

Complex

Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 2ICS304IRA

Topic:

Stream Ciphers and SRC4

Session - I3

Experiential Learning
(site visits)

Forum Theater

Jigsaw Discussion

Inquiry Learning

Role Playing

Active Review Sessions
(Games or Simulations)

Interactive Lecture

Hands-on Technology

Case Studies

Brainstorming

Groups Evaluations

Peer Review

Informal Groups

Triad Groups

Large Group
Discussion

Think-Pair-Share

Writing

(Minute Paper)

Self-assessment

Pause for reflection

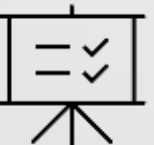
Simple

AIM OF THE SESSION




To make students understand basic concepts of Stream Ciphers and apply SRC4 algorithm on a given plaintext.

INSTRUCTIONAL OBJECTIVES



The objective of this session is to introduce types of Pseudorandom Number Generators.

LEARNING OUTCOMES



At the end of this session, students are expected to know

- Summarize the concepts of Stream Cipher.
- Apply SRC4 cipher to a given plaintext.

This module demonstrates block cipher modes of operation. It also helps to identify which ciphers operate as block ciphers and stream ciphers. Principles of Pseudorandom Number Generators are listed and types of Pseudorandom Number Generators are discussed. Finally, Stream Ciphers and its example RC4 algorithm are demonstrated.

Stream ciphers are a type of symmetric encryption algorithm that operates on individual bits or bytes of data. Unlike block ciphers, which encrypt data in fixed-size blocks, stream ciphers encrypt data on a continuous stream, hence the name. Stream ciphers are commonly used for real-time applications, such as securing network communications, as they can encrypt and decrypt data in a stream-like fashion without requiring buffering or padding.

One of the most well-known and widely used stream ciphers is RC4 (Rivest Cipher 4). RC4 was designed by Ronald Rivest in 1987 and became popular due to its simplicity and efficiency. It was initially a trade secret but later became publicly available, making it widely adopted.

SESSION DESCRIPTION

Stream Ciphers and SRC4

- Stream ciphers are a type of symmetric encryption algorithm that operates on individual bits or bytes of data.
- Unlike block ciphers, which encrypt data in fixed-size blocks, stream ciphers encrypt data on a continuous stream, hence the name.
- Stream ciphers are commonly used for real-time applications, such as securing network communications, as they can encrypt and decrypt data in a stream-like fashion without requiring buffering or padding.

SESSION DESCRIPTION

Stream Ciphers and SRC4

Features of Stream Ciphers:

- ☐ Processes the message bit by bit.
- ☐ Generates pseudo random key stream.
- ☐ Then performs XOR operation with plaintext bit by bit.
- ☐ randomness of stream key completely destroys statistically properties in message.
- ☐ but must never reuse stream key.

