Session 4 – Chapter 6/Chapter 7 (pg. 227-311)

2025 CISSP Mentor Program

CHAPTER 6

Evan Francen

FRSecure

2025 CISSP MENTOR PROGRAM

AGENDA – SESSION 4

Chapter 6/Chapter 7 (from the book)

Chapter 6 - Cryptography and Symmetric Key Algorithms

- Cryptographic Foundations
- Modern Cryptography
- Symmetric Cryptography
- Cryptographic Life Cycle

This lesson.

Chapter 7 - PKI and Cryptographic Applications

- Asymmetric Cryptography
- Hash Functions
- Digital Signatures
- Public Key Infrastructure
- Asymmetric Key Management
- Hybrid Cryptography
- Applied Cryptography
- Cryptographic Attacks


LEARN
ABOUT
ENCRYPTION

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Goals of Cryptography

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Goals of Cryptography

Boils down to four core principles — often remembered by the acronym **C-I-A + N**

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Goals of Cryptography

Boils down to four core principles — often remembered by the acronym **C-I-A + N**

🔐 **1. Confidentiality**

Keep it secret, keep it safe.

- Ensures that data is only accessible by authorized individuals.
- Prevents unauthorized disclosure of information.
- **Example**: Encrypting emails so only the intended recipient can read them.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Goals of Cryptography

Boils down to four core principles — often remembered by the acronym **C-I-A + N**

🔐 **1. Confidentiality**

🧬 **2. Integrity**

Trust the data hasn't been tampered with.

- Ensures that data remains **unchanged** during storage or transmission.
- Protects against **modification**, **insertion**, or **deletion** by unauthorized actors.
- **Example**: Hashes and checksums used to verify downloaded files.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Goals of Cryptography

Boils down to four core principles — often remembered by the acronym **C-I-A + N**

1. Confidentiality

2. Integrity

3. Authentication

Prove you are who you say you are.

- Confirms the identity of the sender or user.
- Ensures that communications or transactions are **originating from a legitimate source**.
- **Example**: Digital certificates or passwords verifying identity during login.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Goals of Cryptography

Boils down to four core principles — often remembered by the acronym **C-I-A + N**

1. Confidentiality
2. Integrity
3. Authentication

These four together form the foundation of secure communication and system trust in cybersecurity. Without them, data can be stolen, modified, faked, or disowned — and the entire digital system collapses under unreliability.

4. Non-repudiation

You can't deny it later.

Guarantees that a sender **cannot deny** having sent a message.

Uses digital signatures and audit logs to **hold parties accountable**.

Example: A signed email proves that *you* sent it, even if you later try to deny it.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptography Concepts

🔑 **Key** - A secret value used in cryptographic algorithms to encrypt or decrypt data.

🔐 **Encryption** - The process of converting plaintext into ciphertext to prevent unauthorized access.

🔒 **Decryption** - The process of converting ciphertext back into readable plaintext using a key.

📜 **Plaintext** - The original, unencrypted data or message.

📃 **Ciphertext** - The encrypted version of plaintext; unreadable without the decryption key.

🔄 **Algorithm** - A step-by-step mathematical procedure used for encryption and decryption.

🔀 **Cipher** - A specific implementation of an encryption algorithm (e.g., AES, DES).

📥 **Symmetric Encryption** - Uses the same key for both encryption and decryption (Fast, but key distribution is a challenge).

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptography Concepts

📤 **Asymmetric Encryption** - Uses a public/private key pair — one to encrypt, the other to decrypt (Solves the key distribution problem).

🔁 **Block Cipher** - Encrypts data in fixed-size blocks (e.g., 128 bits at a time). Example: AES

🌊 **Stream Cipher** - Encrypts data bit by bit or byte by byte. Example: RC4

🧬 **Hashing** - Converts data into a fixed-length digest. It's one-way and not reversible (Used for integrity checks, not encryption).

✍️ **Digital Signature** - A cryptographic method for verifying authenticity and integrity using asymmetric keys (Provides non-repudiation).

👥 **Public Key** - The non-secret key in asymmetric encryption (Can be shared openly).

🕵️ **Private Key** - The secret key in asymmetric encryption (Must be kept confidential).

🧰 **Key Exchange** - The process of securely sharing cryptographic keys between parties (e.g., Diffie-Hellman).

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptography Concepts

📤 **Asymmetric Encryption** - Uses a public/private key pair — one to encrypt, the other to decrypt (Solves the key distribution problem).

Kerckhoffs's Principle

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

- Security should depend only on the secrecy of the **key**, not the algorithm.
- Promotes transparency and peer review of encryption algorithms.

✍️ **Digital Signature** - A cryptographic method for verifying authenticity and integrity using asymmetric keys (Provides non-repudiation).

👥 **Public Key** - The non-secret key in asymmetric encryption (Can be shared openly).

🕵️ **Private Key** - The secret key in asymmetric encryption (Must be kept confidential).

🧰 **Key Exchange** - The process of securely sharing cryptographic keys between parties (e.g., Diffie-Hellman).

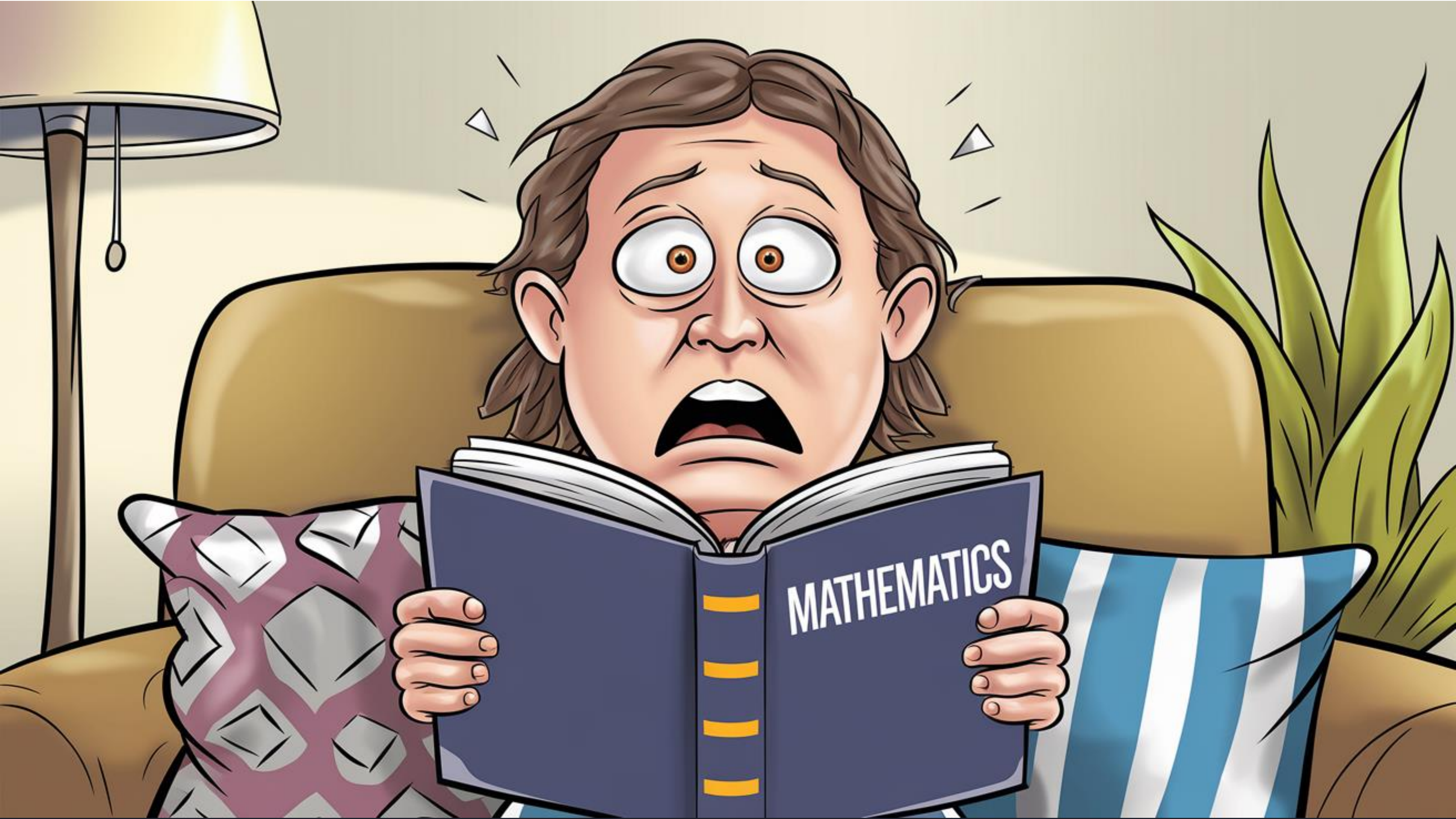
2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics


MATHEMATICS

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Boolean Mathematics in Cryptography: The Basics

Cryptographic Mathematics

Boolean Mathematics in Cryptography: The Basics

- Boolean logic is the mathematical foundation of how computers (and cryptographic algorithms) make decisions using binary values:

  1 = True

  0 = False

- Cryptographic algorithms rely on Boolean operations to manipulate bits in ways that seem random but are precisely defined.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Boolean Mathematics in Cryptography: The Basics

- Boolean logic is the mathematical foundation of how computers (and cryptographic algorithms) make decisions using binary values:

  1 = True

  0 = False

- Cryptographic algori
  seem random but ar

🔧 **Key Boolean Operations Used in Cryptography**

Operation	Symbol	Description	Example A=1, B=0	Result
AND	A ∧ B or A & B	True **only if both** inputs are true	1 AND 0	0
OR	A ∨ B or `A	B`	True if **either** input is true	1 OR 0
NOT	¬A or ~A	Inverts the input	NOT 1	0
XOR	A ⊕ B or A ^ B	True **only if inputs differ**	1 XOR 0	1

Matters most in cryptography

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why XOR Matters Most in Cryptography

- XOR (exclusive OR) is the superstar of Boolean logic in crypto. Why?

