Cryptography

First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 5 Diploma in Cyber Security.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 5 Units

The study guide includes a number of features to enhance your studies:

📝	'Over to you:' activities for you to apply what you have learned.
🌍	'Industry Insights:' discover up-to-date trends, expert opinions, and real-world examples from cryptography practice.
🧭	'Did you know?' highlights interesting facts or surprising information to deepen your understanding.
💼	'Case studies:' realistic scenarios to reinforce and test your understanding.
📱	'Revision on the go:' use your phone camera to capture key pieces of learning and save them as revision notes.
❗	'Need to know:' key pieces of information highlighted in the text.
💡	'Examples:' illustrating points made in the text to show how it works in practice.

Note: Website addresses current as of March 2026.

Level 5 Cryptography

About this unit

This unit aims to provide you with the knowledge and skills needed to understand and apply cryptographic principles in cyber security contexts. Cryptography is the foundation of information security – it protects the confidentiality, integrity, and authenticity of data across every sector, from banking and healthcare to government and defence.

You will study the concept and history of cryptography, explore symmetric and asymmetric encryption methods, examine how cryptographic techniques underpin the security of cyber-enabled networks and devices, and understand the standards and protocols that govern their use. You will analyse the regulatory and legal landscape surrounding encryption, including data protection regulations, export controls, and lawful interception requirements.

You will then develop practical knowledge of attack methods targeting encrypted data, additional encryption techniques, key escrow and recovery principles, and the design of comprehensive encryption plans for organisations.

By the end of this unit, you will have the knowledge to assess cryptographic implementations, evaluate their effectiveness, and design encryption strategies that meet the security needs of modern organisations – capabilities that are essential for careers in information security and that align with professional certifications including CompTIA Security+ and CISSP.

Chapter One – Understanding Cryptographic Principles and Modes

Introduction

This chapter provides the theoretical foundation for cryptography. You will define the concept and application of cryptography, trace its historical evolution from ancient ciphers to modern quantum-resistant algorithms, analyse symmetric and asymmetric encryption in depth, examine hashing and digital signatures, evaluate how cryptographic methods underpin the communications security of cyber-enabled networks and devices, and study the key cryptographic standards and protocols used across industry.

Learning Outcomes

On completing this chapter, you will be able to:

- Understand key cryptographic principles and modes.

Assessment Criteria

1.1 Define the concept and application of cryptography.

1.2 Explain symmetric and asymmetric modes and approaches.

1.3 Assess how cryptographic methods and standards underpin the communications security of cyber-enabled networks and devices.

1.1 The concept and application of cryptography

Over to you – Video Watch: What Is Cryptography?

Watch this YouTube video:

Title: Cryptography: Crash Course Computer Science #33

Channel: CrashCourse

Duration: 12:32

Link: https://www.youtube.com/watch?v=jhXCTbFnK8o

After watching, list the three main goals of cryptography (CIA triad) and explain how encryption, hashing, and digital signatures each contribute to achieving these goals.

Defining Cryptography

Cryptography is the science and practice of securing information by transforming it into an unreadable format (ciphertext) that can only be converted back to its original form (plaintext) by authorised parties who possess the correct key. The word derives from the Greek kryptos (hidden) and graphein (to write).

Cryptography is distinct from, but related to, several other disciplines:

- **Cryptology** – the overarching science encompassing both cryptography (making codes) and cryptanalysis (breaking codes).
- **Cryptanalysis** – the study of methods for defeating cryptographic protections, including code-breaking, side-channel attacks, and mathematical analysis.
- **Steganography** – the practice of hiding the existence of a message (e.g. concealing data within an image file), as opposed to cryptography which hides the meaning of a message.

The CIA Triad and Cryptographic Goals

Cryptography serves four fundamental security objectives, often referred to as the pillars of information security:

- **Confidentiality** – ensuring that information is accessible only to authorised parties. Achieved through encryption (symmetric and asymmetric).
- **Integrity** – ensuring that information has not been altered or tampered with during storage or transmission. Achieved through hashing algorithms and message authentication codes (MACs).
- **Authentication** – verifying the identity of the sender or the origin of data. Achieved through digital signatures, certificates, and challenge-response protocols.
- **Non-repudiation** – ensuring that the sender cannot deny having sent a message. Achieved through digital signatures using asymmetric cryptography.

Core Terminology

Term	Definition
Plaintext	The original, readable data before encryption.
Ciphertext	The scrambled, unreadable output after encryption.
Encryption	The process of converting plaintext into ciphertext using an algorithm and a key.

Decryption	The reverse process of converting ciphertext back into plaintext.
Key	A secret value used by an algorithm to encrypt and/or decrypt data. Security depends on key secrecy and length.
Cipher	An algorithm for performing encryption or decryption.
Algorithm	A defined set of mathematical steps used in encryption (e.g. AES, RSA).
Key space	The total number of possible keys for a given algorithm. Larger key spaces are harder to brute-force.
XOR (Exclusive OR)	A fundamental binary operation used extensively in cryptographic algorithms. Returns 1 when inputs differ, 0 when they match.

Applications of Cryptography

Cryptography is embedded in virtually every aspect of modern digital life:

- **Secure communications** – HTTPS/TLS secures web browsing; end-to-end encryption protects messaging (Signal, WhatsApp); VPNs encrypt network tunnels.
- **Data protection** – full disk encryption (BitLocker, LUKS) protects data at rest; database encryption protects sensitive records.
- **Authentication systems** – password hashing (bcrypt, Argon2) protects stored credentials; Kerberos uses symmetric cryptography for network authentication; multi-factor authentication often relies on cryptographic tokens.
- **Digital commerce** – payment card processing uses encryption throughout; digital certificates verify merchant identity; blockchain and cryptocurrencies are built on cryptographic primitives.
- **Email security** – PGP/GPG and S/MIME provide email encryption and digital signatures.
- **Software integrity** – code signing certificates verify that software has not been tampered with; package managers verify downloads using cryptographic hashes.
- **IoT and embedded devices** – secure boot processes, firmware signing, and encrypted communications protect connected devices.

! Need to know

Kerckhoffs's Principle (1883) states that a cryptographic system should be secure even if everything about the system, except the key, is public knowledge. Modern cryptography follows this principle – the security of AES, RSA, and other algorithms relies on the secrecy of the key, not the secrecy of the algorithm. This is the opposite of 'security through obscurity', which is considered a flawed approach.

1.2 The history and evolution of cryptography

Ancient and Classical Cryptography

- **Scytale (circa 700 BCE)** – used by the Spartans; a strip of parchment wound around a cylinder of a specific diameter to reveal the hidden message. An early form of transposition cipher.
- **Caesar Cipher (circa 50 BCE)** – a substitution cipher where each letter is shifted by a fixed number of positions in the alphabet. Julius Caesar reportedly used a shift of 3. Trivially easy to break but illustrates fundamental cipher concepts.
- **Vigenère Cipher (1553)** – a polyalphabetic substitution cipher using a keyword to determine variable shifts. Considered 'unbreakable' for three centuries until Charles Babbage and Friedrich Kasiski developed cryptanalytic methods against it in the 19th century.
- **Playfair Cipher (1854)** – a digraph substitution cipher that encrypts pairs of letters using a 5×5 matrix. Used by the British military in the Boer War and World War I.

Mechanical and Electromechanical Era

- **Enigma Machine (1920s–1940s)** – the German rotor-based cipher machine used extensively during World War II. Its cryptanalysis by Polish mathematicians (Marian Rejewski) and later by British codebreakers at Bletchley Park (Alan Turing, Gordon Welchman) was pivotal to the Allied war effort and is considered a foundational moment in the history of computing.
- **Lorenz Cipher (1940s)** – a more complex German cipher machine used for high-command communications. Its breaking led to the construction of Colossus, one of the world's first programmable electronic computers.

