Qualifi Level 5 Diploma in Cyber Security

Cryptography

Level 5: Diploma in Cyber Security
UeCampus Study Guide

Academic Module Study Guide Online Learning

Unit Overview: Three Chapters

Chapter 1

Cryptographic Principles & Modes

CIA triad, symmetric & asymmetric encryption, hashing, digital signatures, TLS, standards

Chapter 2

Standards, Regulations & Laws

ISO 27001, PCI DSS, UK GDPR, export controls, lawful interception, key disclosure, penalties

Chapter 3

Designing an Encryption Plan

Attack methods, side-channel attacks, key escrow, homomorphic encryption, plan design

The CIA Triad and Cryptographic Goals

Confidentiality	Integrity	Authentication	Non-repudiation
Information accessible only to authorised parties	Data not altered or tampered with	Verify identity of sender/origin	Sender cannot deny sending a message
Symmetric & asymmetric encryption	*Hashing (SHA-256), MACs, HMAC*	*Digital signatures, certificates*	*Asymmetric digital signatures*

Kerckhoffs's Principle: security must rely on key secrecy, not algorithm secrecy — the opposite of 'security through obscurity'

The Evolution of Cryptography

700 BCE	**Scytale**	Spartan transposition cipher
50 BCE	**Caesar Cipher**	Simple substitution (shift 3)
1940s	**Enigma**	Mechanical cipher; Turing broke it
1976	**Diffie-Hellman**	First public key exchange
1977	**RSA / DES**	Public key encryption / federal standard
2001	**AES**	Rijndael wins NIST competition
2024	**Post-Quantum**	NIST standardises ML-KEM, ML-DSA

Bletchley Park's codebreaking shortened WWII by an estimated two years and laid the foundation for modern computing

Symmetric Encryption: Algorithms & Modes

Key Algorithms

DES (56-bit)	Deprecated — cracked 1999
3DES (168-bit)	Deprecated by NIST 2023
AES-128/256	Current standard — global
ChaCha20 (256-bit)	Modern stream cipher; TLS 1.3

Block Cipher Modes

ECB – Insecure! Identical blocks = identical ciphertext

CBC – XOR with previous block. Vulnerable to padding oracles

CTR – Counter mode. Parallelisable, efficient

GCM – Authenticated encryption. Recommended for TLS 1.3

Same key for encryption and decryption. Fast for bulk data. Challenge: **secure key distribution** (solved by asymmetric cryptography)

Asymmetric Encryption: Public Key Cryptography

How It Works

- Key pair: public key (shared) + private key (secret)
- Encrypt with public key → only private key decrypts
- Based on hard math: integer factorisation (RSA), discrete logarithm (DH), elliptic curves (ECC)
- 100–1000x slower than symmetric → used for key exchange and signatures, not bulk data

Key Algorithms

RSA	Encryption, signatures, key exchange
Diffie-Hellman	Key exchange only
ECDH / ECDSA	ECC variants – smaller keys, faster
Ed25519	Modern signature standard
ML-KEM (Kyber)	Post-quantum key encapsulation

Hybrid encryption: Asymmetric exchanges a symmetric session key → symmetric encrypts the bulk data. This is how TLS, SSH, PGP, and most secure protocols work.

Symmetric vs Asymmetric: Comparison

Symmetric

- Single shared key
- Very fast
- Key distribution is difficult
- 128–256 bit keys
- Bulk data encryption
- Examples: AES, ChaCha20

Asymmetric

- Public + private key pair
- Much slower (100–1000x)
- Easy key distribution
- 2048–4096 bit (RSA) / 256–521 bit (ECC)
- Key exchange, signatures, authentication
- Examples: RSA, ECDH, Ed25519

In practice, most systems use hybrid encryption — asymmetric for key exchange, symmetric for bulk data

Hashing Algorithms and Digital Signatures

Hash Function Properties

- Deterministic – same input = same hash
- One-way – cannot reverse to find input
- Collision resistant – infeasible to find two matching inputs
- Avalanche effect – 1 bit change = dramatically different hash

Common Algorithms

MD5 (128-bit)	Broken – do not use
SHA-1 (160-bit)	Deprecated – collision found 2017
SHA-256	Current standard
SHA-3 (Keccak)	Alternative design – sponge construction

Digital Signature Process:

Sender hashes message → Encrypts hash with private key (= signature) → Sends message + signature → Receiver decrypts signature with sender's public key → Compares hashes → Match = authentic and unaltered

How Cryptography Underpins Network Security

TLS 1.3

Secures web (HTTPS), email, VoIP.
AES-GCM + ECDH. Single round-trip.

VPN (IPSec / WireGuard)

Encrypted tunnels. IKE + AES
or ChaCha20 + Curve25519.