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why XOR Matters Most in Cryptography

- XOR (exclusive OR) is the superstar of Boolean logic in crypto. Why?
- It's reversible:
  - Plaintext XOR Key = Ciphertext
  - Ciphertext XOR Key = Plaintext
- It creates pseudo-randomness but is still deterministic

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

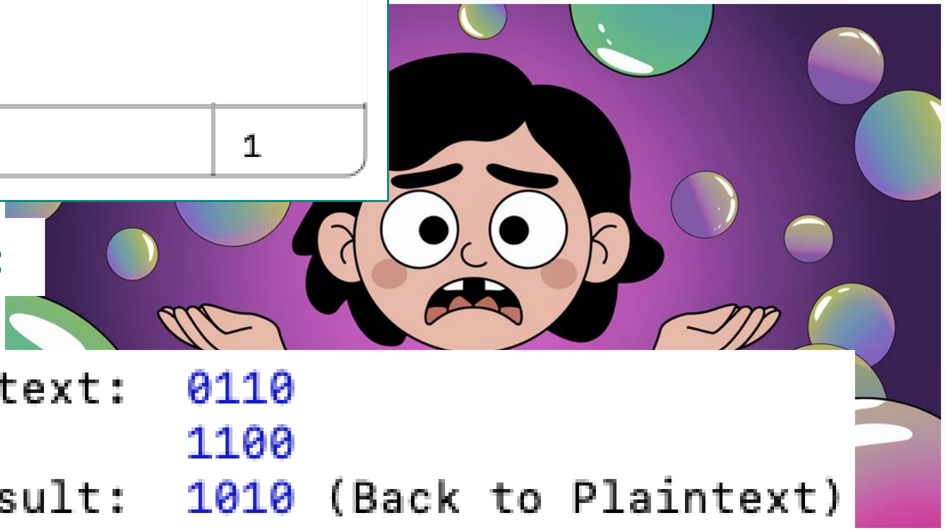
Cryptographic Mathematics

🔧 **Key Boolean Operations Used in Cryptography**

Operation	Symbol	Description	Example A=1, B=0	Result
XOR	A ⊕ B or A ^ B	True **only if inputs differ**	1 XOR 0	1

```
Plaintext:   1010
Key:         1100
XOR Result:  0110 (Ciphertext)
```

Do the XOR again with the same key:



```
Ciphertext:  0110
Key:         1100
XOR Result:  1010 (Back to Plaintext)
```

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

The Modulo Function in Cryptography: The Basics

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

The Modulo Function in Cryptography: The Basics

- Finds the remainder when one number is divided by another.
  - A mod B = Remainder when A is divided by B
  - 17 mod 5 = 2 → because 17 ÷ 5 = 3 remainder **2**

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why Modulo Matters in Cryptography

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why Modulo Matters in Cryptography

1. **It Keeps Numbers in Bounds -** In cryptographic algorithms, we often work with very large numbers (think 2048-bit keys).

The modulo function ensures:

- Results stay within a predictable range
- You don't overflow memory or break arithmetic

Cryptographic Foundations

Cryptographic Mathematics

Why Modulo Matters in Cryptography

2. **It's Used in Key Algorithms -** You'll see modulo in **asymmetric cryptography** especially:

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why Modulo Matters in Cryptography

2. **It's Used in Key Algorithms -** You'll see modulo in **asymmetric cryptography** especially:

Diffie–Hellman Key Exchange

Uses calculations like:

Shared Key = (Other Party's Public Key ^ Your Private Key) mod Prime Number

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why Modulo Matters in Cryptography

2. **It's Used in Key Algorithms -** You'll see modulo in **asymmetric cryptography** especially:

Diffie–Hellman Key Exchange

Uses calculations like:

Shared Key = (Other Party's Public Key ^ Your Private Key) mod Prime Number

RSA Encryption

All encryption and decryption steps rely on:

Ciphertext = (Plaintext ^ Public Key) mod n

Plaintext = (Ciphertext ^ Private Key) mod n

Cryptographic Foundations

Cryptographic Mathematics

Think of Modulo Like a Clock

A clock is a **modulo-12 (or 24) system**. If it’s 10 o’clock now and you add 5 hours:

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Think of Modulo Like a Clock

A clock is a **modulo-12 (or 24) system**. If it's 10 o'clock now and you add 5 hours:

$$(10 + 5) \bmod 12 = 3 \rightarrow \text{It's 3 o'clock}$$

This same wrap-around behavior is **exactly** how we limit values in crypto to stay within key lengths or number ranges.

Key Takeaways

mod = remainder after division
Keeps cryptographic values manageable
Used in key generation, encryption, and digital signatures

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

One-Way Functions in Cryptography: The Basics

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

One-Way Functions in Cryptography: The Basics

A one-way function is a mathematical process that is:

- Easy to compute in one direction, but
- Infeasible to reverse without special information (like a key)

Think of it like a blender:
You can throw ingredients in and make a smoothie easily (forward). But try turning the smoothie back into the exact ingredients — good luck (reverse).

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

One-Way Functions in Cryptography: The Basics

Simple Example (Hashing)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

One-Way Functions in Cryptography: The Basics

Simple Example (Hashing)

Take the word security and apply a hashing algorithm:

$$Hash(\text{"security"}) \rightarrow a3f5c8d...$$

You can calculate the hash easily.

But can you figure out the original input just by looking at the hash? No — that's the one-way part.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why One-Way Functions Matter in Cryptography

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Why One-Way Functions Matter in Cryptography

They're used in cryptographic systems that need:

- **Data integrity** — via hash functions (e.g., SHA-256)
- **Password protection** — store only the hash, not the actual password
- **Digital signatures** — prove authenticity without revealing sensitive data
- **Public-key encryption** — factoring large primes is a one-way process

Not Encryption

A one-way function is not encryption:

- Encryption is reversible (with a key)
- One-way functions are not (by design)

Security Benefit

Even if an attacker sees the result of a one-way function, they:

- Can't figure out the original input
- Can't generate the same output without guessing the exact input

This makes one-way functions ideal for protecting secrets, even in public systems.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Nonce, Zero-Knowledge Proof, Split Knowledge, and Work Function

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Nonce, Zero-Knowledge Proof, Split Knowledge, and Work Function

1. Nonce (Number used once)

a random or pseudo-random value that is used only once in a cryptographic process.

Purpose:

Prevents replay attacks — if a message is reused, the nonce will detect it.

Adds freshness and uniqueness to encryption or authentication attempts.

Think of it like:

A one-time padlock code that changes every time — even if the message stays the same.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Nonce, Zero-Knowledge Proof, Split Knowledge, and Work Function

2. Zero-Knowledge Proof

lets someone prove they know a secret without revealing the secret itself.

Purpose:

Used in authentication, blockchain privacy, and secure voting systems.

Real-world analogy:

Imagine proving you know the password to a vault by unlocking it, but without ever telling anyone the password.

It's secure because the verifier is convinced you know the secret — but learns nothing else.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Nonce, Zero-Knowledge Proof, Split Knowledge, and Work Function

3. Split Knowledge

a security principle where no one person has the full secret.

Purpose:

Ensures separation of duties and prevents insider abuse.

Common in key management, especially manual key entry systems.

Analogy:

Two people each hold half of the launch code. Neither can act alone — both must cooperate.

This increases security and accountability.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Cryptographic Mathematics

Nonce, Zero-Knowledge Proof, Split Knowledge, and Work Fu

The work function helps you answer:

- How hard is this to break?
- Is the cost of attack greater than the value of the data?

4. Work Function

is the estimated effort required (usually in time or computational power) to break a cryptographic system.

Purpose:

Helps determine the strength of a cryptosystem.

Used to set minimum key lengths and algorithm standards.

Example:

A 256-bit AES key has a work function so high (2^{256} tries) that it would take millions of years to brute-force — even with all the computing power on Earth.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers

What is a Cipher?!

A cipher is a method or algorithm used to transform plaintext into ciphertext — in other words, it's the **recipe for scrambling** a message so others can't read it.

Plaintext + Cipher + Key = Ciphertext Ciphertext + Cipher + Key = Plaintext

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers

Codes vs. Ciphers What's the Difference?

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers

Codes vs. Ciphers What's the Difference?

Feature	Code	Cipher
What it changes	Whole words or phrases	Individual letters, bits, or characters
Based on	Meaning (semantics)	Rules and math (algorithms)
Example	"Red Apple" → "Bravo Tango"	"HELLO" → "KHOOR" (Caesar Cipher, shift by 3)
Used for	Hiding or shortening common phrases	Securely scrambling any message
Modern use?	Rare — mostly historical or military shorthand	Common — used in all digital encryption

In Simple Terms:

- A code replaces a message with something else that has meaning.
- A cipher scrambles a message using a rule or formula.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers - Transposition Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

It’s like **shuffling** letters instead of replacing them.

