
CRYPTOGRAPHY
-ATHARVA KATKAR

TABLE OF CONTENTS

- Risks

Polyalphabetic Substitution Cipher

- Vigenère Cipher

Transposition Ciphers

- Definition
- Rail Fence Cipher

Product Ciphers

- Definition

Classical Cryptanalysis

- Frequency Analysis
- Known Plaintext Attack
- Risks & Limitations of Classical Cryptography
- MITRE ATT&CK Mapping

---

10. Modern Symmetric-Key Cryptography

- Introduction
- Characteristics

Block vs Stream Ciphers

- Block Ciphers
- Stream Ciphers

Data Encryption Standard (DES)

- Overview
- Working Principle
- Weaknesses
- Current Status

Triple DES (3DES)

- Overview
- Strengths
- Weaknesses
- Current Status

Advanced Encryption Standard (AES)

- Overview
- Key Sizes
- Strengths
- Usage

Modes of Operation

- ECB
- CBC
- GCM
- Key Management Challenges
- Symmetric Cryptography Attacks
- MITRE ATT&CK Mapping

---

11. Asymmetric (Public-Key) Cryptography

- Introduction
- Characteristics

Public Key Infrastructure (PKI)

- Definition
- Core PKI Components

RSA Algorithm

- Overview
- Working Principle
- Key Sizes
- Strengths
- Weaknesses

Diffie-Hellman Key Exchange

- Definition
- Characteristics
- Weaknesses

Elliptic Curve Cryptography (ECC)

- Overview
- Advantages
- Usage

Digital Signatures

- Purpose
- Working
- Hybrid Cryptosystems
- Asymmetric Cryptography Attacks
- MITRE ATT&CK Mapping

---

12. Hash Functions & Message Integrity

- Introduction
- Characteristics

Common Hash Algorithms

- MD5

- SHA-1
- SHA-2 Family
- SHA-3

Password Hashing

- Password Storage
- Salting
- Key Stretching

Message Authentication Code (MAC)

- Definition
- HMAC

Hash-Based Attacks

- Collision Attack
- Birthday Attack
- Rainbow Table Attack
- Risks of Weak Hashing
- MITRE ATT&CK Mapping

---

13. Cryptographic Attacks & Vulnerabilities

- Introduction

Attack Types

- Brute-Force Attack
- Dictionary Attack
- Man-in-the-Middle Attack
- Known Plaintext Attack
- Chosen Plaintext Attack

- Padding Oracle Attack
- Side-Channel Attacks
- Weak Random Number Generation
- MITRE ATT&CK Mapping

---

14. Cryptography Best Practices

- Use Strong, Modern Algorithms
- Secure Key Management
- Authenticated Encryption
- Proper Certificate Management

---

15. Cryptographic Standards

- Common Standards
- Compliance Frameworks

---

16. Real-World Cryptography Failures

- Weak SSL/TLS Configuration
- Password Hash Breach
- Random Number Generator Failure

---

17. Cryptography in CEH Attack Lifecycle

Conclusion

References

1. Introduction to Cryptography

1.1 Definition of Cryptography

Cryptography is the science of protecting information by transforming it into an unreadable format so that only authorized parties can access it.

In cybersecurity, cryptography ensures:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

CEH Focus:

- How cryptography works
- Where it fails
- How attackers exploit weak implementations

---

2. Objectives of Cryptography

The primary objectives of cryptography are:

2.1 Confidentiality

Ensures that data is only accessible to authorized users.
Examples:

- Encrypting sensitive files
- HTTPS communication

2.2 Integrity

Ensures data is not altered during transmission or storage.
Examples:

- Hashing

- Message Authentication Codes (MAC)

2.3 Authentication

Verifies the identity of users or systems.
Examples:

- Digital certificates
- Public key authentication

2.4 Non-Repudiation

Prevents a sender from denying an action.
Examples:

- Digital signatures

---

3. Importance of Cryptography in Cybersecurity

Cryptography is used in:

- Secure communications (TLS/SSL)
- Data-at-rest protection
- Digital identities
- Secure authentication systems

Without cryptography:

- Data can be intercepted
- Messages can be modified
- Identities can be spoofed

---

4. Cryptographic Terminology (CEH Exam Focus)

Term	Description
Plaintext	Original readable data
Ciphertext	Encrypted unreadable data
Encryption	Converting plaintext to ciphertext
Decryption	Converting ciphertext to plaintext
Cipher	Algorithm used for encryption
Key	Secret value controlling encryption

---

5. Types of Cryptography

5.1 Symmetric Cryptography

- Same key for encryption and decryption
- Fast and efficient

5.2 Asymmetric Cryptography

- Uses public and private key pairs
- Slower but more secure for key exchange

5.3 Hash Functions

- One-way transformation
- Used for integrity verification

(Each type will be covered in separate detailed parts.)

