جامـــعـة المـــسـتـقـبـل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم علوم الامن السيبراني

Cyber Security Department

Subject: Cryptanalysis of Stream Ciphers

Class: 2nd

Lecturer: Asst.Lect Mustafa Ameer Awadh

Lecture: (8)

Study Year: 2024-2025

1.1 Introduction:

Cryptanalysis is the process of analyzing cryptographic algorithms to uncover weaknesses or vulnerabilities that can be exploited to compromise the security of encrypted data. The goal is to break the cipher by recovering the plaintext, the encryption key, or both, without access to the secret key. In the context of stream ciphers, cryptanalysis often targets the dynamic nature of the key stream generation process, seeking to predict or reverse-engineer it. Cryptanalysis techniques applied to stream ciphers often focus on identifying flaws in the pseudo-random number generation (PRNG) or key stream generation algorithms. These flaws may include predictable initialization vectors (IVs), insufficient entropy in the random number generator, or biased outputs that deviate from true randomness. By exploiting these weaknesses, attackers can uncover patterns or correlations within the key stream that reveal critical information about the encryption process. In some cases, cryptanalysis may involve observing a large volume of encrypted messages to identify recurring key stream segments, especially if the cipher reuses initialization vectors or fails to securely implement key management practices. These recurring patterns can be used to infer the internal state of the cipher, enabling the attacker to reconstruct the key stream and decrypt intercepted messages. Additionally, cryptanalysts leverage specific attack methods such as known plaintext attacks, where portions of plaintext are compared with their corresponding cipher text to extract the key stream, or chosen plaintext attacks, where controlled inputs are encrypted to study the cipher's behavior. Advanced techniques, such as differential or linear cryptanalysis, may also be used to deduce relationships between the input and output of the cipher, revealing vulnerabilities in its structure.

2.1Common Cryptanalysis Techniques

1- Brute Force Attack:

- Exhaustively trying all possible keys.
- Feasibility depends on key size (e.g., 128-bit keys make this impractical).

2- Statistical Attacks:

- Exploiting statistical biases in the key stream.
- Example: RC4's biased output makes it vulnerable to statistical attacks.

3- Correlation Attacks:

- Targeting LFSR-based stream ciphers.
- Exploiting correlations between the cipher text and portions of the key stream.

4- Time-Memory Trade-Off (TMTO):

- Storing precomputed values to reduce the computational cost of future attacks.
- Example: Rainbow tables for cracking weak stream cipher keys.

3.1 Key Recovery Attacks

Objective: To recover the secret key used in the stream cipher.

Types of Key Recovery Attacks:

1. Known Plaintext Attack:
   - Assumes access to some plaintext-ciphertext pairs.
   - Example: Finding statistical correlations between the plaintext and the generated key stream.
2. Chosen Plaintext Attack:

- The attacker can select specific plaintexts to encrypt and analyze the resulting cipher text.
- Useful in understanding key stream generation mechanisms.

3. Ciphertext-Only Attack:
   - Only the cipher text is available.
   - Attacker searches for patterns or repetitions in the cipher text.

Example Case: RC4 Key Recovery

- RC4 exhibits key stream biases that enable recovery of secret keys using known plaintext attacks (e.g., WPA-TKIP vulnerability in Wi-Fi networks).

4.1 Linear Cryptanalysis of Stream Ciphers

A technique that models the relationships between plaintext, key stream, and cipher text using linear equations. Typically used for LFSR-based stream ciphers.

Steps in Linear Cryptanalysis:

1. **Identify Biases:** Determine if certain linear combinations of the input and output are biased.
2. **Construct Linear Approximation:** Approximate the output bits as linear functions of input bits and key bits.
3. **Recover Key Bits:** Use statistical analysis to deduce parts of the secret key.

- **Example:** Attack on a simple LFSR-based stream cipherExploiting predictable output to solve for LFSR initial states.

5.1 Differential Cryptanalysis of Stream Ciphers

Differential cryptanalysis of stream ciphers is a method that examines how differences in the input (e.g., initialization vectors or plaintext) influence differences in the output key stream or cipher text. It focuses on identifying predictable patterns in these differences to deduce information about the cipher's internal state or secret key.

Steps in Differential Cryptanalysis:

1. **Select Input Pairs:** Choose pairs of inputs with known differences.
2. **Analyze Output Differences:** Observe how differences propagate through the cipher's structure.
3. **Derive Key Information:** Identify patterns in differences that reveal internal states or key bits.

Example Use Case:

- Attacking a nonlinear combination generator: Observing how changes in input states affect the output key stream.

6.1 Case Studies and Practical Examples

- **Case Study 1: RC4 Vulnerabilities**
  - Statistical biases leading to key recovery.
  - Implications for protocols like WEP and early TLS implementations.
- **Case Study 2: A5/1 Cryptanalysis**
  - Linear attacks on GSM encryption (A5/1): Exploiting weak LFSRs and correlational biases.
  - Practical consequences in mobile network security.

7.1 Defense Mechanisms

- **Countermeasures Against Key Recovery Attacks:**
  - Use of strong, random keys.
  - Frequent key rotation to limit exposure.
- **Preventing Linear and Differential Attacks:**
  - Nonlinear feedback mechanisms in stream cipher design.
  - Increasing the complexity of key stream generators.
- **General Best Practices:**
  - Avoiding predictable or biased initialization vectors (IVs).
  - Adopting modern stream ciphers like ChaCha20, which are designed to resist such attacks.