Ciphers - Transposition Ciphers

A method of encryption that rearranges the order of characters in a message, without changing the actual characters.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers - Transposition Ciphers

It's like **shuffling** letters instead of replacing them.

A method of encryption that rearranges the order of characters in a message, without changing the actual characters.

- **Simple Example**:
  - Original message: HELLO
  - Apply a transposition rule (e.g., reverse the order): OLLEH
- **Why It Matters**:
  - Simple but powerful when combined with substitution.
  - Teach important concepts in modern encryption like **confusion and diffusion**.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers - Substitution Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

You **swap letters** instead of moving them around.

Ciphers - Substitution Ciphers

A method of encryption where each character (or group of characters) in the original message is replaced with a different character or symbol.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers - Substitution Ciphers

You **swap letters** instead of moving them around.

A method of encryption where each character (or group of characters) in the original message is replaced with a different character or symbol.

- **Simple Example: Caesar Cipher**
  - Shift each letter forward by 3 in the alphabet:
    - Plaintext: *HELLO*
    - Ciphertext: *KHOOR*

H → K
E → H
L → O
L → O
O → R

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers - Substitution Ciphers

You **swap letters** instead of moving them around.

A method of encryption where each character (or group of characters) in the original message is replaced with a different character or symbol.

- **Simple Example: Caesar Cipher**
  - Shift each letter forward by 3 in the alphabet:
    - Plaintext: *HELLO*
    - Ciphertext: *KHOOR*

H → K
E → H
L → O
L → O
O → R

- **Common Types:**
  - **Caesar Cipher** – shifts all letters by the same number.
  - **Monoalphabetic Substitution** – uses a fixed substitution alphabet.
  - **Polyalphabetic Substitution** – changes the substitution rule as you go (e.g., Vigenère Cipher).

Why It Matters:

- Substitution introduces confusion in the message — a core concept in modern cryptography.
- Most modern ciphers still rely on advanced forms of substitution under the hood.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – One-Time Pads

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

It's like a disposable secret code sheet that you burn after using.

Ciphers – One-Time Pads

A type of encryption that uses a completely random key that is as long as the message itself — and it's used only once.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

It’s like a disposable secret code sheet that you burn after using.

Ciphers – One-Time Pads

A type of encryption that uses a completely random key that is as long as the message itself — and it’s used only once.

How It Works:

- You create a random key (same length as your message).
- You XOR the key with the plaintext to get ciphertext.
- To decrypt, you XOR the ciphertext with the same key again.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

It's like a disposable secret code sheet that you burn after using.

Ciphers – One-Time Pads

A type of encryption that uses a completely random key that is as long as the message itself — and it's used only once.

How It Works:

ge).

again.

Simple Example:

Let's say your message (in binary) is:

- Plaintext: 10101010
- Key: 11001100
- Ciphertext: 01100110 ← (Plaintext XOR Key)

Now decrypt:

- Ciphertext: 01100110
- Key: 11001100
- Plaintext: 10101010 ← (Ciphertext XOR Key)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – One-Time Pads

It's like a disposable secret code sheet that you burn after using.

ne message itself

Why It's Special:

- Unbreakable — mathematically proven to be 100% secure if used correctly.
- Even the most powerful computers can't crack it without the key.

Why It's Rarely Used:

- Key must be as long as the message
- Key must be completely random
- Key must never be reused
- Key must be securely shared in advance

All of this makes it very impractical for most modern communication.

- Key: 11001100
- Plaintext: 10101010 ← (Ciphertext XOR Key)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Running Key Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

You use a real sentence (like from a novel) to encrypt the message, letter by letter.

Ciphers – Running Key Ciphers

A type of substitution cipher where the key is a long stream of text — often from a book or article — instead of a short repeated key.

Cryptographic Foundations

You use a real sentence (like from a novel) to encrypt the message, letter by letter.

Ciphers – Running Key Ciphers

A type of substitution cipher where the key is a long stream of text — often from a book or article — instead of a short repeated key.

How It Works:

1. You pick a plaintext message:

   MEETATNOON

2. You choose a key that is a long piece of text:

   DEFENDTHEBASE

3. You combine them (usually with a Caesar-style shift based on the key letters).

Each letter in the message is shifted based on the matching letter in the key.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

You use a real sentence (like from a novel) to encrypt the message, letter by letter.

Ciphers – Running Key Ciphers

A type of substitution cipher where the key is a long stream of text — often from a book or article — instead of a short repeated key.

Why Use It?

- More secure than regular substitution because the key isn't repeated.
- Looks more random and harder to crack with frequency analysis.

Weaknesses:

- If the key source (like a book) is known, it becomes easier to guess.
- Still vulnerable to known-plaintext or statistical attacks.

Summary:

- Type: Polyalphabetic substitution cipher
- Key: A long piece of meaningful text (e.g., a book passage)
- Goal: Avoid repeating keys and improve security over simple ciphers

s).

Real-World Analogy:

Imagine sending a secret message to someone, and both of you use page 57 of the same novel as the key. The message is encrypted by blending it with the words on that page.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Block Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Block Ciphers

Think of it like chopping a message into chunks and locking each chunk in its own box.

A method of encryption that takes your plaintext message and breaks it into fixed-size blocks (usually 64 or 128 bits), then encrypts each block one at a time using the same key.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Think of it like chopping a message into chunks and locking each chunk in its own box.

Ciphers – Block Ciphers

A method of encryption that takes your plaintext message and breaks it into fixed-size blocks (usually 64 or 128 bits), then encrypts each block one at a time using the same key.

Simple Example:

If your message is:

HELLO WORLD!

A block cipher might split it into 3 blocks:

[HELLO] [WORLD!] [......]

Each block is encrypted separately (with padding if needed).

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Block Ciphers

Think of it like chopping a message into chunks and locking each chunk in its own box.

A method of encryption that takes your plaintext message and breaks it into fixed-size … the same key.

How It Works:

- Split plaintext into blocks.
- Encrypt each block using the same key and algorithm.
- Optionally apply a mode of operation (like CBC or CTR) to link or randomize blocks.

HELLO WORLD!

A block cipher might split it into 3 blocks:

[HELLO] [WORLD!] [......]

Common Block Ciphers:

- AES (Advanced Encryption Standard) – 128-bit block
- DES (Data Encryption Standard) – 64-bit block
- 3DES – Same block size, but triple-encrypted

Why Use Block Ciphers?

- Great for encrypting files, database records, and data at rest.
- Strong, standardized, and widely supported.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Stream Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Stream Ciphers

Think of it like a walkie-talkie — it encrypts the message as you speak it, bit by bit, on the fly.

A type of encryption that encrypts data one bit or byte at a time, instead of in chunks (like block ciphers).

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Think of it like a walkie-talkie — it encrypts the message as you speak it, bit by bit, on the fly.

Ciphers – Stream Ciphers

A type of encryption that encrypts data one bit or byte at a time, instead of in chunks (like block ciphers).

Simple Example:

Let’s say:

- **Plaintext**: 1010
- **Keystream**: 1100

Then:

Ciphertext = 1010 XOR 1100 = 0110

Decrypt:

0110 XOR 1100 = 1010 (original message)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Think of it like a walkie-talkie — it encrypts the message as you speak it, bit by bit, on the fly.

Ciphers – Stream Ciphers

A type of encryption that encrypts data one bit or byte at a time, instead of in chunks (like block ciphers)

How It Works:

- A keystream (a stream of random-looking bits) is generated using a key.
- The keystream is XORed with the plaintext to produce ciphertext.
- To decrypt, the same keystream is XORed with the ciphertext to recover the plaintext.

- **Keystream:**

Then:

Ciphertex

Decrypt:

Key Features:

- Encrypts data **in real-time**
- Great for streaming audio/video, low-latency environments
- Often **faster** than block ciphers
- Requires strong keystream generation (usually via pseudo-random generators)

Common Pitfalls:

- If you **reuse the key or keystream**, the cipher becomes **trivially breakable**
- RC4 was a popular stream cipher — now **deprecated** due to vulnerabilities

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Confusion and Diffusion

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Confusion and Diffusion

Two pillars of good encryption, designed to hide patterns and make it really hard for attackers to figure out the original message or the key.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Confusion and Diffusion

Two pillars of good encryption, designed to hide patterns and make it really hard for attackers to figure out the original message or the key.

Confusion means making the relationship between the key and the ciphertext as complex as possible.

- The attacker can't easily guess the key, even if they know the algorithm.
- Achieved through substitution (e.g., swapping one value for another).

> Think of it like mixing up all the spices in a recipe so you can't tell which ingredient causes which flavor.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Confusion and Diffusion

Two pillars of good encryption, designed to hide patterns and make it really hard for attackers to figure out the original message or the key.

Diffusion means spreading the plaintext across the ciphertext as widely as possible.

- A small change in the plaintext results in **big changes** in the ciphertext.
- Achieved through **transposition** and complex mixing operations.

Think of it like dropping ink into water — it spreads out so evenly that you can't tell where the drop started.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Confusion and Diffusion

Two pillars of good encryption, designed to hide patterns and make it really hard for

…lely as possible.

…iphertext.

…ns.

Why It Matters:

- Together, confusion and diffusion prevent patterns, making cryptanalysis (like frequency analysis) ineffective.
- They're baked into modern algorithms like AES, DES, and others.

Think of it like dropping ink into water — it spreads out so evenly that you can't tell where the drop started.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Ciphers – Confusion and Diffusion

Quick Recap

Principle	What it does	How it's done
Confusion	Hides relationship to the key	Substitution
Diffusion	Hides patterns in the message	Transposition/mixing

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Modern cryptography refers to the use of mathematics, algorithms, and computer systems to secure data in the digital age.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Modern cryptography refers to the use of mathematics, algorithms, and computer systems to secure data in the digital age.