Modern Cryptography

- **Data Encryption Standard (DES) – 1977** – adopted as a US federal standard. A 56-bit symmetric block cipher that was the workhorse of encryption for two decades before being rendered insecure by advances in computing power.
- **Diffie-Hellman Key Exchange – 1976** – the breakthrough that enabled two parties to establish a shared secret key over an insecure channel without prior communication. This invention launched public key cryptography.
- **RSA – 1977** – developed by Rivest, Shamir, and Adleman, the first practical public key encryption algorithm. Based on the mathematical difficulty of factoring large prime numbers.
- **AES (Advanced Encryption Standard) – 2001** – selected through a NIST public competition to replace DES. The Rijndael algorithm by Belgian cryptographers Joan Daemen and Vincent Rijmen was chosen. AES with 128, 192, or 256-bit keys remains the global standard for symmetric encryption.
- **Elliptic Curve Cryptography (ECC) – 1985/2000s** – proposed independently by Neal Koblitz and Victor Miller. ECC provides equivalent security to RSA with much smaller key sizes, making it ideal for mobile and IoT devices.
- **Post-Quantum Cryptography – 2020s** – NIST has standardised post-quantum algorithms (ML-KEM/CRYSTALS-Kyber for key encapsulation, ML-DSA/CRYSTALS-Dilithium for digital signatures) to protect against future quantum computer attacks.

Did you know?

The work at Bletchley Park during World War II is estimated to have shortened the war by approximately two years and saved millions of lives. The cryptanalysis techniques developed there laid the groundwork for modern computer science and information security. Alan Turing’s theoretical work on computable numbers and his practical codebreaking contributions make him one of the most important figures in both cryptography and computing history.

1.3 Symmetric encryption: algorithms, modes, and applications

Over to you – Video Watch: AES Explained

Watch this YouTube video:

Title: AES Explained (Advanced Encryption Standard) – Computerphile

Channel: Computerphile

Duration: 11:35

Link: https://www.youtube.com/watch?v=O4xNJsjtN6E

After watching, explain the four main operations in each AES round (SubBytes, ShiftRows, MixColumns, AddRoundKey) and why each is necessary for security.

How Symmetric Encryption Works

In symmetric encryption, the same key is used for both encryption and decryption. Both the sender and receiver must possess and protect this shared secret key. Symmetric algorithms are fast, efficient, and suitable for encrypting large volumes of data.

The fundamental challenge of symmetric encryption is key distribution – how do two parties securely share a secret key? This problem is addressed by asymmetric cryptography (Section 1.4), which is often used to securely exchange symmetric keys.

Types of Symmetric Ciphers

Stream ciphers encrypt data one bit or byte at a time, generating a pseudorandom keystream that is XORed with the plaintext. They are fast and suitable for real-time communications. Examples include RC4 (now deprecated due to vulnerabilities) and ChaCha20 (used in modern TLS and WireGuard VPN).

Block ciphers encrypt data in fixed-size blocks (commonly 128 bits). They require a mode of operation to handle messages longer than one block. Examples include AES, DES (deprecated), and 3DES (deprecated).

Key Symmetric Algorithms

Algorithm	Key Size	Status and Notes
DES	56 bits	Deprecated. Cracked by brute force in 1999. Historical significance only.
3DES (Triple DES)	168 bits (effective ~112)	Deprecated by NIST in 2023. Applies DES three times.
AES-128	128 bits	Current standard. Fast, secure, widely deployed globally.
AES-256	256 bits	Highest AES security level. Required for top-secret classifications.
Blowfish	32–448 bits	Replaced by Twofish. Still found in legacy systems.
ChaCha20	256 bits	Modern stream cipher. Used in TLS 1.3 and WireGuard.

Block Cipher Modes of Operation

When encrypting data larger than a single block, a mode of operation determines how blocks are processed. The choice of mode affects security, performance, and error propagation:

- **ECB (Electronic Codebook)** – each block encrypted independently. Insecure because identical plaintext blocks produce identical ciphertext blocks, revealing patterns. Never use for encryption in production.
- **CBC (Cipher Block Chaining)** – each block is XORed with the previous ciphertext block before encryption. Requires an Initialisation Vector (IV). Widely used but vulnerable to padding oracle attacks (e.g. POODLE).
- **CTR (Counter Mode)** – turns a block cipher into a stream cipher by encrypting incrementing counter values and XORing with plaintext. Parallelisable and efficient.
- **GCM (Galois/Counter Mode)** – combines CTR mode encryption with Galois authentication, providing both confidentiality and integrity (authenticated encryption). AES-GCM is the recommended mode for TLS 1.3.
- **CCM (Counter with CBC-MAC)** – another authenticated encryption mode, combining CTR for encryption with CBC-MAC for authentication. Used in wireless security (WPA2).

💡 **Example – Why ECB Mode Is Insecure**

The classic demonstration of ECB's weakness is the 'ECB Penguin': when a bitmap image of the Linux penguin (Tux) is encrypted using ECB mode, the outline of the penguin remains clearly visible in the ciphertext image because identical blocks of colour produce identical ciphertext blocks. Using CBC or CTR mode, the encrypted image appears as random noise. This dramatically illustrates why the choice of mode of operation matters as much as the choice of algorithm.

1.4 Asymmetric encryption: public key cryptography

Over to you – Video Watch: Public Key Cryptography

Watch this YouTube video:

Title: Public Key Cryptography – Computerphile

Channel: Computerphile

Duration: 6:20

Link: https://www.youtube.com/watch?v=GSIDS_lvRv4

After watching, explain the difference between public and private keys and describe a scenario where asymmetric encryption solves a problem that symmetric encryption cannot.

How Asymmetric Encryption Works

Asymmetric (public key) cryptography uses a mathematically linked pair of keys: a public key that can be freely shared and a private key that must be kept secret. Data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa.

The mathematical foundations rely on problems that are computationally easy in one direction but extremely difficult to reverse:

- **Integer factorisation** – it is easy to multiply two large primes together but extremely difficult to factor the resulting product back into its prime components. RSA is based on this problem.
- **Discrete logarithm problem** – in modular arithmetic, computing a^b mod p is easy, but finding b given a, a^b mod p, and p is computationally infeasible. Diffie-Hellman and DSA are based on this.
- **Elliptic curve discrete logarithm** – analogous to the discrete logarithm problem but over elliptic curves. Provides equivalent security with much smaller keys. ECDSA, ECDH, and Ed25519 are based on this.

Key Asymmetric Algorithms

Algorithm	Use Case	Notes
RSA	Encryption, digital signatures, key exchange	Key sizes: 2048, 3072, 4096 bits. Widely used but computationally expensive.
Diffie-Hellman (DH)	Key exchange only	Enables two parties to establish a shared secret over an insecure channel.
ECDH	Key exchange	Elliptic curve variant of DH. Smaller keys, faster, used in TLS.
ECDSA / EdDSA	Digital signatures	Used in TLS, SSH, Bitcoin, and code signing. Ed25519 is the modern standard.
ElGamal	Encryption, signatures	Based on DH. Used in PGP encryption.
ML-KEM (Kyber)	Post-quantum key encapsulation	NIST-standardised in 2024 for quantum-resistant key exchange.

Symmetric vs Asymmetric: Comparison

Feature	Symmetric	Asymmetric
Keys	Single shared key	Key pair (public + private)
Speed	Very fast	Much slower (100–1000x)
Key distribution	Difficult (must share secretly)	Easy (public key can be shared openly)
Key sizes	128–256 bits	2048–4096 bits (RSA) or 256–521 bits (ECC)
Use cases	Bulk data encryption	Key exchange, digital signatures, authentication
Examples	AES, ChaCha20	RSA, ECDH, Ed25519

Hybrid Encryption

In practice, most systems use hybrid encryption – combining the strengths of both approaches. Asymmetric encryption is used to securely exchange a symmetric session key, and that session key is then used for fast, efficient bulk data encryption. This is how TLS/HTTPS, SSH, PGP, and most modern secure communications work.

Did you know?

The Diffie-Hellman key exchange was published in 1976 by Whitfield Diffie and Martin Hellman. However, the concept was independently discovered several years earlier by British cryptographers James Ellis, Clifford Cocks, and Malcolm Williamson at GCHQ, but their work was classified until 1997. Cocks also independently invented what became known as the RSA algorithm, years before Rivest, Shamir, and Adleman published theirs.

