INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

«Approved»

2025 y. «___» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 6**		
Unit Number/ Unit Title	**UNIT 3 CRYPTOGRAPHIC SYSTEMS AND PROTOCOL ENGINEERING**		
Cohort Code:	L06CSPE-U3		
Unit Level	Level 6		
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 unit aims to provide learners with in-depth theoretical and practical knowledge of modern cryptographic systems and secure protocol design. The focus is on understanding core cryptographic algorithms, cryptographic protocols, and their implementation in secure systems. Learners will explore encryption standards, secure communications (e.g., TLS), PKI, blockchain security, and cryptographic lifecycle management to prepare for roles involving crypto analysis and systems security engineering.
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** • Paar, C., & Pelzl, J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Springer. • Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley. • Stallings, W. (2023). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson. • Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography. Self-published online. • Dworkin, M. (2016). Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38.

Learning Outcome	Assessment Criteria
LO1. Examine modern cryptographic algorithms and their practical applications.	1.1 Compare symmetric and asymmetric encryption methods and their real-world use cases. 1.2 Evaluate cryptographic standards (e.g., AES, RSA, ECC) in terms of strength, performance, and vulnerabilities.
LO2. Analyse secure communication protocols and architectures.	2.1 Deconstruct the SSL/TLS handshake and its role in secure web communication. 2.2 Assess the cryptographic components of VPNs, HTTPS, and email security protocols (e.g., PGP, S/MIME).
LO3. Design and implement secure key management and Public Key Infrastructure (PKI).	3.1 Develop a PKI setup including certificate authorities and lifecycle management. 3.2 Apply key rotation, revocation, and secure storage techniques in simulated environments.
LO4. Explore the cryptographic principles behind emerging technologies.	4.1 Explain the use of cryptographic hashing and Merkle trees in blockchain systems. 4.2 Evaluate zero-knowledge proofs and homomorphic encryption for privacy-preserving computation.
LO5. Identify cryptographic vulnerabilities and mitigation strategies.	5.1 Analyse real-world cryptographic failures (e.g., Heartbleed, Logjam). 5.2 Recommend mitigation strategies and secure protocol configurations.

Week	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**: Principles, goals (CIA triad), and historical evolution.	LO1: Modern Cryptographic Algorithms & Applications	
2	**Symmetric Encryption**	**Symmetric Encryption**: Algorithms (AES, DES, 3DES), modes of operation (CBC, GCM), and use cases.	LO1: Modern Cryptographic Algorithms & Applications	
3	**Asymmetric Encryption**	**Asymmetric Encryption**: RSA, ECC, Diffie-Hellman – strengths, trade-offs, and hybrid systems.	LO1: Modern Cryptographic Algorithms & Applications	
4	**Hash Functions & MACs**	**Hash Functions & MACs**: SHA-3, HMAC, and applications in data integrity.	LO1: Modern Cryptographic Algorithms & Applications	
5	**Cryptographic Standards**	**Cryptographic Standards**: NIST/FIPS compliance, AES vs. RSA vs. ECC (performance, security).	LO1: Modern Cryptographic Algorithms & Applications	
6	**Post-Quantum Cryptography**	**Post-Quantum Cryptography**: Threats from quantum computing and emerging algorithms (Lattice-based, etc.).	LO1: Modern Cryptographic Algorithms & Applications	
7	**SSL/TLS Deep Dive**	**SSL/TLS Deep Dive**: Handshake process, cipher suites, and session resumption.	LO2: Secure Communication Protocols	
8	Half-Term Exam	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	
9	**PKI & Certificates**	**PKI & Certificates**: X.509 certificates, chain of trust, and certificate pinning.	LO2: Secure Communication Protocols	

10	**HTTPS & Web Security**	**HTTPS & Web Security**: HSTS, certificate transparency, and common attacks (MITM, BEAST).	LO2: Secure Communication Protocols	
11	**Email Security**	**Email Security**: PGP vs. S/MIME – encryption, signatures, and key distribution.	LO2: Secure Communication Protocols	
12	**VPN Protocols**	**VPN Protocols**: IPsec (IKEv2), WireGuard, OpenVPN – cryptographic underpinnings.	LO2: Secure Communication Protocols	
13	**Secure VoIP & Messaging**	**Secure VoIP & Messaging**: Signal Protocol, ZRTP, and forward secrecy.	LO2: Secure Communication Protocols	
14	Review	- Comprehensive review of all learning outcomes - Practice questions and revision of key topics		
15	Midterm	- **Midterm assessment** covering all learning outcomes (theory and practical elements)		
16	Feedback & Reflection	- Review - Individual feedback on performance - Reflective discussion on key learning points		
17	**Key Lifecycle Management**	**Key Lifecycle Management**: Generation, distribution, rotation, and revocation.	LO3: Key Management & PKI	
18	**PKI Architecture**	**PKI Architecture**: Root vs. intermediate CAs, cross-certification, and trust models.	LO3: Key Management & PKI	
19	**Hardware Security Modules (HSMs)**	**Hardware Security Modules (HSMs)**: Secure key storage and cryptographic operations.	LO3: Key Management & PKI	
20	**OAuth & JWT**	**OAuth & JWT**: Token-based authentication and	LO3: Key Management & PKI	

		cryptographic safeguards.		
21	**Blockchain Key Management**	**Blockchain Key Management**: Wallets, multisig, and hierarchical deterministic (HD) keys.	LO3: Key Management & PKI	
22	**Side-Channel Attacks**	**Side-Channel Attacks**: Mitigations for timing, power analysis, and cold boot attacks.	LO3: Key Management & PKI	
23	**Review**	**Real-World Attacks**: Case studies (Heartbleed, ROCA, DROWN, Logjam).	LO4: Cryptography in Emerging Tech	
24	**Blockchain Cryptography**	**Blockchain Cryptography**: Merkle trees, consensus mechanisms (PoW/PoS), and smart contracts.	LO4: Cryptography in Emerging Tech	
25	**Zero-Knowledge Proofs (ZKPs**	**Zero-Knowledge Proofs (ZKPs)**: zk-SNARKs, Bulletproofs, and privacy applications.	LO4: Cryptography in Emerging Tech	
26	**Homomorphic Encryption**	**Homomorphic Encryption**: Principles, partial vs. fully HE, and use cases (e.g., healthcare).	LO4: Cryptography in Emerging Tech	
27	**Secure Multi-Party Computation (SMPC)**	**Secure Multi-Party Computation (SMPC)**: Privacy-preserving data sharing.	LO4: Cryptography in Emerging Tech	
28	**Cryptographic Agility**	**Cryptographic Agility**: Best practices for protocol hardening, cipher suite prioritization.	LO5: Cryptographic Vulnerabilities & Mitigations	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	