وزارة التعليم العالي والبحث العلمي

قسم علوم الامن السيبراني

Department of Cyber Security

Subject

RC4 Block Cipher

Class: Second

Lecturer: 6

Teaching the subject

RAED ALSHMARY

Introduction

RC4 (Rivest Cipher 4) is a symmetric key encryption algorithm designed by **Ron Rivest** in 1987.

It is classified as a **Stream Cipher**, which means that it encrypts data **one byte at a time** rather than encrypting blocks of data.

RC4 was widely used in many network security protocols because of its **simplicity and high speed**.

Type of Encryption

RC4 belongs to the category of **Stream Ciphers**.
In stream ciphers:

- Data is encrypted **bit by bit or byte by byte**.
- A **pseudo-random key stream** is generated.
- This key stream is combined with the plaintext using the **XOR operation**.

Key Length in RC4

RC4 uses a **variable-length key**.
The key size ranges from:
1 to 256 bytes
This key is used to initialize a **state table consisting of 256 elements**.

Main Phases of the RC4 Algorithm

The RC4 algorithm works in **two main stages**:

1. Key Scheduling Algorithm (KSA)

In this stage:

- A **state array S** is created containing **256 values**.
- The values are initially arranged from **0 to 255**.
- The array is then **permuted (shuffled)** using the secret key.

The purpose of this stage is to produce a **randomized initial state** for encryption.

2. Pseudo Random Generation Algorithm (PRGA)

In this stage:

- The algorithm generates a **pseudo-random key stream**.
- Each byte of the key stream is combined with the plaintext.
- The **XOR operation** is applied to produce the ciphertext.

Encryption Process

The encryption process in RC4 is performed using the **XOR operation**.

The formula is:

Plaintext $\oplus$ KeyStream = Ciphertext

Where:

- Plaintext = original data
- KeyStream = generated pseudo-random sequence
- Ciphertext = encrypted data

Key Length (b)

6. Decryption Process

In RC4, the **same process used for encryption is used for decryption**.

Ciphertext ⊕ KeyStream = Plaintext

Applying the same key stream restores the **original message**.

Advantages of RC4

RC4 has several advantages:

1. Very fast encryption and decryption.
2. Simple algorithm and easy to implement.
3. Requires low computational resources.
4. Efficient for software implementations.

Applications of RC4

RC4 was used in several security protocols, such as:

- SSL (Secure Sockets Layer)
- TLS (Transport Layer Security)
- WEP (Wired Equivalent Privacy) for Wi-Fi networks

However, it is no longer recommended for modern systems.

Security Issues

Despite its speed and simplicity, RC4 has several security weaknesses.

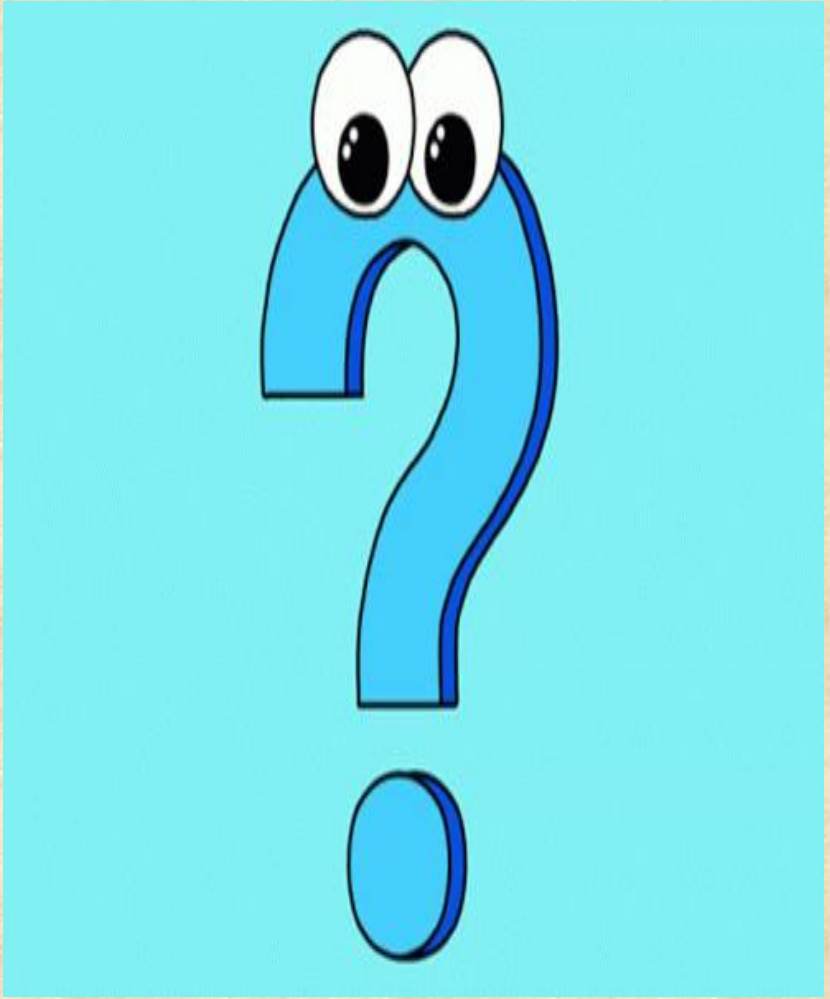
Researchers discovered vulnerabilities related to:

- Key stream biases
- Weak key scheduling

Because of these issues, RC4 has been deprecated in modern cryptographic systems.

Lecture questions

1 - What does RC4 stand for?
2 - RC4 was designed by?
3 - RC4 is classified as?
4 - RC4 encrypts data?
5 - RC4 uses which operation for encryption?
6 - The key length in RC4 is?
7 - The key size in RC4 can be up to?
8 - PRGA stands for?
9 - The purpose of KSA in RC4 is to?
10 - RC4 was widely used in?
11 - RC4 encryption formula is?
12 - RC4 decryption uses?
13 - The RC4 key stream is?
14 - RC4 is mainly designed for?
15 - RC4 is considered insecure today because of?
16 - RC4 generates the key stream using?
17 - Which structure does RC4 mainly use?
18 - RC4 belongs to which type of cryptography?
19 - RC4 works primarily on?
20 - The main weakness of RC4 is?
21 - Modern cryptographic systems replaced RC4 mainly with?



Conclusion

RC4 is a **stream cipher encryption algorithm** that generates a pseudo-random key stream which is combined with plaintext using the **XOR operation** to produce ciphertext.

Although it was widely used in many security protocols, **security vulnerabilities** have led to its replacement by stronger algorithms such as **AES**.


thank
you