1.5 Hashing algorithms and digital signatures

Cryptographic Hash Functions

A cryptographic hash function takes an input of any length and produces a fixed-length output (the hash, or digest) with the following critical properties:

- **Deterministic** – the same input always produces the same hash.
- **One-way (pre-image resistance)** – it is computationally infeasible to reverse the hash to find the original input.
- **Collision resistance** – it is infeasible to find two different inputs that produce the same hash.
- **Avalanche effect** – a small change in the input (even a single bit) produces a dramatically different hash.

Common Hashing Algorithms

Algorithm	Output Size	Status
MD5	128 bits	Broken – collision attacks demonstrated. Do not use for security.
SHA-1	160 bits	Deprecated – practical collision found in 2017 (SHAttered attack).
SHA-256	256 bits	Current standard. Part of SHA-2 family. Widely used in TLS, Bitcoin, code signing.
SHA-512	512 bits	Part of SHA-2 family. Used where higher security margins are needed.
SHA-3 (Keccak)	224–512 bits	NIST standard since 2015. Alternative design to SHA-2. Sponge construction.
BLAKE2 / BLAKE3	Variable	Modern, very fast hashing. Used in password managers, file integrity tools.

Applications of Hashing

- **Password storage** – passwords are hashed (with salt) before storage using specialised algorithms like bcrypt, scrypt, or Argon2. If the database is breached, attackers obtain hashes, not plaintext passwords.
- **Data integrity verification** – software downloads provide SHA-256 checksums so users can verify the file has not been tampered with.
- **Message Authentication Codes (MACs)** – HMAC (Hash-based Message Authentication Code) combines a hash function with a secret key to verify both the integrity and authenticity of a message.
- **Blockchain** – hash chains link blocks together; mining involves computing SHA-256 hashes.
- **Digital forensics** – hashing evidence files ensures chain-of-custody integrity.

Digital Signatures

A digital signature uses asymmetric cryptography to provide authentication, integrity, and non-repudiation. The process works as follows:

- The sender creates a hash of the message.

- The sender encrypts the hash with their private key – this is the digital signature.
- The sender transmits the message along with the signature.
- The receiver decrypts the signature using the sender's public key to obtain the hash.
- The receiver independently hashes the received message and compares the two hashes.
- If they match, the message is authentic and unaltered.

Digital Certificates and PKI

A digital certificate binds a public key to an identity (person, organisation, or server). Certificates are issued by Certificate Authorities (CAs) and form the basis of Public Key Infrastructure (PKI). The X.509 standard defines the format for certificates. When you visit an HTTPS website, your browser verifies the server's digital certificate against a list of trusted CAs to ensure you are communicating with the genuine server.

Over to you – Certificate Inspection

Open your web browser and navigate to any HTTPS website (e.g. https://www.google.com). Click the padlock icon in the address bar and inspect the site's digital certificate. Identify: (1) the certificate issuer (CA), (2) the subject (who the certificate was issued to), (3) the validity period, (4) the public key algorithm and key size, (5) the signature algorithm. Explain how each element contributes to secure communication.

1.6 How cryptographic methods underpin network and device security

Cryptography is the foundation upon which the security of modern networks and devices is built. This section examines the key protocols and implementations.

Transport Layer Security (TLS)

TLS (the successor to SSL) is the most widely deployed cryptographic protocol, securing web traffic, email, VoIP, and many other communications. The TLS 1.3 handshake (standardised in 2018) works as follows:

- Client sends a ClientHello with supported cipher suites and a key share (e.g. ECDH parameters).
- Server responds with chosen cipher suite and its key share.
- Both parties derive the shared session key from the key exchange.
- The server sends its certificate and a signature proving possession of its private key.
- Symmetric encryption (typically AES-256-GCM or ChaCha20-Poly1305) begins using the session key.

TLS 1.3 removed support for insecure algorithms (RC4, DES, 3DES, static RSA key exchange) and reduced the handshake to a single round trip, improving both security and performance.

Virtual Private Networks (VPNs)

VPN protocols use cryptography to create encrypted tunnels:

- **IPSec** – operates at the network layer. Uses IKE (Internet Key Exchange) for key negotiation, AES for encryption, and HMAC for integrity. Used in site-to-site and remote access VPNs.
- **WireGuard** – a modern, lightweight VPN protocol using ChaCha20 for encryption, Poly1305 for authentication, BLAKE2s for hashing, and Curve25519 for key exchange.
- **OpenVPN** – uses TLS for key exchange and AES for data encryption. Highly configurable and widely deployed.

Wireless Security

- **WPA2 (Wi-Fi Protected Access 2)** – uses AES-CCMP for encryption. The standard for wireless security since 2004.
- **WPA3 (2018)** – introduces Simultaneous Authentication of Equals (SAE/Dragonfly) to replace the PSK 4-way handshake, providing forward secrecy and protection against offline dictionary attacks.

Disk and Device Encryption

- **BitLocker (Windows)** – full-volume encryption using AES-128 or AES-256. Uses Trusted Platform Module (TPM) for key protection.
- **LUKS (Linux)** – Linux Unified Key Setup. Provides full disk encryption using dm-crypt with AES.
- **FileVault (macOS)** – full disk encryption using AES-XTS-128.
- **Mobile device encryption** – modern iOS and Android devices encrypt all data by default, using AES with keys derived from the device passcode and hardware-bound keys.

Secure Shell (SSH)

SSH provides encrypted remote access to servers. It uses asymmetric cryptography for authentication (public key authentication with Ed25519 or RSA keys), Diffie-Hellman or ECDH for key exchange, and AES or ChaCha20 for session encryption.

DNS Security (DNSSEC)

DNSSEC adds cryptographic signatures to DNS records, enabling resolvers to verify that DNS responses have not been tampered with. It uses RSA or ECDSA digital signatures to protect the integrity and authenticity of DNS data, defending against cache poisoning and man-in-the-middle attacks.

🌍 Industry Insight – Post-Quantum Cryptography

Quantum computers, when sufficiently powerful, could break RSA and ECC by efficiently solving the mathematical problems they rely on (Shor's Algorithm). NIST finalised the first post-quantum cryptographic standards in 2024: ML-KEM (CRYSTALS-Kyber) for key encapsulation and ML-DSA (CRYSTALS-Dilithium) for digital signatures. Major technology companies including Google, Apple, and Cloudflare have already begun deploying post-quantum hybrid key exchanges in their products. The transition to post-quantum cryptography is one of the most significant challenges facing information security today. Explore: https://csrc.nist.gov/projects/post-quantum-cryptography

1.7 Cryptographic standards and protocols

Cryptographic standards ensure interoperability, security, and trust across systems and organisations:

Key Standards Bodies

- **NIST (National Institute of Standards and Technology)** – publishes Federal Information Processing Standards (FIPS) including FIPS 197 (AES), FIPS 180-4 (SHA-2), FIPS 186-5 (Digital Signature Standard), and FIPS 140-3 (security requirements for cryptographic modules).
- **IETF (Internet Engineering Task Force)** – publishes RFCs defining internet protocols including TLS (RFC 8446), SSH, IPSec, DNSSEC, and certificate standards.
- **ISO/IEC** – ISO/IEC 27001 (information security management) and ISO/IEC 19790 (cryptographic module requirements).
- **PCI DSS (Payment Card Industry Data Security Standard)** – mandates encryption requirements for organisations handling payment card data, including TLS 1.2 or higher for data in transit and strong encryption for stored cardholder data.

FIPS 140-3

FIPS 140-3 is the current standard for validating cryptographic modules. It defines four increasing security levels:

- **Level 1** – basic requirements; at least one approved algorithm.
- **Level 2** – adds tamper-evident seals and role-based authentication.
- **Level 3** – adds tamper-resistant physical security and identity-based authentication.
- **Level 4** – highest security; environmental failure protection.

Common Criteria (ISO/IEC 15408)

An international framework for evaluating the security of IT products, including cryptographic implementations. Products are evaluated against Security Targets and assigned Evaluation Assurance Levels (EAL 1–7).

Over to you – Standards Research

Research and create a comparison table of FIPS 140-3 and Common Criteria. For each standard, identify: (1) the issuing body, (2) the scope (what it covers), (3) the security levels defined, (4) examples of products certified under each standard, and (5) which industries or sectors commonly require each certification. Present your findings in a 400-word report.