---

6. Cryptographic Attacks

Attackers target cryptography by:

- Breaking weak algorithms

- Exploiting poor key management
- Abusing implementation flaws

Note: Cryptography often fails not because of algorithms, but because of human error and misconfiguration.

---

7. Risks of Weak Cryptography

- Data breaches
- Credential theft
- Man-in-the-Middle attacks
- Legal and compliance failures

---

8. MITRE ATT&CK Mapping

Activity	MITRE Tactic	Technique ID	Description
Weak Encryption Abuse	Credential Access	T1552	Unsecured Credentials
MITM	Credential Access	T1557	Man-in-the-Middle
Certificate Abuse	Defense Evasion	T1553	Subvert Trust Controls

Introduction to Classical Cryptography

Classical cryptography refers to early encryption techniques developed before modern computers. These techniques form the foundation of modern cryptography and are still tested in CEH to understand encryption logic and cryptanalysis.

Classical ciphers rely on:

- Character substitution
- Character rearrangement
- Simple mathematical operations

---

2. Substitution Ciphers

2.1 Definition

A substitution cipher replaces each character in plaintext with another character according to a fixed rule.

2.2 Monoalphabetic Substitution Cipher

Working Principle:

- One-to-one mapping between plaintext and ciphertext alphabets
- Same substitution throughout the message

Example:

- Plaintext: ATTACK
- Ciphertext: QZZQEA

Weaknesses:

- Frequency analysis easily breaks it
- Patterns remain visible

2.3 Caesar Cipher

Definition:
A Caesar cipher shifts characters by a fixed number of positions.

Example (Shift = 3):

- Plaintext: HELLO
- Ciphertext: KHOOR

Advantages:

- Simple
- Easy to implement

Disadvantages:

- Only 25 possible keys
- Easily brute-forced

Risks:

- No security against modern attacks
- Educational use only

---

3. Polyalphabetic Substitution Cipher

3.1 Vigenère Cipher

Working Principle:

- Uses a keyword
- Multiple substitution alphabets

Example:

- Plaintext: ATTACK
- Key: LEMON
- Ciphertext: LXFOPV

Strengths:

- Reduces frequency patterns

Weaknesses:

- Vulnerable to Kasiski examination

---

4. Transposition Ciphers

4.1 Definition

Transposition ciphers rearrange characters without changing them.

4.2 Rail Fence Cipher

Example:

- Plaintext: HELLOWORLD
- Ciphertext: HLOOLELWRD

Weakness:

- Letter frequencies remain unchanged

---

5. Product Ciphers

5.1 Definition

Combination of:

- Substitution
- Transposition

Modern ciphers such as AES and DES are examples of product ciphers.

---

6. Classical Cryptanalysis

6.1 Frequency Analysis

- Analyzes letter frequency

- Most common English letter = E

6.2 Known Plaintext Attack

- Attacker knows part of the plaintext

---

7. Risks & Limitations of Classical Cryptography

- No key management
- No authentication
- Easily breakable

---

8. MITRE ATT&CK Mapping

Concept	MITRE Tactic	Technique
Weak Encryption	Credential Access	T1552
Brute Force	Credential Access	T1110

Modern Symmetric-Key Cryptography

1,Introduction to Symmetric-Key Cryptography

Symmetric-key cryptography uses the same secret key for both encryption and decryption. It is widely used due to its speed and efficiency, especially for encrypting large volumes of data.