Key Features of Modern Cryptography:

1. **Based on Strong Math** - Uses complex mathematical problems (like factoring large primes) that are easy to do in one direction, but hard to reverse.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Modern cryptography refers to the use of mathematics, algorithms, and computer systems to secure data in the digital age.

Key Features of Modern Cryptography:

1. **Based on Strong Math** - Uses complex mathematical problems (like factoring large primes) that are easy to do in one direction, but hard to reverse.
2. **Involves Both Symmetric and Asymmetric Algorithms**
   - Symmetric: same key to encrypt and decrypt (e.g., AES)
   - Asymmetric: public key to encrypt, private key to decrypt (e.g., RSA)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Modern cryptography refers to the use of mathematics, algorithms, and computer systems to secure data in the digital age.

Key Features of Modern Cryptography:

1. **Based on Strong Math** - Uses complex mathematical problems (like factoring large primes) that are easy to do in one direction, but hard to reverse.
2. **Involves Both Symmetric and Asymmetric Algorithms**
   - Symmetric: same key to encrypt and decrypt (e.g., AES)
   - Asymmetric: public key to encrypt, private key to decrypt (e.g., RSA)
3. **Used Everywhere** - HTTPS, email encryption, VPNs, secure messaging, digital signatures, blockchain, and more.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Modern cryptography refers to the use of mathematics, algorithms, and computer systems to secure data in the digital age.

Key Features of Modern Cryptography:

1. **Based on Strong Math** - Uses complex mathematical problems (like factoring large primes) that are easy to do in one direction, but hard to reverse.
2. **Involves Both Symmetric and Asymmetric Algorithms**
   - Symmetric: same key to encrypt and decrypt (e.g., AES)
   - Asymmetric: public key to encrypt, private key to decrypt (e.g., RSA)
3. **Used Everywhere** - HTTPS, email encryption, VPNs, secure messaging, digital signatures, blockchain, and more.
4. **Supports Key Security Goals** - Confidentiality, Integrity, Authentication, and Non-repudiation

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Modern cryptography refers to the use of mathematics, algorithms, and computer systems to secure data in the digital age.

Key Features of Modern Cryptography:

Uses complex mathematical problems (like factoring large
lo in one direction, but hard to reverse.

and Asymmetric Algorithms

to encrypt and decrypt (e.g., AES)

y to encrypt, private key to decrypt (e.g., RSA)

S, email encryption, VPNs, secure messaging, digital signatures,
blockchain, and more.

4. **Supports Key Security**
repudiation

Why It Matters:

Modern cryptography enables:

- Secure online banking
- Private communications
- Safe e-commerce
- Protection against data breaches

In a Nutshell:
Modern cryptography is the science of keeping digital data secure — not with secrecy, but with math that's nearly impossible to break.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Cryptographic Keys

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Cryptographic Keys

Think of the key like the combination to a safe — without it, the contents stay secure.

A cryptographic key is a secret value used by an encryption algorithm to lock (encrypt) or unlock (decrypt) data.

Cryptographic keys are the **core secret ingredient** that makes encryption work — keep them strong, long, and protected at all costs.

Key Roles in Encryption:

- **Encryption**: turns plaintext into ciphertext using a key
- **Decryption**: turns ciphertext back into plaintext using the same key (symmetric) or a related key (asymmetric)

Type	Description	Example
Symmetric	Same key for both encryption & decryption	AES, DES
Asymmetric	Uses a public key to encrypt, private key to decrypt	RSA, ECC

Why Keys Matter:

- The strength and secrecy of the key determine how secure your data is.
- Even the strongest algorithm is useless if the key is weak or exposed.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Symmetric Key Algorithms

WORDS

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Symmetric Key Algorithms

Think of it like a shared house key — both people use the exact same key to lock and unlock the door.

Symmetric key algorithms use the **same secret key** for both encryption and decryption of data.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Symmetric Key Algorithms

Think of it like a shared house key — both people use the exact same key to lock and unlock the door.

Symmetric key algorithms use the **same secret key** for bo data.

Key Weakness:

- If the **key is intercepted**, the entire system is compromised.
- Doesn’t scale well for large groups (more keys needed).

How It Works:

- Sender encrypts the message with a secret key.
- Receiver uses that same key to decrypt it.

Key Features:

- **Fast and efficient** — ideal for large volumes of data
- Requires a **secure way to share the key** (key distribution is the big challenge)
- Common in file encryption, backups, and internal systems

Common Symmetric Algorithms:

- AES (Advanced Encryption Standard) – modern, strong, widely used
- 3DES – older but still seen in legacy systems
- Blowfish, IDEA, RC5, RC6 – various use cases, some deprecated

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Asymmetric Key Algorithms

Modern Cryptography

Think of it like a locked mailbox: anyone can drop a letter in (public key), but only the owner can open it (private key).

Asymmetric Key Algorithms

Asymmetric key algorithms use two different but mathematically related keys:

- A **public key** to encrypt
- A **private key** to decrypt

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Asymmetric Key Algorithms

Think of it like a locked mailbox: anyone can drop a letter in (public key), but only the owner can open it (private key).

Asymmetric key algorithms use two different but mathematically related keys:

- A **public key** to encrypt
- A **private key** to decrypt

Asymmetric encryption uses a key pair: one to lock, the other to unlock — making it powerful for secure communication between strangers.

How It Works:

1. You share your public key with anyone.
2. They use it to encrypt a message for you.
3. Only you can decrypt it with your private key (which you keep secret).

Key Features:

- Solves the key distribution problem — no need to secretly share a key
- Enables digital signatures, secure key exchange, and authentication
- Slower than symmetric encryption — usually used to secure keys, not bulk data

Common Asymmetric Algorithms:

- RSA – most widely used for secure data exchange and digital signatures
- ECC (Elliptic Curve Cryptography) – faster and more efficient at smaller key sizes
- Diffie-Hellman – used for secure key exchange, not encryption directly

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Hashing Algorithms

Modern Cryptography

It’s like a digital fingerprint: no matter how big the input, the hash is always the same length — and totally unique (ideally).

Hashing Algorithms

A one-way function that takes any input (like a file, message, or password) and produces a fixed-size string of characters — called a hash or digest.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

It’s like a digital fingerprint: no matter how big the input, the hash is always the same length — and totally unique (ideally).

Hashing Algorithms

A one-way function that takes any input (like a file, message, or password) and produces a fixed-size string of characters — called a hash or digest.

Key Properties:

- **One-way**: You can’t reverse a hash to get the original data.
- **Deterministic**: Same input always gives the same hash.
- **Collision-resistant**: Hard to find two different inputs that produce the same hash.
- **Fast**: Quickly calculates a digest, even for large files.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Modern Cryptography

Hashing algorithms don't encrypt — they verify. They prove the data hasn't changed, but you can't get the data back from the hash.

Hashing Algorithms

It's like a digital fingerprint: no matter how big the input, the hash is always the same length — and totally unique (ideally).

A one-way function that takes any input (like a file, message, or password) and produces a fixed-size string of characters — called a hash or digest.

Key Properties:

- **One-way**: You can't reverse a hash to get the original data.
- **Deterministic**: Same input always gives the same hash.
- **Collision-resistant**: Hard to find two different inputs that produce the same hash.
- **Fast**: Quickly calculates a digest, even for large files.

Hashing is like blending a smoothie — you can see what it became, but you can't reverse it to pull the banana and strawberries back out.

What Hashes Are Used For:

- Data integrity checks (detect tampering)
- Storing passwords securely (hashed, not plaintext)
- Digital signatures
- Checksums and file verification

Common Hashing Algorithms:

SHA-2 (e.g., SHA-256, SHA-512) – modern and secure
SHA-1 – outdated, broken (still seen in legacy systems)
MD5 – very fast but highly insecure (don't use for security)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

An encryption method where the same secret key is used to both encrypt and decrypt data, making it fast but dependent on secure key sharing.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

CHAPTER 6

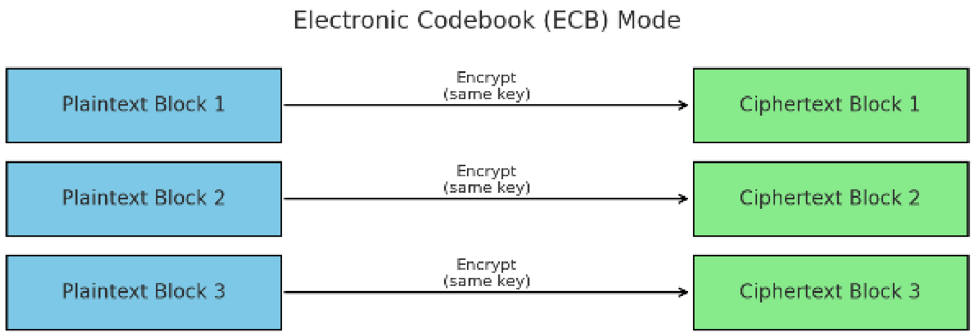
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

1. **Electronic Codebook (ECB) Mode** - Each block is encrypted independently with the same key.
   - **Simple but insecure** — identical plaintext blocks = identical ciphertext blocks.
   - **Not recommended** except for tiny, random data (e.g., encryption keys).
   - **Think**: Copy-paste patterns — visible in encrypted images.



