KL (DEEMED TO BE UNIVERSITY)

Department of CSE(HONORS)

CRYPTANALYSIS & CYBER DEFENSE 21CS3041RA

Topic:

RC4

Session -14

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

- Demonstrate RC4 cipher to a given plaintext.

Module Description

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.

SESSION INTRODUCTION

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

RC4

- RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security.
- A variable key-length from 1 to 256 bytes is used to initialize a 256-byte state vector S, with elements S[0] to S[255].
- At all times, S contains a permutation of all 8-bit numbers from 0 through 255.

RC4

- For encryption and decryption, a byte key k is generated from S by selecting one of the 255 entries in a systematic fashion.
- RC4 operates based on a pseudorandom key stream that is generated using a secret key.
- The key stream is then combined with the plaintext using a bitwise exclusive OR (XOR) operation to produce the ciphertext.
- To decrypt the ciphertext, the same key stream is generated and XORed with the ciphertext, resulting in the original plaintext.

SESSION DESCRIPTION

RC4

```
/* Initialization  of S */
for i = 0 to 255 do
S[i] = i
T[i] = K[i mod keylen]
/* Initial Permutation */
j = 0
for i = 0 to 255 do
j = (j + S[i] + T[i]) (mod 256)
swap (S[i], S[j])
```

SESSION DESCRIPTION

RC4

RC4 Stream Generation:

Stream generation involves cycling through all the elements of S[i] and for each S[i], swapping S[i] with another byte in S according to scheme dictated by the current configuration of S.

```
i = j = 0
for each message byte Mi
i = (i + 1) (mod 256)
j = (j + S[i]) (mod 256)
swap(S[i], S[j])
t = (S[i] + S[j]) (mod 256)
Ci = Mi XOR S[t]
```

RC4

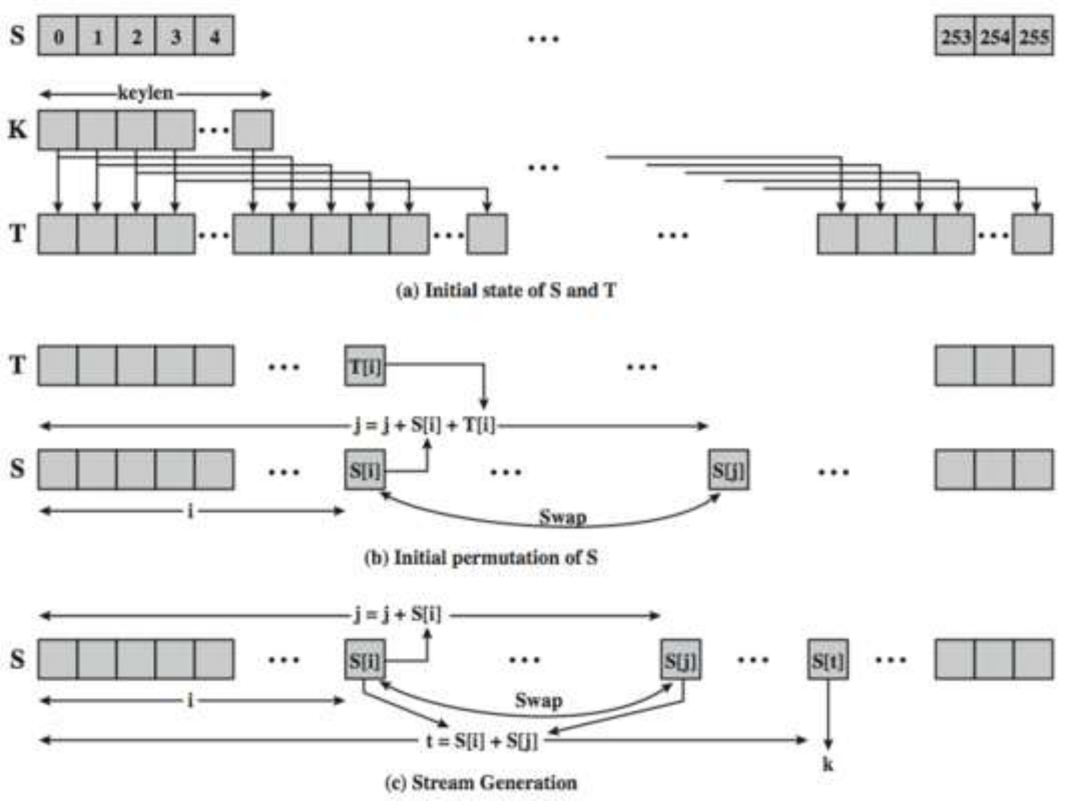

Figure 14.1: RC4 Overview

SESSION DESCRIPTION

RC4

- The key stream generation in RC4 is based on a permutation of all possible bytes (256 values) determined by the secret key.
- It uses a variable-length key ranging from 1 to 256 bytes, making it flexible for different applications.
- RC4 consists of two main components: the key-scheduling algorithm (KSA) and the pseudo-random generation algorithm (PRGA).

SESSION DESCRIPTION

RC4

- The KSA initializes an internal state array (S-box) by permuting the values 0 to 255 based on the key.
- This step ensures that each element of the S-box depends on the entire key.
- The PRGA generates the key stream by repeatedly modifying the state array and outputting a pseudorandom byte.

SESSION DESCRIPTION

RC4

- While RC4 was widely used, it has been discovered to have several security vulnerabilities over time.
- Weaknesses in its key scheduling algorithm and biases in its output stream have been identified, making it susceptible to attacks.
- Due to these vulnerabilities, RC4 is no longer recommended for use in secure systems, and more advanced stream.

SELF-ASSESSMENT QUESTIONS

1. What does RC4 stand for?

a) Rivest Cipher 4
b) Ron's Code 4
c) Random Cipher 4
d) Reliable Cipher 4

2. Who designed the RC4 algorithm?

a) Ron Rivest
b) Bruce Schneier
c) Phil Zimmermann
d) Whitfield Diffie

SELF-ASSESSMENT QUESTIONS

3. Which of the following is NOT a common use of RC4?

a) WEP encryption in Wi-Fi networks

b) SSL/TLS in secure communications

c) Disk encryption

d) Password hashing

4. What type of cipher is RC4?

a) Symmetric block cipher
b) Symmetric stream cipher
c) Asymmetric block cipher
d) Asymmetric stream cipher

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. Summarize the key setup process in the RC4 algorithm.
2. Explain how the pseudo-random generation algorithm (PRGA) works in RC4.
3. Discuss the potential security vulnerabilities associated with RC4.
4. Compare and contrast RC4 with other symmetric stream ciphers.
5. Summarize the impact of key length on the security of RC4

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, Algorthms, 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

(DEEMED TO BE UNIVERSITY)

Team – CACD