CEH Focus:

- Algorithms
- Key sizes
- Strengths and weaknesses
- Real-world usage

---

2. Characteristics of Symmetric Cryptography

- Single shared secret key
- Fast encryption and decryption
- Requires secure key distribution
- Less computational overhead

---

3. Block Ciphers vs Stream Ciphers

3.1 Block Ciphers

- Encrypt fixed-size blocks of data
- Common block sizes: 64-bit or 128-bit

Examples:

- DES
- AES

3.2 Stream Ciphers

- Encrypt data bit-by-bit or byte-by-byte

Examples:

- RC4

---

4. Data Encryption Standard (DES)

4.1 Overview

- DES is a 64-bit block cipher with a 56-bit key developed in the 1970s

4.2 Working Principle

- 16 rounds of encryption
- Feistel structure

4.3 Weaknesses

- Short key length
- Vulnerable to brute-force attacks

4.4 Current Status

- Considered insecure
- Deprecated

---

5. Triple DES (3DES)

5.1 Overview

- 3DES applies DES three times with different keys

5.2 Strengths

- Improved security over DES

5.3 Weaknesses

- Slow
- Vulnerable to meet-in-the-middle attacks

5.4 Current Status

- Being phased out

---

6. Advanced Encryption Standard (AES)

6.1 Overview

- AES is the current industry-standard symmetric encryption algorithm

6.2 Key Sizes

- 128-bit
- 192-bit
- 256-bit

6.3 Strengths

- Strong security
- Efficient
- Resistant to known attacks

6.4 Usage

- Disk encryption
- VPNs
- HTTPS

---

7. Modes of Operation

7.1 ECB (Electronic Codebook)

- Identical plaintext blocks → identical ciphertext

- Not secure

7.2 CBC (Cipher Block Chaining)

- Uses Initialization Vector (IV)
- More secure than ECB

7.3 GCM (Galois/Counter Mode)

- Provides confidentiality and integrity
- Preferred mode

---

8. Key Management Challenges

- Secure key distribution
- Key storage
- Key rotation

Note: Key compromise = data compromise

---

9. Symmetric Cryptography Attacks

- Brute-force attacks
- Known plaintext attacks
- Weak mode exploitation

---

10. MITRE ATT&CK Mapping

Concept	MITRE Tactic	Technique ID
Weak Cipher Use	Credential Access	T1552
Key Exposure	Credential Access	T1555

Asymmetric (Public-Key) Cryptography

1.Introduction to Asymmetric Cryptography

Asymmetric cryptography uses two mathematically related keys:

- **Public Key** – shared openly
- **Private Key** – kept secret

It solves the key distribution problem present in symmetric cryptography and is widely used for:

- Secure key exchange
- Authentication
- Digital signatures

---

2. Characteristics of Asymmetric Cryptography

- Uses two different keys
- Slower than symmetric encryption
- Enables secure communication over untrusted networks
- Often combined with symmetric cryptography in real systems

---

3. Public-Key Infrastructure (PKI)

3.1 Definition

PKI is a framework that manages:

- Digital certificates
- Public-private key pairs
- Trust relationships

3.2 Core PKI Components

- Certificate Authority (CA)
- Registration Authority (RA)
- Digital certificates
- Certificate Revocation Lists (CRL)

---

4. RSA (Rivest–Shamir–Adleman)

4.1 Overview

- Most widely used asymmetric encryption algorithm

4.2 Working Principle

- Based on factorization of large prime numbers
- Key pair generated using mathematical operations

4.3 Key Sizes

- 1024-bit (deprecated)
- 2048-bit (standard)
- 4096-bit (high security)

4.4 Strengths

- Well-studied
- Widely supported

4.5 Weaknesses

- Slow
- Vulnerable if key size is small
- Poor random number generation can break security

---

5. Diffie-Hellman Key Exchange

5.1 Definition

- Allows two parties to securely exchange a symmetric key over an insecure channel

5.2 Characteristics

- Does not encrypt data directly
- Used for key agreement

5.3 Weaknesses

- Vulnerable to Man-in-the-Middle (MITM) attacks without authentication

---

6. Elliptic Curve Cryptography (ECC)

6.1 Overview

- Provides strong security with smaller key sizes

6.2 Advantages

- Faster than RSA
- Smaller keys
- Lower power consumption (ideal for mobile)

6.3 Usage

- Mobile devices
- IoT
- TLS

---

7. Digital Signatures

7.1 Purpose

- Authentication
- Integrity

- Non-repudiation

7.2 Working

1. Hash the message
2. Encrypt hash with private key
3. Verify using public key

---

8. Hybrid Cryptosystems

Real-world systems combine:

- Asymmetric cryptography (key exchange)
- Symmetric cryptography (data encryption)

Example:

- HTTPS (TLS)

---

9. Asymmetric Cryptography Attacks

- Man-in-the-Middle
- Weak key sizes
- Poor certificate validation

---

10. MITRE ATT&CK Mapping

Concept	MITRE Tactic	Technique ID
Certificate Abuse	Defense Evasion	T1553
MITM	Credential Access	T1557
Weak Key Use	Credential Access	T1552

Hash Functions & Message Integrity

---

1. Introduction to Hash Functions

Hash functions are cryptographic algorithms that transform input data of any size into a fixed-length output, called a hash value or message digest.

Hashing is primarily used to ensure:

- Data integrity
- Password protection
- Digital signatures

---

2. Characteristics of Cryptographic Hash Functions

A secure hash function must satisfy:

- Deterministic – Same input → same hash
- Fast computation
- Preimage resistance – Cannot derive input from hash
- Collision resistance – No two inputs produce the same hash
- Avalanche effect – Small input change → large output change

---

3. Common Hash Algorithms

3.1 MD5 (Message Digest 5)

Overview:

- Produces 128-bit hash
- Widely used historically

Weaknesses:

- Collision attacks exist
- Considered broken

Current Status:

- ❌ Not secure for cryptographic use

3.2 SHA-1 (Secure Hash Algorithm 1)

Overview:

- Produces 160-bit hash

Weaknesses:

- Vulnerable to collision attacks

Current Status:

- ❌ Deprecated

3.3 SHA-2 Family

Includes:

- SHA-256
- SHA-384
- SHA-512

Strengths:

- Strong collision resistance
- Widely adopted

Usage:

- Digital signatures
- TLS
- File integrity

3.4 SHA-3

- Based on Keccak algorithm
- Alternative to SHA-2
- Resistant to length extension attacks

---

4. Hashing Passwords

4.1 Password Storage

- Passwords are stored as hashes
- Prevents plaintext password storage

4.2 Salting

- Random value added before hashing
- Prevents rainbow table attacks

4.3 Key Stretching

- Increases computational cost
- Examples: PBKDF2, bcrypt

---

5. Message Authentication Code (MAC)

5.1 Definition

MAC ensures:

- Integrity
- Authentication

5.2 HMAC

- Combines hash function + secret key
- Resistant to tampering

---

6. Hash-Based Attacks

6.1 Collision Attack

- Two different inputs → same hash

6.2 Birthday Attack

- Exploits probability of collisions

6.3 Rainbow Table Attack

- Precomputed hashes for password cracking

---

7. Risks of Weak Hashing

- Password compromise
- Forged digital signatures
- Data integrity loss

---

8. MITRE ATT&CK Mapping

Concept	MITRE Tactic	Technique ID
Weak Hash Use	Credential Access	T1552
Password Cracking	Credential Access	T1110

Cryptographic Attacks & Vulnerabilities

---

1. Introduction to Cryptographic Attacks

Cryptographic attacks exploit weak algorithms, poor implementations, improper configurations, and human errors rather than breaking strong algorithms mathematically.

CEH emphasizes understanding how cryptography fails in real-world systems.

---

2. Brute-Force Attack

2.1 Definition

An attacker tries all possible keys or passwords until the correct one is found.

2.2 Factors Affecting Brute Force

- Key length
- Key randomness
- Computational power

2.3 Mitigation

- Strong key lengths
- Rate limiting
- Account lockout

---

3. Dictionary Attack

3.1 Definition

Uses a predefined list of common passwords or phrases.

3.2 Mitigation

- Strong password policies
- Salting and hashing

---

4. Man-in-the-Middle (MITM) Attack

4.1 Definition

An attacker intercepts and possibly alters communication between two parties.

4.2 Cryptographic Context

- Exploits weak key exchange
- Poor certificate validation

4.3 Mitigation

- Proper certificate validation
- Mutual authentication

---

5. Known Plaintext Attack

5.1 Definition

The attacker knows part of the plaintext and its corresponding ciphertext.

