INTERNATIONAL QUALIFICATIONS

AND ASSESSMENT CENTRE (IQAC)

Approved:

2025 y «__» _____

Programme	**CYBER SECURITY DIPLOMA - LEVEL 7**		
Unit Number/ Unit Title	**UNIT 2 ADVANCED CRYPTANALYSIS AND QUANTUM-RESISTANT SYSTEMS**		
Cohort Code:	L07ACQS-U2		
Unit Level	Level 7		
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 explores advanced cryptanalysis techniques and the design of quantum-resistant systems. Learners will assess classical and modern encryption vulnerabilities and evaluate emerging cryptographic schemes suitable for post-quantum security landscapes.
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** • Buchmann, J. (2013). Introduction to Cryptography. • Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. • Stinson, D. R., & Paterson, M. (2018). Cryptography: Theory and Practice. • NIST PQC Standardization Reports. • Schneier, B. (2015). Applied Cryptography.

Learning Outcome	Assessment Criteria
LO1. 1. Understand cryptographic vulnerabilities in current systems.	1.1 Explain side-channel, brute-force, and algebraic attacks. 1.2 Analyse real-world case studies of compromised cryptosystems.
LO2. 2. Apply cryptanalysis techniques to assess security.	2.1 Demonstrate use of differential and linear cryptanalysis. 2.2 Simulate attacks on sample cryptographic algorithms.
LO3. 3. Explore quantum computing implications on encryption.	3.1 Explain the principles of quantum computing. 3.2 Assess how Shor's and Grover's algorithms affect RSA, ECC, AES.
LO4. **4. Evaluate quantum-resistant cryptographic schemes.**	4.1 Analyse lattice-based, hash-based, and multivariate schemes. 4.2 Compare NIST PQC finalists.
LO5. 5. Design recommendations for cryptographic resilience.	5.1 Propose migration plans to quantum-safe cryptography. 5.2 Evaluate implementation barriers and organizational readiness.

Week	Learning Outcome / Topic	Learning and Teaching Activities	Which assessment criteria does the session relate to?	Day/month/ year/ signature
1	**Introduction to Cryptanalysis**	**Introduction to Cryptanalysis** – Goals, methodologies, and ethical considerations.	LO1: Understand cryptographic vulnerabilities in current systems.	
2	**Side-Channel Attacks**	**Side-Channel Attacks** – Timing, power analysis, and fault injection (e.g., Spectre/Meltdown).	LO1: Understand cryptographic vulnerabilities in current systems.	
3	**Brute-Force & Rainbow Table Attacks**	**Brute-Force & Rainbow Table Attacks** – Mitigations (key stretching, salting).	LO1: Understand cryptographic vulnerabilities in current systems.	
4	**Algebraic & Mathematical Attacks**	**Algebraic & Mathematical Attacks** – Exploiting weak key generation (e.g., ROCA vulnerability).	LO1: Understand cryptographic vulnerabilities in current systems.	
5	**Case Study: Broken Cryptosystems**	**Case Study: Broken Cryptosystems** – RSA-768, WEP, SHA-1 collisions.	LO1: Understand cryptographic vulnerabilities in current systems.	
6	**Workshop: Identifying Vulnerabilities in Open-Source Crypto Libraries**.	**Workshop: Identifying Vulnerabilities in Open-Source Crypto Libraries**.	LO1: Understand cryptographic vulnerabilities in current systems.	
7	**Differential Cryptanalysis**	**Differential Cryptanalysis** – Theory and application (e.g., DES breakage)	LO2: Apply cryptanalysis techniques to assess security.	
8	Review	- Review of LO1 topics - Practice questions and mock assessment - **Half-term assessment** based on LO1 (theory)	LO1 LO2	

8	**Linear Cryptanalysis**	**Linear Cryptanalysis** – Approximating S-boxes (e.g., FEAL cipher attacks).	LO2: Apply cryptanalysis techniques to assess security.	
10	**Boomerang & Related-Key Attacks**	**Boomerang & Related-Key Attacks** – Case study: AES-192/256 theoretical weaknesses.	LO2: Apply cryptanalysis techniques to assess security.	
11	**Simulation Lab: Attacking Toy Ciphers**	**Simulation Lab: Attacking Toy Ciphers** (e.g., Simplified AES/SPN networks).	LO2: Apply cryptanalysis techniques to assess security.	
12	**Frequency Analysis & Classical Cipher Breaks**	**Frequency Analysis & Classical Cipher Breaks** – Caesar, Vigenère, Enigma emulation.	LO2: Apply cryptanalysis techniques to assess security.	
13	**Hands-on: Cryptool 2 or Python Scripting for Cryptanalysis**	**Hands-on: Cryptool 2 or Python Scripting for Cryptanalysis**	LO2: Apply cryptanalysis techniques to assess security.	
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	**Quantum Computing Fundamentals**	**Quantum Computing Fundamentals** – Qubits, superposition, and entanglement.	LO3: Explore quantum computing implications on encryption.	
18	**Shor's Algorithm**	**Shor's Algorithm** – Polynomial-time factorization of RSA/ECC.	LO3: Explore quantum computing implications on encryption.	

19	**Grover's Algorithm**	**Grover's Algorithm** – Quadratic speedup for symmetric key searches (AES implications).	LO3: Explore quantum computing implications on encryption.	
20	**Post-Quantum Threat Timeline**	**Post-Quantum Threat Timeline** – NIST's predictions vs. current quantum hardware.	LO3: Explore quantum computing implications on encryption.	
21	**Debate: Quantum Supremacy vs. Practical Cryptanalytic Feasibility**.	**Debate: Quantum Supremacy vs. Practical Cryptanalytic Feasibility**.	LO3: Explore quantum computing implications on encryption.	
22	**Simulation: Qiskit/IBM Quantum Lab for Grover's Algorithm Demo**	**Simulation: Qiskit/IBM Quantum Lab for Grover's Algorithm Demo**	LO3: Explore quantum computing implications on encryption.	
23	**Review**	**Lattice-Based Cryptography** – NTRU, Kyber, and LWE problems.	LO4: Evaluate quantum-resistant cryptographic schemes.	
24	**Hash-Based Signatures**	**Hash-Based Signatures** – SPHINCS+, XMSS, and one-time signatures.	LO4: Evaluate quantum-resistant cryptographic schemes.	
25	**Multivariate & Code-Based Schemes**	**Multivariate & Code-Based Schemes** – Rainbow, McEliece, BIKE.	LO4: Evaluate quantum-resistant cryptographic schemes.	
26	**NIST PQC Finalist Analysis**	**NIST PQC Finalist Analysis** – CRYSTALS-Kyber vs. Dilithium vs. Falcon.	LO4: Evaluate quantum-resistant cryptographic schemes.	
27	**Final Project**	**Migration Pathways to PQC** – Hybrid systems, crypto-agility frameworks. **Implementation Challenges** – Legacy systems, regulatory hurdles, cost analysis.	LO5: Design recommendations for cryptographic resilience.	

28	**Final Project**	**Policy & Standardization** – NIST, ETSI, and IETF timelines. **Final Project: Quantum-Resistant Security Plan** – For a hypothetical organization.	LO5: Design recommendations for cryptographic resilience.	
29	Final Exam Preparation & Review	LO1, LO2, LO3, LO4	LO1, LO2, LO3, LO4	
30	Final Exam		LO1, LO2, LO3, LO4	