وزارة التعليم العالي والبحث العلمي

قسم علوم الامن السيبراني

Department of Cyber Security

Subject

RC5 Block Cipher

Class: Second

Lecturer: 5

Teaching the subject

RAED ALSHMARY

Introduction

RC5 is a **symmetric key block cipher** designed by Ronald Rivest in **1994**.
It belongs to the **Rivest Cipher (RC) family** and was developed to be:

- Simple
- Fast
- Flexible
- Efficient for both software and hardware implementation.

RC5 was also considered as a candidate for replacing the Data Encryption Standard.

Type of Algorithm

RC5 is classified as a:
Block Cipher

This means that:
•Data is divided into **blocks**
•Each block is encrypted separately using the same secret key.

RC5 Parameters

One of the main features of RC5 is flexibility, because it uses three adjustable parameters.
The algorithm is written as:
RC5 – w / r / b
Where:

Parameter	Meaning
w	Word size
r	Number of rounds
b	Key length in bytes

1 - Word Size (w)

The **word size** determines the number of **bits in each word**.
Common values include:

- 16 bits
- 32 bits (most common)
- 64 bits

RC5 processes **two words per block**, therefore:
Block Size = 2w

Example:
If w = 32
Then
Block Size = **64 bits**

2 - Number of Rounds (r)

The **number of rounds** represents how many times the encryption operations are repeated.

Possible values:

0 – 255 rounds

However, typical values are:

12 rounds

20 rounds

Increasing the number of rounds:

- improves security
- slightly decreases speed

3 - Key Length (b)

The **key length** determines the size of the **secret encryption key**.

Range:

0 – 255 bytes

Example key sizes:

- 16 bytes
- 32 bytes

A longer key provides **stronger security**.

Main Stages of RC5

RC5 consists of **three main stages**:

1.Key Expansion

2.Encryption

3.Decryption

1 - Key Expansion

In this stage, the secret key **K** is converted into a **subkey table** called:

S Table

This table is used during encryption.

The number of subkeys is:

T = 2(r + 1)

Example:

If

r = 12

Then:

T = **26 subkeys**

The key expansion process includes:

1-Copying the key into an array **L**

2 -Creating the subkey array **S**

3 - Mixing the values of **S** and **L** several times

This process produces strong and random-looking subkeys.

2- Encryption Process

During encryption:
1.The plaintext block is divided into two words:
A and B
2.Initial values from the **S table** are added.
3.For each round:
•XOR operation is applied
•Rotation is performed
•Subkeys are added
4.After completing **r rounds**, the output becomes the:
Ciphertext

3 - Decryption Process

The **decryption process** is simply the reverse of encryption.
It includes:
Reverse rotations
Subtractions instead of additions
XOR operations
After reversing all rounds, the **original plaintext** is recovered.

Basic Operations in RC5

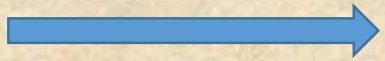
RC5 uses three simple operations:

Operation	Description
Addition	Modular addition
XOR	Exclusive OR operation
Rotation	Circular bit rotation

1. Addition
Numbers are added using:

mod 2^w

2. XOR
The **XOR operation** mixes the bits of the data with the key values.

3. Rotation
RC5 uses **circular left rotation**.
The rotation amount depends on the **data itself**, which is called:
Data-Dependent Rotation
This increases the algorithm's security.
10110001  01100011

Advantages of RC5

Simple design
- High speed
- Flexible parameters
- Efficient implementation
- Good resistance against many cryptographic attacks

Disadvantages of RC5

Originally protected by a patent
- Security depends on proper parameter selection
- Less commonly used today compared with modern algorithms like Advanced Encryption Standard.

Lecture questions

1 - Who developed the RC5 algorithm?

2- RC5 was introduced in which year?

3 - RC5 belongs to which type of cryptographic algorithms?

4 - RC5 is an example of which encryption system?

5 - In RC5 parameters, the symbol w represents?

6 - The block size in RC5 equals?

7 - Typical values for the word size w include?

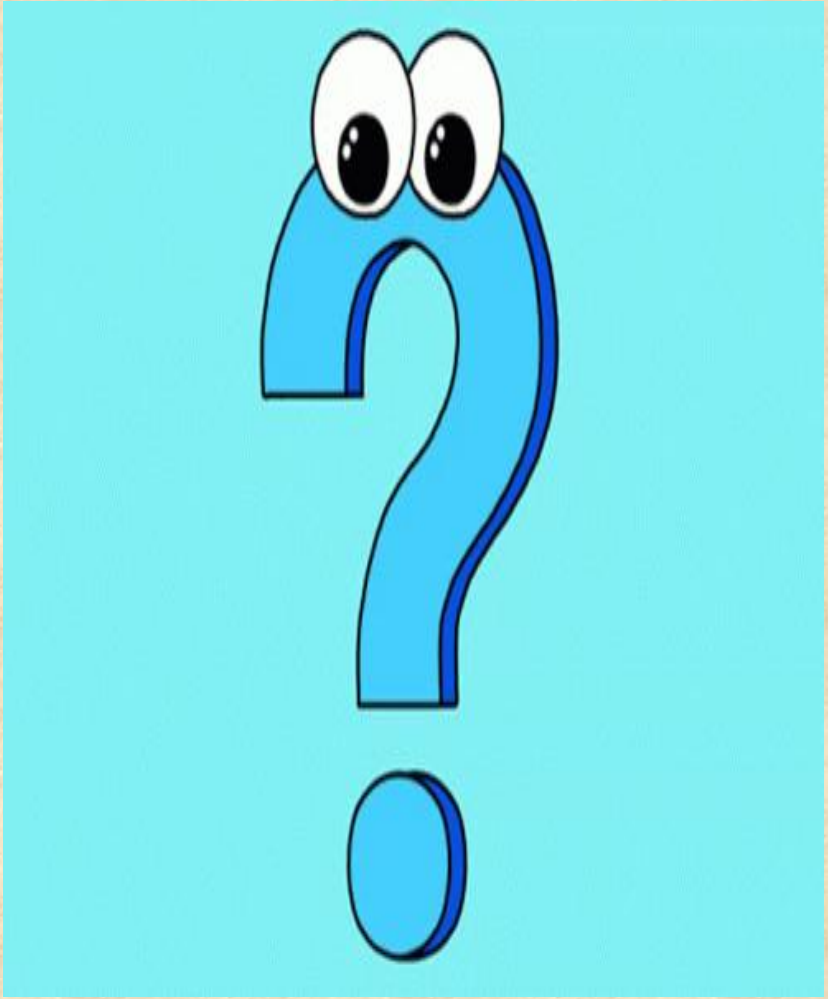
8 - The number of rounds in RC5 can range between?

9 - Commonly used number of rounds in RC5 is?

10 - The maximum key length in RC5 is?

11- The decryption process in RC5 is?

12 - Which modern encryption standard replaced older algorithms like DES in many systems?



Conclusion

RC5 is a symmetric block cipher developed by Ronald Rivest in 1994. It is known for its simplicity, speed, and flexibility. The algorithm uses three parameters: word size (w), number of rounds (r), and key length (b). It relies on three main operations: addition, XOR, and rotation, and consists of three stages: key expansion, encryption, and decryption.


thank
you