5.2 Mitigation

- Strong encryption algorithms
- Random initialization vectors (IVs)

---

6. Chosen Plaintext Attack

6.1 Definition

The attacker chooses plaintexts and observes the resulting ciphertexts.

---

7. Padding Oracle Attack

7.1 Definition

Exploits padding error messages in block cipher modes to reveal plaintext.

7.2 Mitigation

- Use authenticated encryption modes (GCM)
- Return generic error messages

---

8. Side-Channel Attacks

8.1 Types

- Timing attacks
- Power analysis
- Electromagnetic leakage

8.2 Mitigation

- Constant-time algorithms
- Hardware-based protections

---

9. Weak Random Number Generation

9.1 Risk

Predictable keys, nonces, and initialization vectors.

9.2 Mitigation

- Use cryptographically secure random number generators

---

10. MITRE ATT&CK Mapping

Attack	MITRE Tactic	Technique ID
Brute Force	Credential Access	T1110
MITM	Credential Access	T1557
Weak Crypto	Defense Evasion	T1552

Cryptography Best Practices

---

1. Use Strong, Modern Algorithms

- AES-128/256 for symmetric encryption
- RSA-2048+ or ECC for asymmetric encryption
- SHA-256 or higher for hashing

---

2. Secure Key Management

- Protect private keys
- Rotate keys periodically
- Use Hardware Security Modules (HSMs)

---

3. Use Authenticated Encryption

- Prefer AES-GCM or ChaCha20-Poly1305
- Prevents tampering and padding oracle attacks

---

4. Proper Certificate Management

- Validate certificates
- Use trusted Certificate Authorities (CAs)
- Implement certificate revocation

---

5. Cryptographic Standards

5.1 Common Standards

- AES (FIPS 197)
- RSA (PKCS #1)

- SHA (FIPS 180)
- TLS (RFC 8446)

5.2 Compliance Frameworks

- PCI-DSS
- HIPAA
- GDPR

---

6. Real-World Cryptography Failures (Case Studies)

6.1 Case Study 1: Weak SSL/TLS Configuration

Issue:

- Outdated TLS version
- Weak cipher suites

Impact:

- MITM attacks
- Data interception

Lesson:

- Disable legacy protocols

6.2 Case Study 2: Password Hash Breach

Issue:

- MD5 used without salt

Impact:

- Mass password cracking

Lesson:

- Use salted, strong hashes

6.3 Case Study 3: Random Number Generator Failure

Issue:

- Predictable RNG

Impact:

- Private key recovery

Lesson:

- Use cryptographically secure RNG (CSPRNG)

---

7. Cryptography in CEH Attack Lifecycle

Phase	Crypto Aspect
Reconnaissance	Certificate analysis
Exploitation	Weak crypto abuse
Post-Exploitation	Credential decryption
Covering Tracks	Encrypted exfiltration

---

8. Complete MITRE ATT&CK Mapping

Area	Tactic	Technique ID
Weak Crypto	Credential Access	T1552
MITM	Credential Access	T1557
Key Theft	Credential Access	T1555

---

9. CEH Exam Strategy – Cryptography Module

9.1 High-Probability Exam Topics

- AES vs DES vs 3DES
- RSA vs ECC
- Hashing vs encryption
- Salting & HMAC
- MITM and certificate attacks

9.2 Common Exam Traps

- Confusing hashing with encryption
- Assuming algorithms fail instead of implementations
- Ignoring key management

---

10. Quick Revision Table

Concept	Key Point
AES	Symmetric standard
RSA	Public-key encryption
ECC	Small key, strong security
SHA-256	Secure hashing
GCM	Authenticated encryption

---

11. Best Defensive Crypto Architecture

- Hybrid encryption
- Strong key management
- Regular audits
- Secure coding practices

Conclusion

Cryptography is the backbone of modern cybersecurity, but its strength depends on correct implementation, key management, and configuration. CEH emphasizes understanding cryptography not just to secure systems, but to recognize how attackers exploit weak cryptographic designs.

Mastering this module equips you to:

- Identify weak crypto implementations
- Prevent MITM and credential theft
- Design secure communication systems

References

1. EC-Council CEHv13 Official Curriculum
2. NIST Cryptographic Standards
3. MITRE ATT&CK Framework
4. OWASP Cryptographic Storage Guide
5. RFCs for TLS and PKI