Cryptography Exam Section B - Study Guide

Question 6: Cryptanalysis and Attacks on Cryptosystems (6 Marks)

Cryptanalysis is the science of breaking cryptographic codes and ciphers. It involves analyzing cryptographic systems to find weaknesses and recover plaintext from ciphertext without knowing the key.

Common Attacks on Cryptosystems:

- **Ciphertext-only attack**: Attacker has only ciphertext
- **Known-plaintext attack**: Attacker has pairs of plaintext and corresponding ciphertext
- **Chosen-plaintext attack**: Attacker can choose plaintexts and obtain corresponding ciphertexts
- **Chosen-ciphertext attack**: Attacker can choose ciphertexts and obtain corresponding plaintexts
- **Brute force attack**: Trying all possible keys systematically
- **Frequency analysis**: Analyzing letter/pattern frequencies in ciphertext

Question 7: Two Basic Cryptographic Algorithms with Figures (6 Marks)

1. Symmetric Key Cryptography

```
Plaintext → [Encryption with Key K] → Ciphertext
Ciphertext → [Decryption with Key K] → Plaintext

Sender ←→ Shared Secret Key K ←→ Receiver
```

- Same key used for encryption and decryption
- Examples: AES, DES, RC4

2. Asymmetric Key Cryptography

```
Plaintext → [Encryption with Public Key] → Ciphertext
Ciphertext → [Decryption with Private Key] → Plaintext

Sender uses Receiver's Public Key
Receiver uses their Private Key
```

- Different keys for encryption and decryption
- Examples: RSA, ECC, Diffie-Hellman

Question 8: Stream Cipher vs Block Cipher Comparison (4 Marks)

Aspect	Stream Cipher	Block Cipher
Data Processing	One bit/byte at a time	Fixed-size blocks (e.g., 128 bits)
Speed	Faster, real-time	Slower due to block processing
Memory	Low memory requirements	Higher memory for buffering
Error Propagation	Single bit error affects one bit	Error affects entire block
Examples	RC4, ChaCha20	AES, DES, 3DES

Example:

- **Stream Cipher**: RC4 encrypts each byte of "HELLO" individually
- **Block Cipher**: AES encrypts "HELLO" as a 128-bit block (with padding)

Question 9: Known-Plaintext vs Chosen-Plaintext Attack (4 Marks)

Known-Plaintext Attack:

- Attacker has pairs of plaintext and corresponding ciphertext
- Attacker cannot choose the plaintext
- Uses existing plaintext-ciphertext pairs to deduce the key
- Example: Having intercepted messages with known content

Chosen-Plaintext Attack:

- Attacker can choose specific plaintexts to encrypt
- Has access to encryption oracle
- Can strategically select plaintexts to reveal key information
- More powerful than known-plaintext attack
- Example: Submitting specific inputs to an encryption service

Question 10: Unconditionally Secure vs Computationally Secure Cipher (4 Marks)

Unconditionally Secure Cipher:

- Secure against adversaries with unlimited computational power
- Security doesn't depend on computational limitations
- Ciphertext provides no information about plaintext
- Example: One-time pad (when used correctly)
- Theoretical perfect security

Computationally Secure Cipher:

- Secure against adversaries with limited computational resources
- Security relies on computational difficulty of breaking the cipher
- Could theoretically be broken with enough time/resources
- Example: AES, RSA
- Practical security for real-world applications

Question 11: Rail Fence Cipher for "CRYPTOGRAPHY" (4 Marks)

Rail Fence Technique with 3 rails:

```
C P G P Y
 R Y T O R A H
  Y O P
```

Reading the rails:

- Rail 1: C P G P Y
- Rail 2: R Y T O R A H
- Rail 3: Y O P

Ciphertext: CPGPYRYTORAH YOP **Final Answer:** CPGPYRYTORAHYOP

Question 12: Why Symmetric Cryptography is Bad for Huge Data (4 Marks)

Reasons symmetric cryptography struggles with huge data:

1. **Key Distribution Problem**: Need to securely share keys with all parties
2. **Key Management**: n(n-1)/2 keys needed for n users to communicate
3. **Scalability Issues**: Exponential growth in key management complexity
4. **Single Point of Failure**: If key is compromised, all data is vulnerable

Solution: Hybrid cryptosystems using asymmetric crypto for key exchange and symmetric crypto for data encryption.

Question 13: Cyclic Group Definition (6 Marks)

A group G with operator * is said to be a **cyclic group** when:

Definition: There exists an element $g \in G$ such that every element of G can be expressed as a power of g.

Formal Definition: G is cyclic if $\exists g \in G$ such that $G = \langle g \rangle = \{g^n \mid n \in Z\}$

Properties:

- g is called a **generator** of the group
- All elements can be written as $g^0, g^1, g^2, ..., g^{k-1}$ for finite group of order k
- Cyclic groups are always abelian (commutative)

Example:

- $Z_5 = \{0, 1, 2, 3, 4\}$ under addition mod 5
- Generator: 1 (since $1, 2\equiv1+1, 3\equiv1+1+1, 4\equiv1+1+1+1, 0\equiv1+1+1+1+1$)

Question 14: Fermat's Little Theorem Proof for P=13, a=11 (6 Marks)

Fermat's Little Theorem: If p is prime and gcd(a,p) = 1, then $a^{p-1} \equiv 1 \pmod p$

Given: P = 13, a = 11 **To Prove:** $11^{12} \equiv 1 \pmod{13}$

Step-by-step calculation:

- $11^1 \equiv 11 \pmod{13}$
- $11^2 \equiv 121 \equiv 121 - 9\times13 \equiv 121 - 117 \equiv 4 \pmod{13}$
- $11^3 \equiv 11 \times 4 \equiv 44 \equiv 44 - 3\times13 \equiv 44 - 39 \equiv 5 \pmod{13}$
- $11^4 \equiv 11 \times 5 \equiv 55 \equiv 55 - 4\times13 \equiv 55 - 52 \equiv 3 \pmod{13}$
- $11^6 \equiv (11^3)^2 \equiv 5^2 \equiv 25 \equiv 25 - 13 \equiv 12 \pmod{13}$
- $11^{12} \equiv (11^6)^2 \equiv 12^2 \equiv 144 \equiv 144 - 11\times13 \equiv 144 - 143 \equiv 1 \pmod{13}$

Therefore: $11^{12} \equiv 1 \pmod{13}$ ✓ **Fermat's Little Theorem holds true**

Question 15: Multiplicative Inverse of 11 mod 13 using Extended Euclidean Algorithm (6 Marks)

Find: 11^{-1} mod 13 (multiplicative inverse of 11 modulo 13)

Extended Euclidean Algorithm:

```
gcd(13, 11):
13 = 1 × 11 + 2
11 = 5 × 2 + 1
2 = 2 × 1 + 0
```

Working backwards:

$1 = 11 - 5 \times 2$

$1 = 11 - 5 \times (13 - 1 \times 11)$

$1 = 11 - 5 \times 13 + 5 \times 11$

$1 = 6 \times 11 - 5 \times 13$

Therefore: $6 \times 11 \equiv 1 \pmod{13}$

Answer: The multiplicative inverse of 11 mod 13 is **6**

Verification: $11 \times 6 = 66 \equiv 1 \pmod{13}$ ✓ (since $66 = 5 \times 13 + 1$)