CHAPTER 6

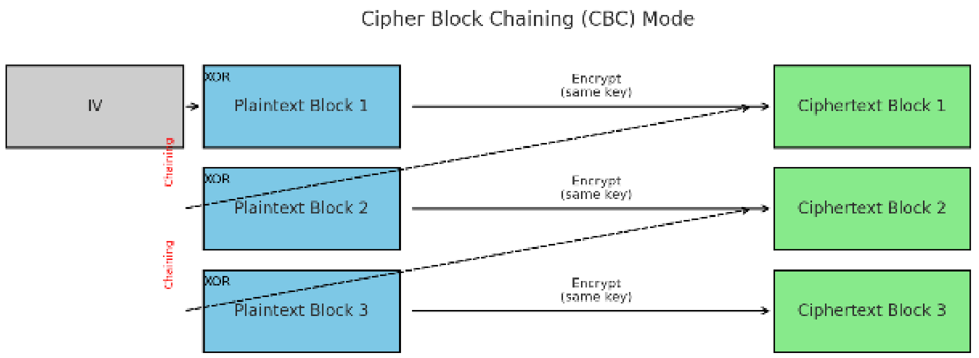
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

2. **Cipher Block Chaining (CBC) Mode** - Each plaintext block is XORed with the previous ciphertext block before encryption.
   - Requires an **IV (Initialization Vector)** for the first block.
   - **More secure** than ECB — hides patterns.
   - **Errors propagate** to the next block, which can be both a feature and a flaw.



CHAPTER 6

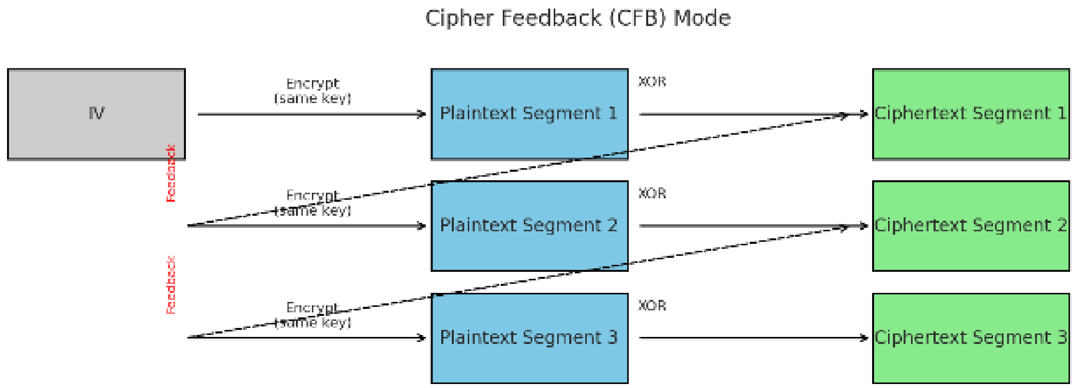
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

3. **Cipher Feedback (CFB) Mode** - Turns a block cipher into a stream cipher by feeding back part of the ciphertext into the next block's encryption.
   - Encrypts **smaller units** (e.g., 8 bits) at a time.
   - **Self-synchronizing** — useful for stream data.
   - Errors affect **two blocks** (not the whole stream).



CHAPTER 6

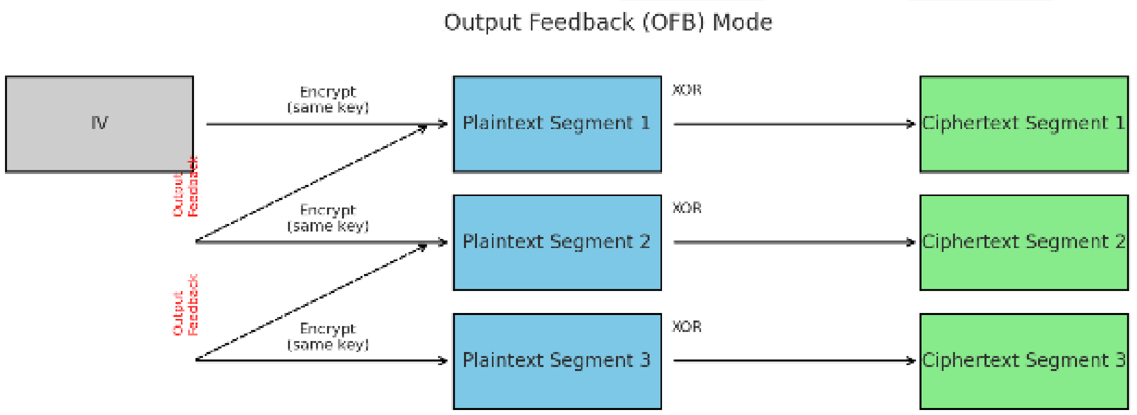
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

4. **Output Feedback (OFB) Mode** - Like CFB, but feeds the output of encryption, not the ciphertext, into the next block.
   - Also converts block cipher to **stream cipher**.
   - **No error propagation** — great for noisy channels.
   - Requires strict IV management.



CHAPTER 6

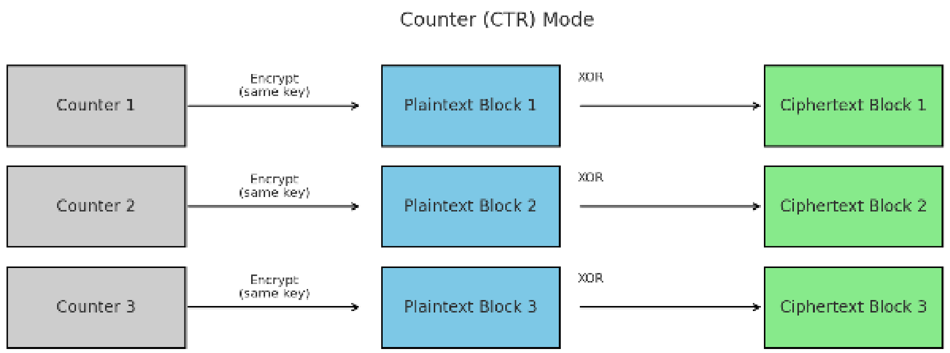
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

5. **Counter (CTR) Mode** - Uses a counter value that's encrypted and then XORed with the plaintext.
    - Can be **parallelized** (very fast).
    - Turns block cipher into **stream cipher**.
    - Each block gets a **unique counter value** — no repeats



CHAPTER 6

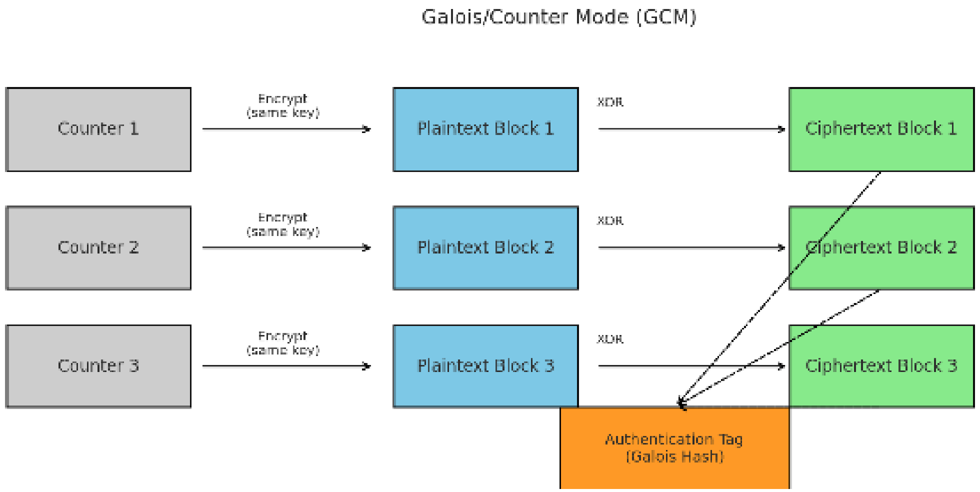
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

6. **Galois/Counter Mode (GCM)** - Combines CTR mode encryption with a MAC (Message Authentication Code) for integrity.
   - Provides **confidentiality and integrity** in one go.
   - **Widely used** in modern systems (e.g., TLS, SSH).
   - Efficient and secure if used correctly



CHAPTER 6

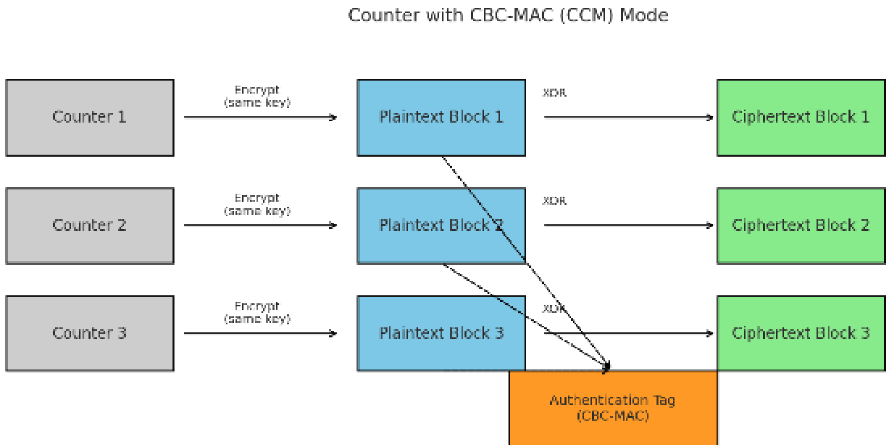
Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

7. **Counter with CBC-MAC (CCM) Mode** - Combines CTR for encryption and CBC-MAC for authentication.
   - Similar goal as GCM: **authenticated encryption**.
   - Common in constrained devices like **IoT and wireless networks**.
   - **More rigid and slower** than GCM, but still secure.



CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Block Cipher Modes of Operation

Define how blocks of plaintext are encrypted, especially when messages are longer than a single block. Each mode affects security, performance, and how errors propagate.

Mode	Type	Pattern Hiding	Error Propagation	Use Case
ECB	Block	❌ None	❌ None	Obsolete/simple
CBC	Block	✅ Good	⚠️ One block ahead	General use
CFB	Stream	✅ Good	⚠️ One block ahead	Streams
OFB	Stream	✅ Good	❌ None	Unreliable links
CTR	Stream	✅ Excellent	❌ None	High-speed apps
GCM	Stream	✅ + Integrity	❌ None	TLS, VPNs
CCM	Stream	✅ + Integrity	❌ None	IoT, Wi-Fi

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Data Encryption Standard

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Data Encryption Standard

A symmetric key block cipher developed in the 1970s by IBM and adopted by the U.S. government as a federal standard for data encryption in 1977.

Legacy:
- DES paved the way for stronger ciphers like 3DES and AES.
- Still important for understanding the history of encryption.

Symmetric Cryptography

Data Encryption Standard

A symmetric key block cipher developed in the 1970s by IBM and adopted by the U.S. government as a federal standard for data encryption in 1977.

Key Facts:

- **Block size**: 64 bits
- **Key size**: 56 bits (plus 8 bits for parity, total 64)
- **Encryption type**: Symmetric
- **Algorithm**: Feistel network with 16 rounds

DES was once the gold standard for encryption, but today it's considered broken and obsolete due to its short key length.

Why It's No Longer Secure:
- The 56-bit key is too short by modern standards.
- Can be brute-forced in hours or less with modern computing power.
- Was officially withdrawn as a federal standard in 2005.

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Triple DES

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It’s like putting your data through three locks instead of one.

Triple DES

Triple DES (3DES) is an enhancement of the original Data Encryption Standard (DES) that applies the DES algorithm three times to each data block to increase security.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Triple DES

It's like putting your data through three locks instead of one.

Triple DES (3DES) is an enhancement of the original Data Encryption Standard (DES) that applies the DES algorithm three times to each data block to increase security.

How It Works:

3DES encrypts each 64-bit block in one of two main ways:

Encrypt → Decrypt → Encrypt using either:

- **3 different keys** (most secure)
- **2 keys** (less secure but still better than DES)

C = E_k3(D_k2(E_k1(P)))

Key Sizes:

- 168 bits (3 independent 56-bit keys)
- 112 bits (2 keys reused: K1 = K3)

Strengths:

- Much stronger than regular DES
- Used in legacy systems like banking (e.g.,

Weaknesses:

- Slow (3 times the work of DES)
- Still vulnerable to certain attacks like meet-in-the-middle
- Retired by NIST — officially deprecated after 2023

3DES was a clever way to extend DES's life, but today it's outdated — being replaced by AES in nearly all modern

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

International Data Encryption Algorithm (IDEA)

It was widely used in early versions of PGP (Pretty Good Privacy) for secure email and file encryption.

Symmetric Cryptography

International Data Encryption Algorithm (IDEA)

A symmetric key block cipher designed to be a secure and efficient alternative to DES, originally developed in the early 1990s.

It was widely used in early versions of PGP (Pretty Good Privacy) for secure email and file encryption.

Symmetric Cryptography

International Data Encryption Algorithm (IDEA)

A symmetric key block cipher designed to be a secure and efficient alternative to DES, originally developed in the early 1990s.

Key Characteristics:

- **Block size**: 64 bits
- **Key size**: 128 bits
- **Rounds**: 8.5 rounds of encryption
- **Structure**: Uses modular addition, bitwise XOR, and multiplication modulo $2^{16} + 1$ for confusion and diffusion

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It was widely used in early versions of PGP (Pretty Good Privacy) for secure email and file encryption.

International Data Encryption Algorithm (IDEA)

A symmetric key block cipher designed to be a secure and efficient alternative to DES, originally developed in the early 1990s.

Key Characteristics:

- **Block size**: 64 bits
- **Key size**: 128 bits
- **Rounds**: 8.5 rounds of encryption
- **Structure**: Uses modular addition, bitwise XOR, and multiplication modulo $2^{16} + 1$ for confusion and diffusion

Weaknesses:

- Slower than some modern ciphers like AES
- Patent restrictions (originally) limited widespread adoption
- Mostly considered legacy now

Strengths:

- Very strong for its time — no practical attacks known against full IDEA
- More secure than DES, and resistant to differential and linear cryptanalysis

IDEA was a robust and innovative cipher for its era, known for strong encryption and resistance to known attacks — but it's largely been replaced by more modern standards like AES.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Blowfish

Symmetric Cryptography

It’s a flexible and efficient algorithm widely used in early encryption software.

Blowfish

A symmetric key block cipher designed by **Bruce Schneier** in 1993 to be fast, free, and secure, especially as a replacement for DES.

Symmetric Cryptography

It's a flexible and efficient algorithm widely used in early encryption software.

Blowfish

A symmetric key block cipher designed by **Bruce Schneier** in 1993 to be fast, free, and secure, especially as a replacement for DES.

Key Characteristics:

- **Block size**: 64 bits
- **Key size**: Variable — from 32 bits to 448 bits
- **Rounds**: 16
- **Structure**: Feistel network with complex key scheduling

Strengths:

- Fast and compact — ideal for embedded systems
- Public domain — no patents or licensing fees
- Highly configurable key size supports strong encryption

Weaknesses:

- 64-bit block size is now considered too small for modern use (susceptible to birthday attacks on large volumes of data)
- Replaced by more modern algorithms like AES and Twofish

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

SKIPJACK

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It was part of a government-backed plan to allow strong encryption with a built-in backdoor for law enforcement

SKIPJACK

A symmetric key block cipher developed by the U.S. National Security Agency (NSA) in the early 1990s for use in the controversial **Clipper Chip** encryption initiative.

Symmetric Cryptography

It was part of a government-backed plan to allow strong encryption with a built-in backdoor for law enforcement

SKIPJACK

A symmetric key block cipher developed by the U.S. National Security Agency (NSA) in the early 1990s for use in the controversial **Clipper Chip** encryption initiative.

Key Characteristics:

- **Block size**: 64 bits
- **Key size**: 80 bits
- **Rounds**: 32
- **Structure**: Unbalanced Feistel network

Strengths (technically):

- Strong for its time, and later declassified with no major flaws found
- Simple and lightweight

Controversies:

- Initially classified by the NSA, causing widespread distrust
- Tied to the Clipper Chip, which was rejected by the public due to privacy concerns
- The idea of key escrow (government-held access keys) was heavily criticized

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Rivest Ciphers

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Rivest Ciphers

The Rivest Ciphers (RC) are a family of symmetric encryption algorithms designed by Ron Rivest. Each version represents a different approach to balancing speed, security, and flexibility.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Rivest Ciphers

The Rivest Ciphers (RC) are a famil
Rivest. Each version represents a d
flexibility.

RC6 - Block Cipher (AES Finalist)

- **Block size**: 128 bits
- **Key size**: 128, 192, or 256 bits
- **Rounds**: 20
- **Use case**: Designed as a candidate for the AES competition
- **Status**: Strong and secure, but AES was ultimately selected over RC6

RC4 - Stream Cipher

- **Type**: Stream cipher
- **Key size**: Variable (up to 2048 bits)
- **Use case**: Was widely used in SSL/TLS, WEP, WPA
- **Status**: Deprecated — vulnerable to biases in its keystream; no longer considered secure

RC5 - Block Cipher

- **Block size**: Variable (typically 64 or 128 bits)
- **Key size**: Variable (up to 2040 bits)
- **Rounds**: Variable (commonly 12 or 16)
- **Strength**: Highly flexible — allows tuning of key size, block size, and number of rounds
- **Status**: Secure in general, but newer algorithms have overtaken it in popularity

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Advanced Encryption Standard (AES)

Symmetric Cryptography

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

Advanced Encryption Standard (AES)

The current U.S. government standard for symmetric key encryption, and it’s one of the most widely used and trusted encryption algorithms in the world.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Advanced Encryption Standard (AES)

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

The current U.S. government standard for symmetric key encryption, and it's one of the most widely used and trusted encryption algorithms in the world.

Key Characteristics:

- **Block size**: 128 bits
- **Key sizes**: 128, 192, or 256 bits
- **Rounds**:
  - 10 for 128-bit keys
  - 12 for 192-bit keys
  - 14 for 256-bit keys
- **Structure**: Based on the Substitution-Permutation Network (not Feistel)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

Advanced Encryption Standard (AES)

The current U.S. government standard for symmetric key encryption, and it's one of the most widely used and trusted encryption algorithms in the world.