Reading List

- Aumasson, J.-P. (2021) Serious cryptography: a practical introduction to modern encryption. 2nd edn. San Francisco: No Starch Press.
- Katz, J. and Lindell, Y. (2021) Introduction to modern cryptography. 3rd edn. Boca Raton: CRC Press.
- Paar, C. and Pelzl, J. (2024) Understanding cryptography: a textbook for students and practitioners. 2nd edn. Berlin: Springer.
- Smart, N.P. (2022) Cryptography made simple. 2nd edn. Cham: Springer.

- Stallings, W. (2022) Cryptography and network security: principles and practice. 8th edn. Harlow: Pearson.
- Wong, D. (2021) Real-world cryptography. Shelter Island: Manning Publications.

Summary

In this chapter, you have developed a comprehensive understanding of cryptographic principles and modes. You have defined cryptography, its goals, and its applications across modern digital systems. You have traced the evolution of cryptography from ancient ciphers to post-quantum algorithms.

You have analysed symmetric encryption in depth, including algorithms (AES, ChaCha20), modes of operation (ECB, CBC, CTR, GCM), and their appropriate use cases. You have studied asymmetric cryptography, including RSA, Diffie-Hellman, and elliptic curve algorithms, and understand how hybrid encryption combines both approaches.

You have examined hashing algorithms and digital signatures, and how they provide integrity, authentication, and non-repudiation. You have evaluated how cryptographic methods underpin the security of networks and devices through protocols including TLS, IPSec, SSH, and wireless security. Finally, you have studied the key cryptographic standards and certification frameworks.

Chapter Two – Standards, Regulations, and Laws Governing Encryption

Introduction

This chapter examines the regulatory and legal landscape surrounding encryption. You will study the key data protection standards and frameworks, analyse UK and international encryption regulations, explore the legal domains of lawful interception, export controls, and key disclosure, and evaluate the consequences of non-compliance for organisations and individuals.

Learning Outcomes

On completing this chapter, you will be able to:

- Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption.

Assessment Criteria

4.1 Explain the key principles of the related standards, regulations and laws and why they are in place.

4.2 Assess the consequences for organisations and individuals of non-compliance with these standards, regulations and laws.

2.1 Key data protection standards and frameworks

ISO/IEC 27001 and the ISO 27000 Family

ISO/IEC 27001 is the international standard for information security management systems (ISMS). It requires organisations to assess risks and implement appropriate controls, including cryptographic controls. ISO/IEC 27002 provides detailed guidance on implementing these controls, with specific sections on:

- Cryptographic controls policy – establishing organisational rules for the use of cryptography.
- Key management – covering the full lifecycle of cryptographic keys: generation, distribution, storage, rotation, revocation, and destruction.
- The use of encryption for protecting data at rest, in transit, and in use.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS is mandatory for any organisation that processes, stores, or transmits payment card data. Its encryption requirements include:

- Requirement 3: Protect stored account data using strong cryptography (AES-256 recommended).
- Requirement 4: Encrypt transmission of cardholder data across open, public networks using TLS 1.2 or higher.
- Requirement 3.5: Protect cryptographic keys used for encryption of stored data, including key management procedures.
- PCI DSS v4.0 (effective March 2025) strengthens requirements for key rotation, algorithm selection, and monitoring.

NIST Cybersecurity Framework (CSF) and Special Publications

- **NIST CSF 2.0 (2024)** – the updated framework includes cryptography within the Protect function, emphasising encryption for data protection.
- **NIST SP 800-175B** – guideline for using cryptographic standards (comprehensive guidance on algorithm selection).
- **NIST SP 800-57** – recommendation for key management (three parts covering key management practices, best practices for organisations, and application-specific guidance).
- **NIST SP 800-131A** – transitions for cryptographic algorithms and key lengths (defines which algorithms are acceptable, deprecated, or disallowed).

Cyber Essentials and Cyber Essentials Plus (UK)

The UK government-backed Cyber Essentials scheme requires organisations to implement basic security controls, including the use of encryption. Cyber Essentials Plus includes verified testing of controls. While not prescriptive about specific algorithms, the scheme requires encryption of data in transit and increasingly recommends encryption at rest.

📝 **Over to you – Video Watch: Understanding End-to-End Encryption and Data Protection**

Watch this YouTube video:

Title: End to End Encryption (E2EE) – Computerphile

Channel: Computerphile

Duration: 12:42
Link: https://www.youtube.com/watch?v=jkV1KEJGKRA
After watching, explain how end-to-end encryption protects user data and describe three scenarios where encryption supports GDPR compliance requirements.

2.2 UK and international encryption regulations

UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

The UK GDPR does not specifically mandate encryption, but Article 32 requires organisations to implement 'appropriate technical and organisational measures' to secure personal data, and explicitly lists encryption as an example. The ICO (Information Commissioner's Office) strongly recommends encryption as a key security measure, particularly for:

- Personal data stored on portable devices (laptops, USB drives, smartphones).
- Personal data transmitted over public networks.
- Sensitive personal data (special category data under Article 9).

The Data (Use and Access) Act 2025, enacted on 19 June 2025, modernises the UK's data protection framework with targeted amendments to the UK GDPR. It retains encryption as a recommended technical measure and strengthens the ICO's enforcement powers.

EU General Data Protection Regulation (EU GDPR)

The EU GDPR (Regulation 2016/679) similarly references encryption as an appropriate technical measure under Article 32. Article 34 provides a significant incentive: if a data breach occurs but the affected data was encrypted with a method that renders it unintelligible to unauthorised persons, the organisation may be exempt from notifying affected individuals.

US Encryption Regulations

- **HIPAA (Health Insurance Portability and Accountability Act)** – requires encryption as an 'addressable' safeguard for electronic protected health information (ePHI). If encryption is not implemented, organisations must document why an equivalent measure is used.
- **GLBA (Gramm-Leach-Bliley Act)** – requires financial institutions to protect customer information, with encryption being a primary recommended measure.
- **SOX (Sarbanes-Oxley Act)** – requires protection of financial reporting data, with encryption commonly used to meet its security requirements.
- **State laws** – many US states have data breach notification laws that provide a 'safe harbour' exemption if breached data was encrypted (e.g. California Consumer Privacy Act).

International Frameworks

- **eIDAS Regulation (EU)** – establishes a legal framework for electronic identification and trust services, including qualified electronic signatures that have the legal equivalent of handwritten signatures.
- **NIS2 Directive (EU, 2024)** – the updated Network and Information Security Directive requires essential and important entities to implement cryptographic measures as part of their cybersecurity risk management.

2.3 Legal domains: lawful interception, export controls, and key disclosure

Lawful Interception

Governments worldwide maintain the legal authority to intercept communications under certain circumstances. This creates a fundamental tension between individual privacy (protected by encryption) and law enforcement and national security needs:

- **UK Investigatory Powers Act 2016 ('Snoopers' Charter')** – grants law enforcement and intelligence agencies powers to require communications service providers to assist with interception. Technical Capability Notices (TCNs) can require providers to maintain the ability to remove encryption they have applied. The Act has sparked significant debate about its implications for end-to-end encryption.
- **US Communications Assistance for Law Enforcement Act (CALEA)** – requires telecommunications carriers to ensure their systems can comply with lawful interception orders.
- **The 'Going Dark' debate** – the ongoing tension between law enforcement agencies (who argue encryption hinders criminal investigations) and privacy advocates and technologists (who argue that weakening encryption undermines everyone's security).

Export Controls

Cryptographic software and hardware are subject to export controls in many countries:

- **Wassenaar Arrangement** – a multilateral export control regime with 42 participating states. Dual-use cryptographic products are included in its control lists. Mass-market encryption products (e.g. web browsers) are generally exempt.
- **US Export Administration Regulations (EAR)** – the Bureau of Industry and Security (BIS) controls the export of encryption technology. Products using encryption above certain thresholds require export licences or classification reviews.
- **Historical context** – during the 1990s 'Crypto Wars', the US classified strong encryption as a munition and severely restricted exports. These restrictions were largely relaxed in 2000, but the debate continues.

