks 2. Digital resources

	3. Verbal support 4. Variable outcomes 5. Collaborative learning 6. Ongoing assessment 7. Flexible-pace learning
Equality & Diversity	Variety of teaching techniques will be employed to ensure that the needs of each individual learner are met.
Safeguarding & Prevent	Safeguarding policies and the Prevent duty are strictly observed to ensure the safety, well-being, and inclusivity of all students and staff.
Health & Safety	SIRM H&S policies will be maintained.
Learning Resources	**Teaching and Learning Materials** • Stallings, W. (2017). "Cryptography and Network Security: Principles and Practice." Pearson. • Schneier, B. (2015). "Applied Cryptography: Protocols, Algorithms, and Source Code in C." Wiley. • Katz, J., & Lindell, Y. (2020). "Introduction to Modern Cryptography." CRC Press. • Ferguson, N., Schneier, B., & Kohno, T. (2010). "Cryptography Engineering: Design Principles and Practical Applications." Wiley. • Menezes, A., van Oorschot, P., & Vanstone, S. (1996). "Handbook of Applied Cryptography." CRC Press.

Learning Outcome	Assessment Criteria
LO1. 1. Understand fundamental concepts of cryptography.	1.1 Define cryptography and its importance in information security. 1.2 Explain the principles of symmetric and asymmetric cryptography. 1.3 Describe common cryptographic algorithms (e.g., AES, RSA, SHA).
LO2. 2. Apply cryptographic techniques to secure data.	2.1 Demonstrate the encryption and decryption of data using symmetric algorithms. 2.2 Implement public key infrastructure (PKI) for secure communications. 2.3 Use hash functions for data integrity and authentication.
LO3. 3. Analyze cryptographic protocols.	3.1 Evaluate the strengths and weaknesses of different cryptographic protocols. 3.2 Assess the security of cryptographic implementations in various applications.

No	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cryptography**	**Introduction to Cryptography** Definition, history, and role in cybersecurity	LO1: Fundamental Concepts	
2	**Cryptographic Goals**	**Cryptographic Goals** Confidentiality, integrity, authenticity, non-repudiation	LO1: Fundamental Concepts	
3	**Symmetric Cryptography**	**Symmetric Cryptography** Principles, key exchange problem, block vs. stream ciphers	LO1: Fundamental Concepts	
4	**Asymmetric Cryptography**	**Asymmetric Cryptography** Public/private keys, mathematical foundations (prime numbers, modular arithmetic)	LO1: Fundamental Concepts	
5	**Common Cryptographic Algorithms**	**Common Cryptographic Algorithms** AES (symmetric), RSA (asymmetric), SHA (hashing)	LO1: Fundamental Concepts	
6	**Symmetric Encryption in Practice**	**Symmetric Encryption in Practice** AES modes (CBC, GCM), key management	LO2: Cryptographic Techniques	
7	**Asymmetric Encryption in Practice**	**Asymmetric Encryption in Practice** RSA key generation, encryption/decryption	LO2: Cryptographic Techniques	
8	Half-Term Exam	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**Public Key Infrastructure (PKI)**	**Public Key Infrastructure (PKI)** Digital certificates, Certificate Authorities (CAs), trust chains	LO2: Cryptographic Techniques	

10	**Hash Functions**	**Hash Functions** SHA-256, MD5 (risks), HMAC for authentication	LO2: Cryptographic Techniques	
11	**Digital Signatures**	**Digital Signatures** RSA/DSA signatures, verification	LO2: Cryptographic Techniques	
12	**SSL/TLS Protocol**	**SSL/TLS Protocol** Handshake process, cipher suites, forward secrecy	LO3: Cryptographic Protocols	
13	**Secure Email (PGP/GPG)**	**Secure Email (PGP/GPG)** Key rings, encryption/decryption workflows	LO3: Cryptographic Protocols	
14	Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics	LO3: Cryptographic Protocols	
15	**Midterm**	- **Midterm assessment** covering all learning outcomes (theory and practical elements)	LO3: Cryptographic Protocols	
16	Feedback & Reflection	- Review - Individual feedback on performance - Reflective discussion on key learning points	LO3: Cryptographic Protocols	
17	**Cryptographic Weaknesses**	**Cryptographic Weaknesses** Brute force, side-channel attacks, quantum threats	LO3: Cryptographic Protocols	
18	**Cryptanalysis Basics**	**Cryptanalysis Basics** Frequency analysis, rainbow tables, birthday attacks	LO3: Cryptographic Protocols	
19	**Post-Quantum Cryptography**	**Post-Quantum Cryptography** Lattice-based, hash-based cryptography	LO3: Cryptographic Protocols	

20	**Disk Encryption**	**Disk Encryption** BitLocker, LUKS, VeraCrypt	Applications & Case Studies	
21	**Password Security**	**Password Security** Salting, bcrypt, Argon2	Applications & Case Studies	
22	**Blockchain Cryptography**	**Blockchain Cryptography** Elliptic Curve Digital Signatures (ECDSA) in Bitcoin	Applications & Case Studies	
23	Review	**Project** Design a secure communication protocol	Applications & Case Studies	
24	**Cryptography in IoT**	**Cryptography in IoT** Lightweight protocols (ChaCha20-Poly1305)	Applications & Case Studies	
25	**Case Study: Cryptographic Failures**	**Case Study: Cryptographic Failures** Heartbleed, ROCA vulnerability	Applications & Case Studies	
26	**OpenSSL Lab**	**OpenSSL Lab** Generate keys, encrypt files, create CSRs	Hands-On & Ethics	
27	**Wireshark TLS Analysis**	**Wireshark TLS Analysis** Inspect HTTPS traffic, identify cipher suites	Hands-On & Ethics	
28	**Ethical Considerations**	**Ethical Considerations** Key escrow, government backdoors, export controls	Hands-On & Ethics	
29	Final Exam Preparation & Review	LO1, LO2, LO3	LO1, LO2, LO3	
30	Final Exam		LO1, LO2, LO3	