WPA3 (Wi-Fi)

SAE/Dragonfly protocol. Forward secrecy; offline attack resistant.

SSH

Encrypted remote access. Ed25519 auth + AES session.

Disk Encryption

BitLocker (Windows), LUKS (Linux), FileVault (macOS). AES-256.

Post-Quantum Cryptography: NIST standardised ML-KEM (Kyber) and ML-DSA (Dilithium) in 2024. Google, Apple, and Cloudflare already deploying hybrid post-quantum key exchanges.

Standards, Regulations, and Laws

ISO 27001

ISMS standard. Requires cryptographic controls policy and key management lifecycle.

PCI DSS v4.0

Mandates AES-256 for stored card data. TLS 1.2+ for transmission. Key rotation.

UK GDPR

Encryption as ‘appropriate technical measure’. Breach exemption if data encrypted.

RIPA Part III

Key disclosure law. Up to 2 years’ imprisonment for non-compliance (5 years for national security).

Non-Compliance Consequences:

- UK GDPR: up to £17.5M or 4% of turnover
- PCI DSS: $5K–$100K/month + loss of card processing
- Reputational damage, legal liability, operational disruption, criminal prosecution

Methods of Attack on Encrypted Data

Cryptographic Attacks

- Brute-force – try every key (56-bit feasible; 128-bit infeasible)
- Dictionary – try common passwords/phrases
- Rainbow table – precomputed hashes (defeated by salting)
- Birthday attack – find hash collisions faster than brute force
- Known/chosen plaintext – deduce key from plaintext-ciphertext pairs

Side-Channel Attacks

- Timing – measure operation time to infer key
- Power analysis – monitor power consumption (SPA/DPA)
- Electromagnetic – capture EM emissions from devices
- Cache timing – Spectre/Meltdown leaked crypto keys
- Social engineering – phishing, coercion (‘rubber hose’ cryptanalysis)

The weakest point in any cryptographic system is often the human — social engineering bypasses all technical controls

Additional Encryption Methods

Homomorphic Encryption

Compute on encrypted data without decrypting. Revolutionary for cloud processing.

Quantum Key Distribution

Uses quantum mechanics for theoretically perfect key distribution (BB84 protocol).

Format-Preserving Encryption

Encrypts while preserving format (16-digit card → 16-digit). NIST: FF1, FF3-1.

Tokenisation

Replaces sensitive data with non-reversible tokens. Widely used in payments.

Attribute-Based Encryption

Access policies embedded in encryption. Fine-grained control by role/attributes.

Confidential Computing: Intel SGX, AMD SEV, ARM TrustZone create encrypted memory enclaves — protecting data in use alongside encryption at rest and in transit.

Key Escrow, Recovery, and Management

Escrow Architectures

- Single agent – one party holds key copy (single point of failure)
- Split-key (Shamir's Secret Sharing) – key split into shares; threshold (e.g. 3-of-5) to reconstruct
- Corporate escrow – BitLocker recovery keys in Active Directory

Key Management Best Practices

- Separate roles – custodians ≠ users
- Dual control – critical ops need 2+ people
- Regular rotation – annual or more frequent
- HSMs – hardware security modules for high-value keys
- Secure destruction – crypto-erase at end-of-life

The Clipper Chip (1993):

The US government proposed a chip with government-escrowed keys for all telecommunications encryption. Abandoned after widespread opposition and a fundamental design flaw discovered by cryptographer Matt Blaze. Remains a cautionary tale of mandatory government key escrow.

Designing an Encryption Plan: 8 Components

1. Scope & Objectives
2. Data Classification
3. Encryption Standards
4. Implementation Plan
5. Key Management
6. Roles & Responsibilities
7. Monitoring & Compliance
8. Quantum Readiness

An encryption plan translates policy into practice — covering data at rest, in transit, and in use across the entire organisation

Key Takeaways

- Cryptography serves four goals: confidentiality, integrity, authentication, and non-repudiation — the foundation of information security
- Symmetric encryption (AES, ChaCha20) is fast for bulk data; asymmetric (RSA, ECC) solves key distribution — hybrid systems combine both
- Block cipher mode matters: GCM provides authenticated encryption; ECB is insecure; always use AES-GCM or ChaCha20-Poly1305
- Hash functions (SHA-256) provide integrity; digital signatures provide authentication and non-repudiation — MD5 and SHA-1 are broken
- TLS 1.3, IPSec, WPA3, SSH, and disk encryption all depend on cryptographic methods to secure communications and data
- UK GDPR recommends encryption; PCI DSS mandates it; RIPA Part III enables compelled key disclosure — compliance is non-negotiable
- Side-channel attacks target physical implementation, not the algorithm — timing, power, EM emissions, and human factors
- An encryption plan covers 8 components: scope, data classification, standards, implementation, key management, roles, monitoring, and quantum readiness