Key Disclosure Laws

- **UK Regulation of Investigatory Powers Act 2000 (RIPA), Part III** – allows authorities to serve a notice requiring an individual to disclose an encryption key or provide plaintext data. Failure to comply is a criminal offence, carrying a maximum penalty of 2 years' imprisonment (5 years in cases involving national security or child indecency).
- **Other jurisdictions** – Australia (Telecommunications and Other Legislation Amendment Act 2018), France, India, and others have varying key disclosure or decryption assistance requirements.

💼 Case Study – The Encryption Debate

In 2016, the FBI demanded that Apple create a modified version of iOS to bypass the encryption on an iPhone used by the San Bernardino shooter. Apple refused, arguing that creating such a tool would compromise the security of all iPhone users.

Task: Research this case and write a 500-word analysis covering: (1) the legal arguments on both sides, (2) the technical implications of creating a 'backdoor', (3) the eventual outcome, and (4) your assessment of the appropriate balance between

encryption and lawful access. Consider the implications for both individual privacy and public safety.

2.4 Consequences of non-compliance

Organisations and individuals face severe consequences for failing to comply with encryption-related standards, regulations, and laws:

Regulatory Penalties

- **UK GDPR / Data Protection Act 2018** – the ICO can impose fines of up to £17.5 million or 4% of annual global turnover, whichever is higher. The ICO has issued significant fines for data breaches where encryption was not adequately implemented.
- **EU GDPR** – fines of up to €20 million or 4% of annual global turnover.
- **PCI DSS** – non-compliance can result in fines of $5,000–$100,000 per month, increased transaction fees, and loss of the ability to process card payments.
- **HIPAA** – penalties range from $100 to $50,000 per violation, up to $1.5 million per year for repeated violations.

Reputational Damage

Data breaches involving unencrypted personal data cause significant reputational harm. Public notification requirements under the UK GDPR (Article 34) and equivalent laws mean that breaches become public knowledge, leading to loss of customer trust, negative media coverage, and long-term brand damage.

Operational Consequences

- Business disruption during breach investigation and remediation.
- Cost of breach response: forensic investigation, legal fees, customer notification, credit monitoring services.
- Loss of contracts and business relationships, particularly in sectors requiring PCI DSS or ISO 27001 compliance.
- Regulatory enforcement notices requiring specific remedial actions.

Criminal Liability

- **RIPA Part III** – failure to disclose encryption keys when served with a valid notice: up to 2 years' imprisonment (5 years for national security/child indecency cases).
- **Computer Misuse Act 1990 (UK)** – using encryption to facilitate unauthorised access to computer systems or data.
- **Data Protection Act 2018** – knowingly or recklessly obtaining, disclosing, or retaining personal data without consent is a criminal offence.

> 💡 **Example – Real-World Enforcement**
>
> In 2020, British Airways was fined £20 million by the ICO following a data breach affecting 400,000 customers. The investigation found inadequate security measures, including insufficient encryption of personal data. While the initial proposed fine was £183 million, it was reduced due to the economic impact of COVID-19 and mitigating factors. This case illustrates that regulators consider the adequacy of encryption as a key factor in determining both liability and the severity of penalties.

Reading List

- Calder, A. and Watkins, S. (2024) IT governance: an international guide to data security and ISO 27001/ISO 27002. 8th edn. London: Kogan Page.
- ICO (2025) Encryption and data protection guidance. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/ (Accessed: 15 March 2026).
- NIST (2024) Cybersecurity framework 2.0. Available at: https://www.nist.gov/cyberframework (Accessed: 15 March 2026).
- PCI Security Standards Council (2024) PCI DSS v4.0. Available at: https://www.pcisecuritystandards.org/ (Accessed: 15 March 2026).
- Voigt, P. and von dem Bussche, A. (2024) The EU General Data Protection Regulation (GDPR): a practical guide. 2nd edn. Cham: Springer.

Summary

In this chapter, you have examined the key standards, regulations, and laws governing encryption. You have studied ISO 27001, PCI DSS, NIST frameworks, and Cyber Essentials. You have analysed the UK GDPR, EU GDPR, and international encryption regulations.

You have explored the legal domains of lawful interception, export controls, and key disclosure, understanding the tensions between privacy and law enforcement. You have evaluated the consequences of non-compliance, including regulatory penalties, reputational damage, operational impact, and criminal liability.

Chapter Three – Designing an Encryption Plan

Introduction

This chapter is the practical heart of the unit. You will analyse the methods of attack used against encrypted data, evaluate additional encryption methods, examine key escrow and recovery principles, assess the importance of robust encryption arrangements, learn to evaluate existing encryption implementations, and design a comprehensive encryption plan for an organisation.

Learning Outcomes

On completing this chapter, you will be able to:

- Design an encryption plan and courses of action for a given organisation.

Assessment Criteria

3.1 Explain the methods of attack used to target encrypted data.

3.2 Assess the additional encryption methods available.

3.3 Explain the key principles of escrow and recovery.

3.4 Explain the importance of having robust encryption arrangements within IT systems.

3.5 Evaluate the existing encryption arrangements.

3.6 Design an encryption plan to meet the needs of a given organisation, with recommended courses of actions.

3.1 Methods of attack used to target encrypted data

Over to you – Video Watch: How Encryption Is Attacked

Watch this YouTube video:

Title: Secret Key Exchange (Diffie-Hellman) – Computerphile

Channel: Computerphile

Duration: 8:40

Link: https://www.youtube.com/watch?v=NmM9HA2MQGI

After watching, explain how key exchange enables secure communication and describe why a man-in-the-middle attack could compromise this process. Then consider why attacking the human element is often more practical than attacking the cryptographic algorithm itself.

Direct Cryptographic Attacks

- **Brute-force attack** – systematically trying every possible key until the correct one is found. The feasibility depends on key length: a 56-bit DES key can be brute-forced in hours; a 128-bit AES key would take billions of years with current technology.
- **Dictionary attack** – trying commonly used passwords or phrases. Effective against weak passwords used to derive encryption keys.
- **Rainbow table attack** – using precomputed tables of hash values to reverse hashes. Defeated by the use of salt (random data added to each password before hashing).
- **Birthday attack** – exploiting the mathematics of the birthday paradox to find hash collisions more efficiently than brute force. A hash function with n-bit output has collision resistance of approximately n/2 bits.
- **Known-plaintext attack** – the attacker has both the plaintext and corresponding ciphertext and uses these to deduce the key or break subsequent encryptions.
- **Chosen-plaintext / chosen-ciphertext attack** – the attacker can encrypt/decrypt chosen messages and analyse the results to extract the key.
- **Frequency analysis** – analysing the frequency distribution of characters in ciphertext to break substitution ciphers. Not effective against modern algorithms.

Side-Channel Attacks

Side-channel attacks exploit information leaked by the physical implementation of a cryptographic system, rather than attacking the algorithm itself:

- **Timing attacks** – measuring the time taken by cryptographic operations to infer information about the key. For example, if comparing a password takes longer when more characters match, an attacker can deduce the password character by character.
- **Power analysis** – monitoring the power consumption of a device during cryptographic operations. Simple Power Analysis (SPA) and Differential Power Analysis (DPA) can extract keys from smart cards and embedded devices.
- **Electromagnetic analysis** – capturing electromagnetic emissions from a device to extract cryptographic keys.
- **Cache timing attacks** – exploiting variations in cache access times. The Spectre and Meltdown vulnerabilities (2018) demonstrated that CPU speculative execution could leak cryptographic keys through cache timing.
- **Acoustic cryptanalysis** – analysing sounds produced by computers during cryptographic operations to extract keys.

Implementation Attacks

- **Padding oracle attack** – exploits error messages from decryption systems that reveal whether padding is valid. The POODLE attack (2014) used this against SSL 3.0 and CBC mode.
- **Key reuse vulnerabilities** – using the same key or nonce for multiple encryptions can catastrophically weaken security (e.g. WEP's IV reuse led to trivial cracking of Wi-Fi encryption).
- **Random number generator weaknesses** – if the source of randomness for key generation is predictable, the resulting keys can be guessed. The Debian OpenSSL vulnerability (2008) reduced the key space to only 32,768 possibilities.