How AES Works (Simplified):

Each round of AES performs 4 core operations:

1. **SubBytes** – Substitutes each byte using a predefined S-box (adds confusion)
2. **ShiftRows** – Shifts rows of the matrix (adds diffusion)
3. **MixColumns** – Mixes data in columns (adds more diffusion)
4. **AddRoundKey** – Combines the block with a round key (key-dependent transformation)

AES works on a 4x4 matrix of bytes, often called the state, transforming it over multiple rounds until it's scrambled beyond recognition.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

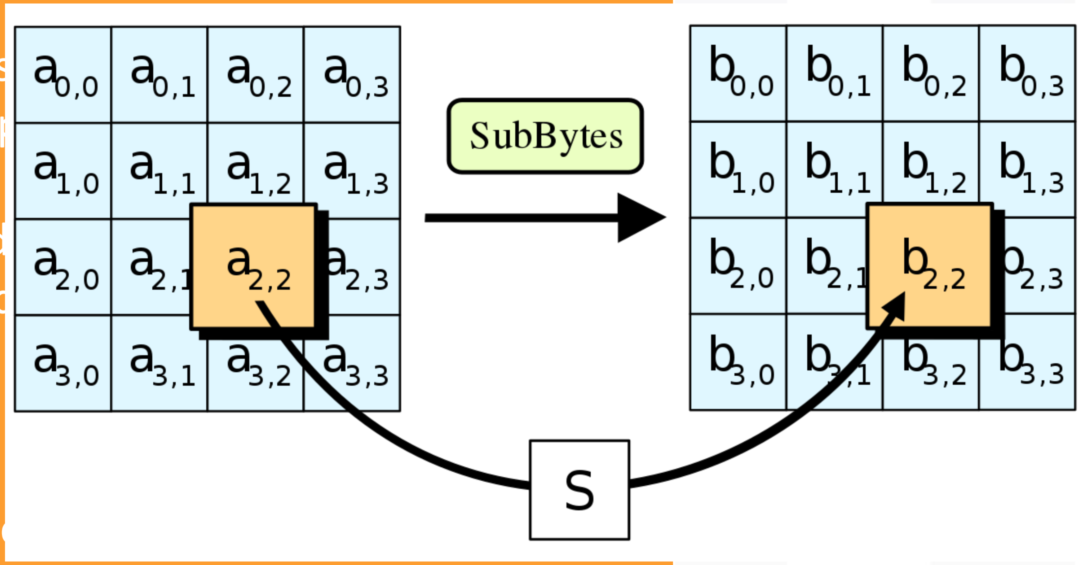
Advanced Encryption Standard (AES)

The current U.S. government standard for symmetric key encryption, and it's one of the most widely used and trusted encryption algorithms in the world.

How AES Works (Simplified):

Each round of AES performs 4 core operations

1. **SubBytes** – Substitutes each byte using a confusion)
2. **ShiftRows** – Shifts rows of the matrix (add
3. **MixColumns** – Mixes data in columns (add
4. **AddRoundKey** – Combines the block with transformation)



AES works on a 4x4 matrix of bytes, often call multiple rounds until it's scrambled beyond recognition.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

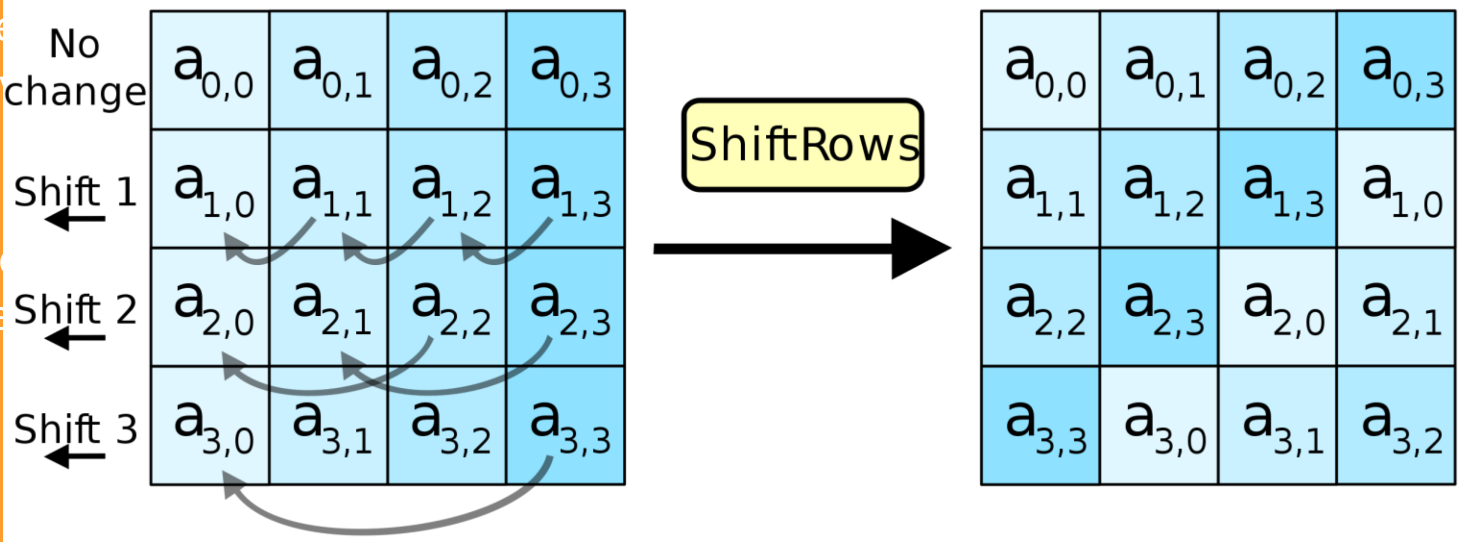
Advanced Encryption Standard (AES)

The current U.S. government standard for symmetric key encryption, and it's one of the most widely used and trusted encryption algorithms in the world.

How AES Works (Simplified):

Each round of AES performs 4 core

1. **SubBytes** – Substitutes each b confusion)
2. **ShiftRows** – Shifts rows of the
3. **MixColumns** – Mixes data in c
4. **AddRoundKey** – Combines the transformation)



AES works on a 4x4 matrix of byte multiple rounds until it's scrambled beyond recognition.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Advanced Encryption Standard (AES)

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

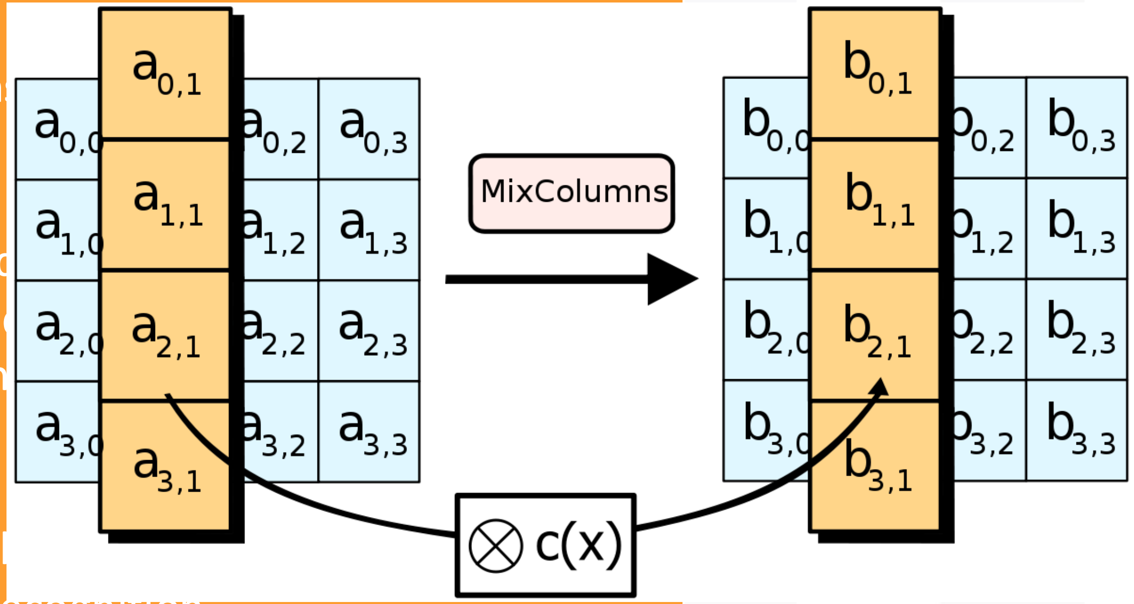
The current U.S. government standard for symmetric key encryption, and it's one of the most widely used and trusted encryption algorithms in the world.

How AES Works (Simplified):

Each round of AES performs 4 core operation

1. **SubBytes** – Substitutes each byte using a confusion)
2. **ShiftRows** – Shifts rows of the matrix (ad
3. **MixColumns** – Mixes data in columns (ad
4. **AddRoundKey** – Combines the block with transformation)

AES works on a 4x4 matrix of bytes, often cal multiple rounds until it's scrambled beyond recognition.



CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

Advanced Encryption Standard (AES)

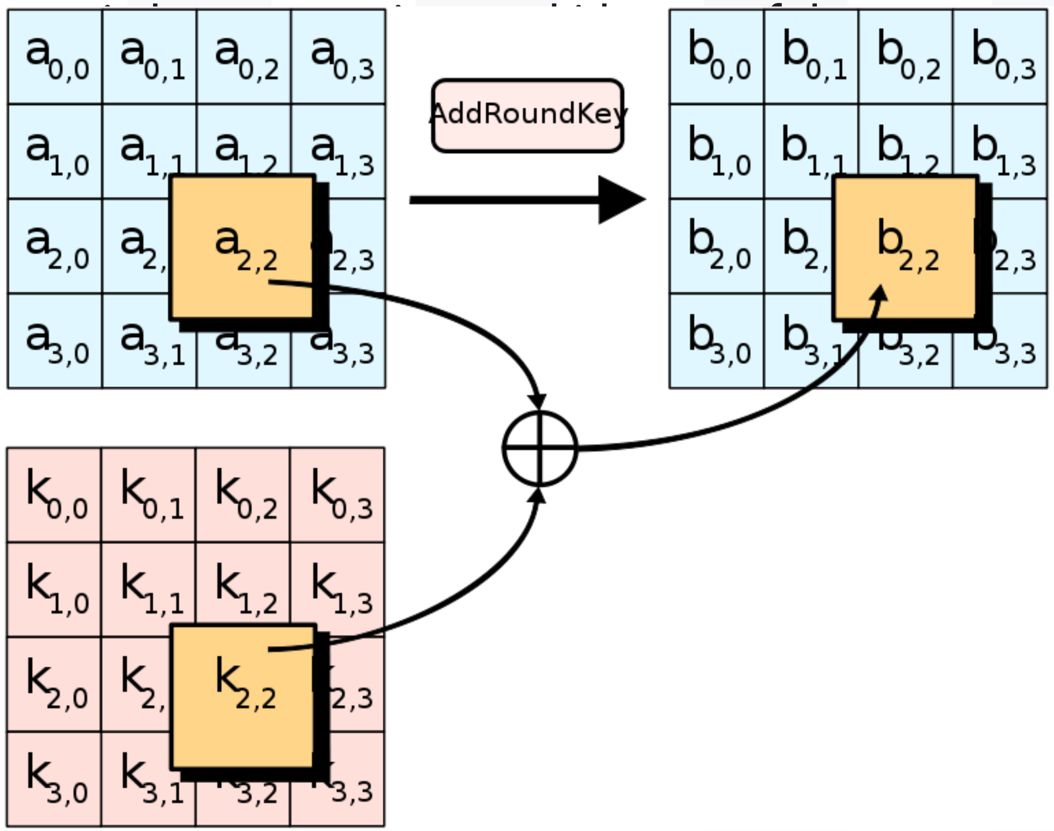
The current U.S. government standard for sym
most widely used and trusted encryption algor

How AES Works (Simplified):

Each round of AES performs 4 core operations:

1. **SubBytes** – Substitutes each byte using a pred
confusion)
2. **ShiftRows** – Shifts rows of the matrix (adds di
3. **MixColumns** – Mixes data in columns (adds m
4. **AddRoundKey** – Combines the block with a ro
transformation)

AES works on a 4x4 matrix of bytes, often called t
multiple rounds until it's scrambled beyond recog



CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

It replaced DES and 3DES due to their weaknesses, offering stronger security and better performance.

Advanced Encryption Standard (AES)

The current U.S. government standard for symmetric key encryption, and it's one of the most widely used and trusted encryption algorithms in the world.

How AES Works (Simplified):

Each round of AES performs 4 core operations:

1. **SubBytes** – Substitutes each byte using a predefined S-box (adds confusion)
2. **ShiftRows** –
3. **MixColumns**
4. **AddRoundK**
   transformation)

AES works on a 4x4 matrix of bytes, often called the state, transforming it over multiple rounds until it's scrambled beyond recognition.

Strengths:

- Fast and efficient in both hardware and software
- Resistant to all known practical attacks
- Approved for top-secret U.S. government data (when using 192- or 256-bit keys)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

CAST

CAST was developed in the 1990s and became a standard in some secure applications, including versions of PGP (Pretty Good Privacy).

Symmetric Cryptography

CAST

A family of symmetric key block ciphers designed for flexibility and security, named after its creators Carlisle Adams and Stafford Tavares (hence the name CAST).

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

CAST was developed in the 1990s and became a standard in some secure applications, including versions of PGP (Pretty Good Privacy).

CAST

A family of symmetric key block ciphers designed for flexibility and security, named after its creators Carlisle Adams and Stafford Tavares (hence the name CAST).

Key Characteristics:

- **Block size**: 64 bits (CAST-128) or 128 bits (CAST-256)
- **Key size**:
  - CAST-128: 40 to 128 bits
  - CAST-256: 128, 160, 192, 224, or 256 bits
- **Structure**: Feistel network with variable rounds (12 or 16)

Limitations:
- CAST-128's 64-bit block size is considered small by modern standards
- Less commonly used today in favor of AES and other modern algorithms

Strengths:
- Designed to resist known cryptanalytic attacks, including differential and linear cryptanalysis
- CAST-128 is fast and efficient — used in PGP 6 and 7
- CAST-256 was submitted as a candidate for the AES competition (but not selected)

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Comparison of Symmetric Encryption Algorithms

Algorithm	Block Size	Key Size	Rounds	Security	Status
DES	64 bits	56 bits	16	Broken (brute force)	Obsolete
3DES	64 bits	112/168 bits	48 (3 x 16)	Legacy, secure but slow	Legacy
AES	128 bits	128/192/256 bits	10/12/14	Modern, very secure	Current Standard
Blowfish	64 bits	32-448 bits	16	Secure but 64-bit block size limits	Still used in some apps
IDEA	64 bits	128 bits	8.5	Strong but outdated	Replaced by AES
CAST-128	64 bits	40-128 bits	12 or 16	Secure but aging	Used in older PGP
RC5	Variable	0-2040 bits	Variable	Flexible, less common today	Rarely used
RC6	128 bits	128/192/256 bits	20	AES finalist, strong	Not selected as AES, but secure

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Symmetric Key Management

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Symmetric Cryptography

Symmetric Key Management

Symmetric key management is all about **securely creating, distributing, storing, and recovering encryption keys**. While symmetric encryption is fast, key management is its Achilles' heel — and where security often fails.

Concept	What It Is	Strengths	Weaknesses / Risks
Creation and Distribution	Generating secure keys and getting them to both parties	Fast, under your control	Must ensure secure delivery; if intercepted = compromise
Offline Distribution	Physically handing over the key (e.g., USB, paper)	High control, no network exposure	Inconvenient, not scalable; risk of loss or theft
Public Key Encryption	Use asymmetric encryption (e.g., RSA) to securely send symmetric key	Solves the key distribution problem	Slower; adds complexity
Diffie–Hellman	A key exchange method that securely establishes a shared key over an insecure channel	No prior key sharing needed; secure	Vulnerable to man-in-the-middle without authentication
Storage	How and where keys are kept (e.g., HSMs, encrypted databases)	Ensures availability	If storage is compromised, all encrypted data is at risk
Destruction	Securely erasing keys after use or expiration	Prevents unauthorized reuse	Must ensure thorough deletion (e.g., zeroize memory)
Key Escrow and Recovery	A third party keeps a copy of the key for recovery or oversight	Helps with backup, compliance	Risk of abuse, unauthorized access, loss of trust
Fair Cryptosystems	All parties involved can access the key only with mutual consent (e.g., both parties present)	Balances access and control	Requires coordination, not ideal for emergencies
Escrowed Encryption Standard (EES)	U.S. government's 1990s attempt at encryption with built-in backdoor (e.g., SKIPJACK)	Government access to encrypted comms	Rejected due to privacy and trust concerns

2025 CISSP MENTOR PROGRAM

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Life Cycle

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Life Cycle

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

1. **Planning & Selection**

- Choose appropriate algorithms, key lengths, and protocols based on risk, compliance, and performance needs.
- Example: AES-256 for high-security data.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

2. **Implementation**

- Deploy the cryptographic controls in systems and applications.
- Ensure secure configuration and integration (e.g., using TLS correctly).

> Think of it as the “birth-to-death” process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

3. **Key Generation**

- Generate strong, random keys using cryptographically secure random number generators.
- Follow best practices for entropy and key strength.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the "birth-to-death" process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

4. **Key Distribution**

- Share symmetric keys securely (offline, asymmetric encryption, Diffie-Hellman).
- Ensure only intended parties receive the key.

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

5. **Key Usage**

- Use keys for their intended purpose only (encryption, signing, etc.).
- Apply least privilege and access controls.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the "birth-to-death" process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

6. **Key Storage**

- Store keys securely using HSMs, encrypted files, or key management systems (KMS).
- Prevent unauthorized access and leakage.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

7. **Key Rotation / Renewal**

- Periodically regenerate and replace keys to limit the damage if a key is compromised.
- Often driven by policy, compliance, or system changes.

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

8. **Key Revocation** - Invalidate a key before its scheduled expiration (e.g., if compromised).

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Cryptographic Life Cycle

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

8. **Key Revocation** - Invalidate a key before its scheduled expiration (e.g., if compromised).
9. **Key Expiry** - Keys should have defined lifespans — auto-expire after a certain period.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

Think of it as the “birth-to-death” process of cryptographic tools and secrets.

Cryptographic Life Cycle

The Cryptographic Life Cycle refers to the stages that cryptographic systems and keys go through — from creation to retirement — to ensure ongoing security, integrity, and compliance.

Key Phases of the Cryptographic Life Cycle

8. **Key Revocation** - Invalidate a key before its scheduled expiration (e.g., if compromised).
9. **Key Expiry** - Keys should have defined lifespans — auto-expire after a certain period.
10. **Key Destruction** - Securely erase keys so they can never be recovered (zeroization, shredding memory).

The cryptographic life cycle ensures that encryption and key management remain secure and effective over time — and failure at any stage can undermine the whole system.

CHAPTER 6

Cryptography and Symmetric Key Algorithms

CONGRATULATIONS!

That wasn't so bad, was it?

Be sure to review the "Summary", "Study Essentials", "Written Lab", and "Review Questions" from the book.

Next Up: Chapter 7 PKI and Cryptographic Applications