SESSION DESCRIPTION

Stream Ciphers and SRC4

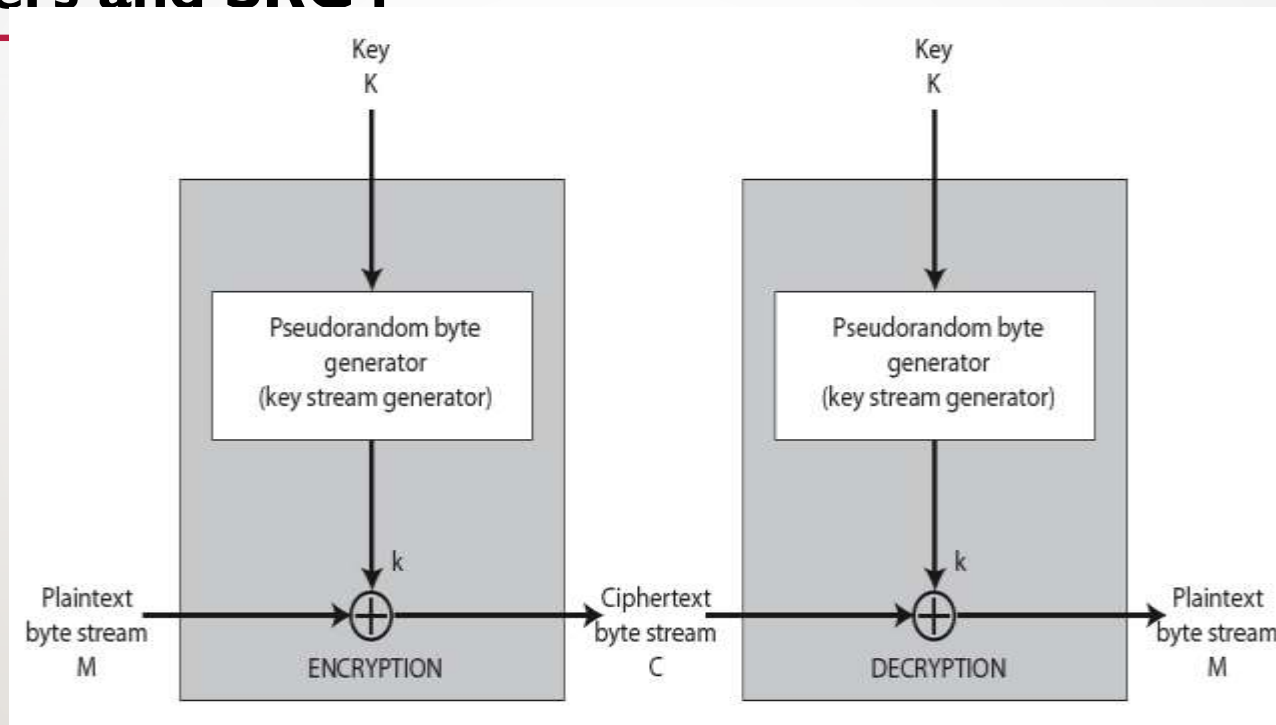


Figure 13.1: Structure of Stream Ciphers

Note: Copyrights of this diagram are reserved for original author

SESSION DESCRIPTION

Stream Ciphers and SRC4

One of the most well-known and widely used stream ciphers is RC4 (Rivest Cipher 4). RC4 was designed by Ronald Rivest in 1987 and became popular due to its simplicity and efficiency. It was initially a trade secret but later became publicly available, making it widely adopted.

- ☐ Some design considerations are:
- ☐ long period with no repetitions
- ☐ statistically random
- ☐ depends on large enough key
- ☐ large linear complexity
- ☐ If properly designed, can be as secure as a block cipher with same size key.
- ☐ Usually simpler & faster.

SESSION DESCRIPTION

Stream Ciphers and SRC4

SRC4:

- The RC4 algorithm, also referred to as Rivest Cipher 4 or Ron's Code 4, is a symmetric stream cipher widely utilized for encryption purposes.
- Developed by Ron Rivest in 1987, RC4 gained popularity due to its simplicity and speed.
- It found application in various protocols, including WEP for Wi-Fi networks and SSL/TLS for secure communications.

SESSION DESCRIPTION

Stream Ciphers and SRC4

A simplified explanation of the RC4 algorithm entails the following steps:

Key Setup:

- Initialization of two 256-byte arrays, S and T, with values ranging from 0 to 255.
- Permutation of the values in array S based on the provided key.
- Repetition of the permutation process for array T until it is fully populated with the key.

SESSION DESCRIPTION

Stream Ciphers and SRC4

Encryption/Decryption:

- Generation of a pseudorandom stream of bytes, referred to as the keystream, by combining the values from arrays S and T.
- XOR operation between each byte of the plaintext/ciphertext and the corresponding byte from the keystream, resulting in the encrypted/decrypted output.

SESSION DESCRIPTION

Pseudo-random Generation Algorithm (PRGA):

- Initialization of two indices, i and j , set to 0.
- Execution of a loop for the pseudo-random generation algorithm:
- Increment of index i .
- Modification of array S by swapping its values based on the current index i .
- Calculation of the pseudo-random index j using array S .
- Swapping of the values at indices $S[i]$ and $S[j]$.
- Retrieval of the pseudo-random value from array S by adding the values at $S[i]$ and $S[j]$ modulo 256.

SELF-ASSESSMENT QUESTIONS

1. Which of the following best describes a stream cipher?

- a) A symmetric encryption algorithm that operates on fixed-size blocks
- b) An asymmetric encryption algorithm used for key exchange
- c) A symmetric encryption algorithm that operates on individual bits or bytes
- d) An encryption algorithm used specifically for secure hash functions

2. In a stream cipher, the keystream is generated by:

- a) XORing the plaintext with a secret key
- b) Adding the plaintext and the secret key
- c) Multiplying the plaintext and the secret key
- d) Generating random bits using a pseudo-random number generator

SELF-ASSESSMENT QUESTIONS

3. Which of the following is a characteristic of stream ciphers?

- a) They are generally slower compared to block ciphers
- b) They require a larger key size for equivalent security compared to block ciphers
- c) They can encrypt data in parallel at high speeds
- d) They are more resistant to cryptanalysis attacks compared to block ciphers

4. The security of a stream cipher mainly relies on:

- a) The size of the plaintext
- b) The strength of the secret key
- c) The length of the ciphertext
- d) The complexity of the encryption algorithm

SUMMARY

In summary, stream ciphers like SRC4 are encryption algorithms that encrypt data in a continuous stream. SRC4, in particular, gained popularity due to its simplicity and efficiency. However, it has since been found to have security vulnerabilities and is no longer considered secure for use in modern cryptographic applications..

TERMINAL QUESTIONS

1. Illustrate Psuedorandom Number Generators using bock ciphers with a neat diagram
2. Demonstrate ANSI X9.17 Psuedorandom Number Generators
3. Elaborate the SRC4 Ciphers
4. Outline the advantage and disadvantage of Stream Ciphers

REFERENCES FOR FURTHER LEARNING OF THE SESSION

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015.
3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011
4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

THANK YOU



Team – CACD