Social Engineering and Human Factors

- **Phishing** – tricking users into revealing passwords or encryption keys.
- **Rubber hose cryptanalysis** – coercing key holders through threats or force (the humorous term highlights that the weakest point in any cryptographic system is often the human).
- **Insider threats** – authorised users who misuse their access to encrypted data.
- **Shoulder surfing / keylogging** – capturing passwords or keys as they are entered.

3.2 Additional encryption methods

Homomorphic Encryption

Homomorphic encryption allows computations to be performed directly on encrypted data without decrypting it first. The result, when decrypted, matches the result of performing the same computations on the plaintext. This is revolutionary for cloud computing and outsourced data processing, as it allows organisations to process sensitive data without ever exposing it. Fully Homomorphic Encryption (FHE) supports arbitrary computations but remains computationally expensive. Partially homomorphic and somewhat homomorphic schemes are more practical for specific use cases.

Quantum Key Distribution (QKD)

QKD uses principles of quantum mechanics to distribute encryption keys with theoretically perfect security. Any attempt to eavesdrop on the quantum channel disturbs the quantum states, alerting the communicating parties. BB84 (developed by Bennett and Brassard in 1984) is the foundational QKD protocol. QKD networks are already operational in limited deployments (e.g. between financial institutions and government agencies), though they require specialised hardware and are limited by distance.

Format-Preserving Encryption (FPE)

FPE encrypts data while preserving its format (e.g. a 16-digit credit card number remains a 16-digit number after encryption). This is valuable in legacy systems where database schemas, validation rules, and application logic expect data in a specific format. NIST has approved FF1 and FF3-1 as FPE standards.

Searchable Encryption

Allows searches to be performed on encrypted data without decrypting it. This enables encrypted databases to respond to queries while keeping the underlying data protected. Techniques include searchable symmetric encryption (SSE) and order-preserving encryption (OPE).

Tokenisation

While not strictly encryption, tokenisation replaces sensitive data with non-sensitive tokens that have no mathematical relationship to the original data. A token vault maps tokens back to original values. Widely used in payment processing (replacing credit card numbers with tokens) and healthcare. Unlike encryption, tokenisation cannot be reversed without access to the token vault.

Attribute-Based Encryption (ABE)

ABE allows access policies to be embedded within the encryption itself. Data can only be decrypted by users whose attributes (e.g. department, clearance level, role) match the embedded policy. This enables fine-grained access control without managing individual keys.

Industry Insight – Confidential Computing

Confidential computing protects data in use by performing computation within hardware-based Trusted Execution Environments (TEEs). Technologies like Intel SGX, AMD SEV, and ARM TrustZone create encrypted memory enclaves where even the operating system and hypervisor cannot access the data being processed. Combined with encryption at rest and in transit, confidential computing provides protection throughout

the entire data lifecycle – a concept known as ‘always encrypted’ or ‘encrypt everything’. Major cloud providers (Azure, GCP, AWS) now offer confidential computing services.

3.3 Key escrow and recovery principles

What Is Key Escrow?

Key escrow is an arrangement where cryptographic keys are held in trust by a third party (the escrow agent). In the event that the key holder is unavailable, incapacitated, or under legal obligation, the escrowed keys can be retrieved to decrypt the data.

Key Escrow Architectures

- **Single escrow agent** – one trusted third party holds a copy of the key. Simple but creates a single point of failure and a high-value target for attackers.
- **Split-key escrow** – the key is split into multiple shares using a scheme such as Shamir's Secret Sharing. Each share is held by a different escrow agent. A threshold number of shares (e.g. 3 of 5) must be combined to reconstruct the key. This provides resilience against both loss and compromise.
- **Corporate key escrow** – organisations maintain internal escrow of encryption keys (e.g. BitLocker recovery keys stored in Active Directory). This ensures business continuity if an employee leaves or forgets their password.

Key Recovery

Key recovery is the broader process of regaining access to encrypted data when the original key is lost or unavailable. Key recovery mechanisms include:

- Recovery keys – a secondary key stored securely that can decrypt the data (e.g. BitLocker recovery keys, FileVault recovery keys).
- Key backup – maintaining encrypted copies of keys in a secure key management system (KMS).
- Hardware Security Modules (HSMs) – dedicated hardware devices that securely generate, store, and manage cryptographic keys. HSMs are tamper-resistant and provide FIPS 140-3 validated security.
- Key Management Interoperability Protocol (KMIP) – a standard protocol for managing cryptographic keys across different vendors and systems.

The Clipper Chip Controversy

The most famous key escrow proposal was the US government's Clipper Chip (1993), which would have required a government-escrowed key in all telecommunications encryption. The proposal was abandoned after widespread opposition from privacy advocates, civil liberties organisations, and the technology industry. Cryptographer Matt Blaze also discovered a fundamental flaw in the Clipper Chip's design that allowed the escrow mechanism to be bypassed. The Clipper Chip remains a cautionary example of the risks of government-mandated key escrow.

Best Practices for Key Management

- Separate roles: key custodians should not be the same individuals who use the keys.
- Dual control: critical key management operations should require two or more authorised individuals.
- Key rotation: keys should be changed regularly (rotation periods depend on the sensitivity of the data and the volume of data encrypted).
- Key destruction: when keys reach end-of-life, they must be securely destroyed using methods appropriate to the storage medium.
- Audit trails: all key management operations should be logged and monitored.

Over to you – Key Management Policy

Write a key management policy for a medium-sized financial services company. Your policy should cover: (1) key generation (algorithms, key lengths, randomness sources), (2) key distribution (methods, secure channels), (3) key storage (HSMs, software-based, backup procedures), (4) key rotation schedule, (5) key escrow and recovery procedures, (6) key destruction, and (7) roles and responsibilities. Present as a formal policy document of approximately 600 words.

3.4 The importance of robust encryption arrangements

Robust encryption arrangements are essential for organisations of all sizes. The consequences of weak or absent encryption have been demonstrated repeatedly through high-profile data breaches.

Protection Against Data Breaches

Encryption is the last line of defence. Even if perimeter security, access controls, and monitoring fail, properly encrypted data remains unreadable to unauthorised parties. This significantly reduces the impact of a breach.

Regulatory Compliance

As examined in Chapter Two, numerous regulations require or strongly recommend encryption. Organisations that fail to implement adequate encryption face regulatory penalties, mandatory breach notifications, and enforcement actions.

Customer and Stakeholder Trust

Customers increasingly expect organisations to protect their data. Demonstrating strong encryption practices – through certifications (ISO 27001, SOC 2), compliance reports, and transparent privacy policies – builds trust and can be a competitive differentiator.

Intellectual Property Protection

For many organisations, intellectual property (trade secrets, research data, proprietary algorithms, product designs) is their most valuable asset. Encryption protects this data from competitors, nation-state espionage, and insider threats.

Defence in Depth

Encryption should be part of a layered security strategy (defence in depth) that includes:

- Encryption at rest – protecting stored data (databases, files, backups).
- Encryption in transit – protecting data moving across networks (TLS, VPN, SSH).
- Encryption in use – protecting data during processing (confidential computing, TEEs).
- End-to-end encryption – protecting data from sender to receiver with no intermediary access.

3.5 Evaluating existing encryption arrangements

Before designing a new encryption plan, it is essential to evaluate the organisation's current cryptographic posture:

Encryption Audit Framework

- **Inventory** – catalogue all systems, applications, databases, and communication channels. For each, document: what data is processed, whether encryption is applied, the algorithm and key length used, the mode of operation, and the key management procedures.
- **Algorithm assessment** – identify any deprecated or weak algorithms still in use (DES, 3DES, RC4, MD5, SHA-1, RSA < 2048 bits). These represent immediate risks.
- **Key management review** – assess key generation (quality of randomness), distribution (secure channels?), storage (HSMs vs. software?), rotation (regular schedule?), and destruction procedures.
- **Protocol assessment** – verify that TLS 1.2 or 1.3 is used (not SSL or TLS 1.0/1.1). Check cipher suite configurations for strong choices (AES-GCM, ChaCha20-Poly1305). Verify certificate management and validity.
- **Compliance mapping** – map current encryption practices against applicable regulatory requirements (UK GDPR, PCI DSS, ISO 27001, sector-specific regulations).
- **Gap analysis** – identify gaps between current practices and best practice or regulatory requirements. Prioritise gaps by risk severity.

Tools for Encryption Assessment

- **SSL Labs (ssllabs.com)** – free online tool for testing TLS configuration of web servers. Provides a letter grade (A+ to F) and detailed analysis.
- **testssl.sh** – open-source command-line tool for testing TLS/SSL encryption on any server.
- **Nmap** – network scanner with scripts for enumerating supported cipher suites and protocols.
- **CIS Benchmarks** – configuration guidelines from the Center for Internet Security, including encryption-specific recommendations for operating systems, databases, and applications.

💼 Case Study – Encryption Audit

A UK-based healthcare provider stores patient records in a SQL Server database, transmits data between clinics over the internet, issues laptops to staff, and uses email to communicate with patients. An audit reveals: (1) the database uses TDE with AES-256 (good), (2) inter-clinic data transfers use TLS 1.0 (poor), (3) 30% of laptops do not have BitLocker enabled, (4) email to patients is not encrypted, and (5) encryption keys are stored in a configuration file on the database server.

Task: (1) Assess each finding against UK GDPR and NHS Data Security and Protection Toolkit requirements. (2) Prioritise the risks (high/medium/low). (3) Recommend specific remedial actions for each finding. (4) Estimate the effort and cost of each remediation. Present as a structured audit report.

3.6 Designing an encryption plan for a given organisation

An encryption plan is a comprehensive document that defines an organisation's approach to implementing and managing encryption across all systems, data, and communications. It translates policy into practice.

Components of an Encryption Plan

1. Scope and Objectives

Define the boundaries of the plan: which systems, data classifications, and communication channels are covered. State the objectives (e.g. protect personal data, meet PCI DSS compliance, defend against ransomware).

2. Data Classification

Classify data by sensitivity: public, internal, confidential, restricted/secret. Each classification level determines the encryption requirements:

- Public – no encryption required for storage; TLS for transmission.
- Internal – encryption recommended at rest; TLS required in transit.
- Confidential – encryption required at rest and in transit (AES-256, TLS 1.2+).
- Restricted – encryption mandatory everywhere with strongest available algorithms; strict key management; access logging.

3. Encryption Standards

Specify the algorithms, key lengths, and modes of operation approved for use:

- Symmetric: AES-256-GCM (preferred) or AES-128-GCM (acceptable) for data encryption.
- Asymmetric: RSA-3072+ or ECDSA P-256+ for signatures; ECDH P-256+ for key exchange.
- Hashing: SHA-256 or SHA-384 for integrity; Argon2id for password storage.
- Protocols: TLS 1.3 (preferred) or TLS 1.2 with approved cipher suites only.
- Prohibited: DES, 3DES, RC4, MD5, SHA-1, SSL, TLS 1.0, TLS 1.1.

4. Implementation Plan

- Data at rest: full disk encryption on all endpoints; TDE for databases; encrypted backups.
- Data in transit: TLS 1.2+ for all web traffic; VPN for remote access; encrypted email for sensitive communications.
- Data in use: evaluate confidential computing for highly sensitive workloads.
- Key management: HSMs for high-value keys; automated key rotation; escrow and recovery procedures.

5. Key Management Plan

Detail the full key lifecycle: generation (HSM or FIPS-validated CSPRNG), distribution (secure out-of-band channels), storage (HSM for master keys, encrypted key stores for operational keys), rotation (annual for most keys, more frequent for high-risk), escrow (Active Directory for BitLocker, HSM-backed for enterprise keys), and destruction (crypto-erase, secure key deletion).

6. Roles and Responsibilities

- CISO / Head of Security: overall accountability for the encryption programme.
- Security Operations: day-to-day management of encryption systems and key management.

- IT Operations: implementation of encryption on endpoints, servers, and networks.
- Development teams: implementing encryption in applications following the plan's standards.
- All staff: compliance with the encryption policy (e.g. not disabling BitLocker, using approved communication channels).

7. Monitoring and Compliance

- Continuous monitoring of TLS configurations (automated scanning).
- Regular audits of encryption implementation (quarterly).
- Certificate management: automated renewal, revocation monitoring.
- Incident response: procedures for cryptographic key compromise.
- Metrics: percentage of data encrypted at rest/in transit, number of deprecated algorithms in use, certificate expiry compliance.

8. Migration and Quantum Readiness

Include a roadmap for migrating away from deprecated algorithms and preparing for post-quantum cryptography. Identify systems using algorithms vulnerable to quantum attacks (RSA, ECDH) and plan for migration to NIST-approved post-quantum algorithms when industry-ready implementations become available.

📝 **Over to you – Encryption Plan Project**

Design a comprehensive encryption plan for the following organisation:

Scenario: A UK-based e-commerce company with 200 employees, processing 50,000 credit card transactions per month, storing customer personal data (names, addresses, email, purchase history), hosting its web application on AWS, using Microsoft 365 for email and collaboration, and issuing laptops to all staff who frequently work remotely.

Your encryption plan should cover all eight components described above. Present as a formal document of approximately 1,500–2,000 words, with clear sections, tables where appropriate, and specific technical recommendations.

Reading List

- Aumasson, J.-P. (2021) Serious cryptography: a practical introduction to modern encryption. 2nd edn. San Francisco: No Starch Press.
- Ferguson, N., Schneier, B. and Kohno, T. (2021) Cryptography engineering: design principles and practical applications. 2nd edn. Indianapolis: Wiley.
- NCSC (2024) Using TLS to protect data. Available at: https://www.ncsc.gov.uk/guidance/tls-external-facing-services (Accessed: 15 March 2026).
- NIST (2024) SP 800-57: recommendation for key management. Available at: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final (Accessed: 15 March 2026).
- Stallings, W. (2022) Cryptography and network security: principles and practice. 8th edn. Harlow: Pearson.
- Wong, D. (2021) Real-world cryptography. Shelter Island: Manning Publications.

Summary

In this chapter, you have developed practical knowledge for designing encryption solutions. You have analysed the full range of attack methods targeting encrypted data, from brute-force and side-channel attacks to social engineering. You have evaluated additional encryption methods including homomorphic encryption, quantum key distribution, and format-preserving encryption.

You have examined key escrow and recovery principles, including the lessons of the Clipper Chip. You have assessed the importance of robust encryption for data protection, compliance, and trust. You have learned to evaluate existing encryption arrangements through structured audits. Finally, you have designed a comprehensive encryption plan covering data classification, standards, implementation, key management, and quantum readiness.

Glossary

Word / Term	Explanation
AES	Advanced Encryption Standard; the current global standard for symmetric encryption (128, 192, or 256-bit keys).
Asymmetric Encryption	Encryption using a key pair (public and private). Also called public key cryptography.
BitLocker	Microsoft's full disk encryption tool for Windows, using AES.
Block Cipher	A symmetric cipher that encrypts data in fixed-size blocks (e.g. 128 bits for AES).
CA (Certificate Authority)	A trusted entity that issues digital certificates binding public keys to identities.
CBC	Cipher Block Chaining; a block cipher mode where each block is XORed with the previous ciphertext.
Ciphertext	The encrypted, unreadable form of data.
CTR	Counter mode; a block cipher mode that turns block ciphers into stream ciphers.
DES	Data Encryption Standard; a deprecated 56-bit symmetric block cipher.
Diffie-Hellman	A key exchange protocol enabling two parties to establish a shared secret over an insecure channel.
Digital Signature	A cryptographic mechanism providing authentication, integrity, and non-repudiation.
ECDSA	Elliptic Curve Digital Signature Algorithm; a modern, efficient digital signature algorithm.
FPE	Format-Preserving Encryption; encrypts data while maintaining its original format.
GCM	Galois/Counter Mode; an authenticated encryption mode providing both confidentiality and integrity.
GDPR	General Data Protection Regulation; EU and UK data protection law.
Hash Function	A one-way function that produces a fixed-length output from any input.
HMAC	Hash-based Message Authentication Code; combines hashing with a secret key for integrity and authentication.
HSM	Hardware Security Module; a dedicated device for secure key generation and storage.
IPSec	Internet Protocol Security; a protocol suite for encrypting network traffic at the IP layer.
IV	Initialisation Vector; a random value used to ensure unique encryption outputs.

Kerberos	A network authentication protocol using symmetric cryptography and tickets.
Key Escrow	An arrangement where cryptographic keys are held by a trusted third party.
LUKS	Linux Unified Key Setup; the standard for full disk encryption on Linux.
NIST	National Institute of Standards and Technology; publishes cryptographic standards.
PCI DSS	Payment Card Industry Data Security Standard; mandates encryption for payment data.
PKI	Public Key Infrastructure; the framework of certificates, CAs, and trust hierarchies.
Plaintext	The original, unencrypted form of data.
Post-Quantum	Cryptographic algorithms designed to resist attacks from quantum computers.
RSA	Rivest-Shamir-Adleman; a widely used asymmetric encryption algorithm.
SHA-256	Secure Hash Algorithm 256-bit; the current standard cryptographic hash function.
Side-Channel Attack	An attack exploiting physical implementation leaks (timing, power, EM emissions).
Stream Cipher	A symmetric cipher that encrypts data one bit/byte at a time.
Symmetric Encryption	Encryption where the same key is used for both encryption and decryption.
TLS	Transport Layer Security; the protocol securing web and internet communications.
Tokenisation	Replacing sensitive data with non-reversible tokens.
X.509	The standard format for digital certificates.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. Cryptography provides confidentiality, integrity, authentication, and non-repudiation.
2. Symmetric encryption uses a pair of public and private keys.
3. AES is the current global standard for symmetric encryption.
4. RSA encryption is based on the difficulty of factoring large prime numbers.
5. MD5 is considered a secure hashing algorithm for current use.
6. TLS 1.3 still supports RC4 and DES cipher suites.
7. A digital signature provides non-repudiation.
8. Side-channel attacks exploit weaknesses in the cryptographic algorithm itself.
9. Key escrow involves a third party holding copies of cryptographic keys.
10. The UK GDPR explicitly mandates encryption for all personal data.
11. The Diffie-Hellman protocol enables secure key exchange over an insecure channel.
12. ECB mode is the recommended mode for AES encryption.
13. Post-quantum cryptography aims to resist attacks from quantum computers.
14. FIPS 140-3 defines four security levels for cryptographic modules.
15. Homomorphic encryption allows computation on encrypted data.
16. PCI DSS requires TLS 1.0 or higher for payment data transmission.
17. A rainbow table attack can be defeated by using salted hashes.
18. BitLocker uses AES for full disk encryption.
19. The Wassenaar Arrangement governs export controls on cryptographic products.
20. Under RIPA Part III, failure to disclose encryption keys can result in imprisonment.

Multiple Choice Questions

1. Which algorithm is the current standard for symmetric encryption?

A. DES B. RSA C. AES D. MD5

2. What is the primary purpose of a digital signature?

A. Encrypt data B. Provide authentication and non-repudiation C. Compress data D. Generate random numbers

3. Which TLS version removed support for insecure algorithms?

A. TLS 1.0 B. TLS 1.1 C. TLS 1.2 D. TLS 1.3

4. What type of attack exploits power consumption patterns during encryption?

A. Brute-force B. Side-channel C. Dictionary D. Birthday

5. Which block cipher mode provides authenticated encryption?

A. ECB B. CBC C. GCM D. CTR

6. What does PKI stand for?

A. Private Key Interface B. Public Key Infrastructure C. Protected Key Index D. Primary Key Identification

7. Which law governs key disclosure in the UK?

A. Data Protection Act 2018 B. Computer Misuse Act 1990 C. RIPA 2000 Part III D. Investigatory Powers Act 2016

8. What is the maximum fine under UK GDPR for data protection failures?

A. £1 million B. £5 million C. £17.5 million or 4% of turnover D. £50 million

9. Which hashing algorithm is currently recommended for security applications?

A. MD5 B. SHA-1 C. SHA-256 D. CRC32

10. What is the key size of AES-256?

A. 128 bits B. 192 bits C. 256 bits D. 512 bits

11. Which protocol is used for secure key exchange?

A. AES B. SHA-256 C. Diffie-Hellman D. MD5

12. What standard validates cryptographic modules?

A. ISO 27001 B. PCI DSS C. FIPS 140-3 D. Common Criteria

13. Elliptic Curve Cryptography provides equivalent security to RSA with:

A. Larger key sizes B. Smaller key sizes C. The same key sizes D. No keys at all

14. Which encryption method allows computation on encrypted data?

A. Symmetric B. Asymmetric C. Homomorphic D. Format-preserving

15. The '3-2-1' rule in backup refers to:

A. 3 keys, 2 algorithms, 1 protocol B. 3 copies, 2 media types, 1 offsite C. 3 users, 2 passwords, 1 token D. 3 servers, 2 networks, 1 cloud

16. Which NIST post-quantum standard is used for key encapsulation?

A. RSA-4096 B. ML-KEM (Kyber) C. AES-512 D. SHA-3

17. What does the acronym CIA stand for in information security?

A. Cipher, Integrity, Access B. Confidentiality, Integrity, Availability C. Cryptography, Internet, Authentication D. Control, Information, Audit

18. Which attack uses precomputed hash tables?

A. Brute-force B. Phishing C. Rainbow table D. Side-channel

19. Shamir's Secret Sharing is used for:

A. Encrypting databases B. Splitting keys into multiple shares C. Hashing passwords D. Signing certificates

20. WPA3 uses which authentication protocol?

A. WEP B. TKIP C. SAE (Dragonfly) D. PSK only

Answers to True/False Questions

1. True. These are the four pillars of cryptographic security.

2. False. Symmetric encryption uses a single shared key; asymmetric encryption uses a key pair.

3. True. AES was standardised by NIST in 2001 and remains the global standard.

4. True. RSA's security relies on the difficulty of factoring the product of two large primes.

5. False. MD5 is broken – collision attacks have been demonstrated. It should not be used for security.

6. False. TLS 1.3 removed support for all insecure algorithms including RC4, DES, and 3DES.

7. True. Digital signatures provide authentication, integrity, and non-repudiation.

8. False. Side-channel attacks exploit physical implementation characteristics (timing, power, EM), not the algorithm.

9. True. Key escrow involves a trusted third party holding copies of keys for recovery.

10. False. The UK GDPR recommends encryption as an appropriate measure but does not mandate it for all data.

11. True. Diffie-Hellman enables secure key exchange over insecure channels.

12. False. ECB mode is insecure; GCM or CTR modes are recommended.

13. True. Post-quantum algorithms are designed to resist attacks from both classical and quantum computers.

14. True. FIPS 140-3 defines Levels 1 through 4 with increasing security requirements.

15. True. Homomorphic encryption enables computation on ciphertext without decryption.

16. False. PCI DSS requires TLS 1.2 or higher (TLS 1.0 and 1.1 are prohibited).

17. True. Adding a unique salt to each password before hashing defeats precomputed rainbow tables.

18. True. BitLocker uses AES-128 or AES-256 for full volume encryption.

19. True. The Wassenaar Arrangement is a multilateral export control regime covering dual-use cryptographic products.

20. True. Under RIPA Part III, failure to disclose encryption keys carries up to 2 years' imprisonment (5 years in national security cases).

Answers to Multiple Choice Questions

1. (C) AES

2. (B) Provide authentication and non-repudiation

3. (D) TLS 1.3

4. (B) Side-channel

5. (C) GCM

6. (B) Public Key Infrastructure

7. (C) RIPA 2000 Part III

8. (C) £17.5 million or 4% of turnover
9. (C) SHA-256
10. (C) 256 bits
11. (C) Diffie-Hellman
12. (C) FIPS 140-3
13. (B) Smaller key sizes
14. (C) Homomorphic
15. (B) 3 copies, 2 media types, 1 offsite
16. (B) ML-KEM (Kyber)
17. (B) Confidentiality, Integrity, Availability
18. (C) Rainbow table
19. (B) Splitting keys into multiple shares
20. (C) SAE (Dragonfly)