وزارة التعليم العالي والبحث العلمي

قسم علوم الامن السيبراني

Department of Cyber Security

Subject

GOST Block Cipher

Class: Second

Lecturer: 4

Teaching the subject

RAED ALSHMARY

Introduction

- **GOST** stands for *Gosudarstvennyi Standard* (Government Standard).
- Full name: *Gosudarstvennyi Standard Soyuza SSR*.
- Official standard number: **28147-89**
- Approved by the Government Committee for Standards of the USSR.
- Believed to be used in:
    - Civilian encryption
    - High-grade communications
    - Possibly classified military systems

Later, S-boxes used by the **Central Bank of the Russian Federation** were published.

General Characteristics of GOST

Property	Value
Block Size	64 bits
Key Size	256 bits
Structure	Feistel Network
Number of Rounds	32
S-boxes	8 (4×4 each)
Key Schedule	Very simple

Working Principle of the GOST Algorithm

GOST follows the **Feistel structure** (same family as **DES**).

Encryption Process:

Split plaintext into:

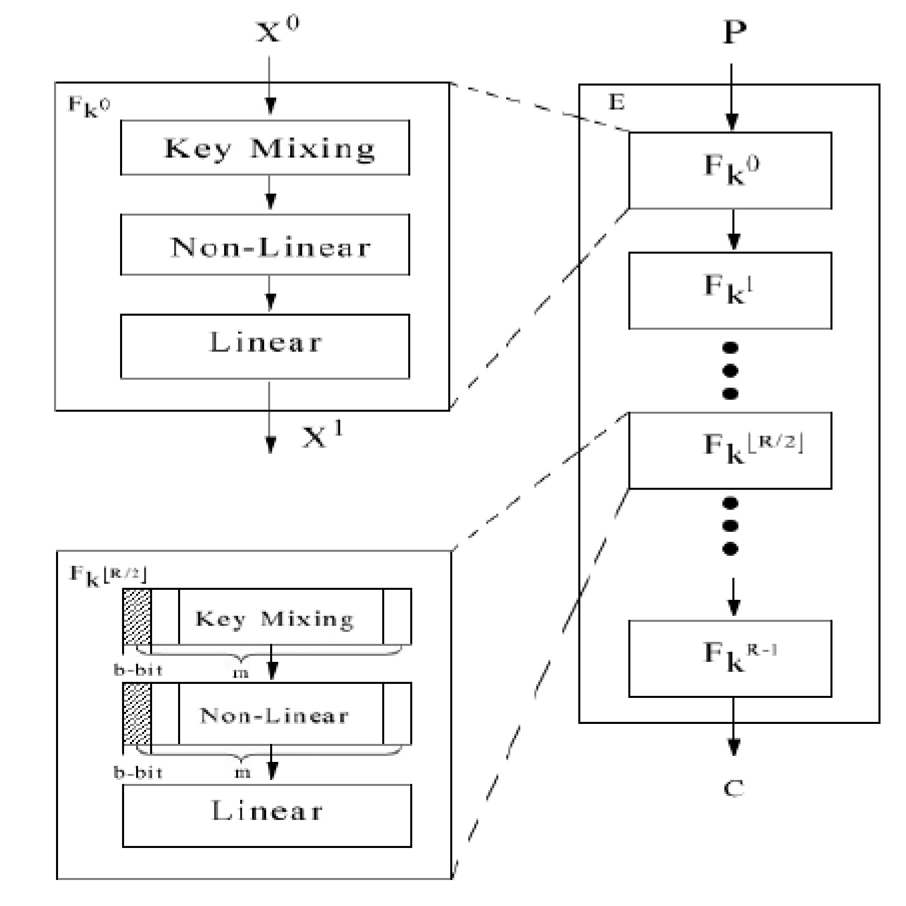
- Left half (L)
- Right half (R)

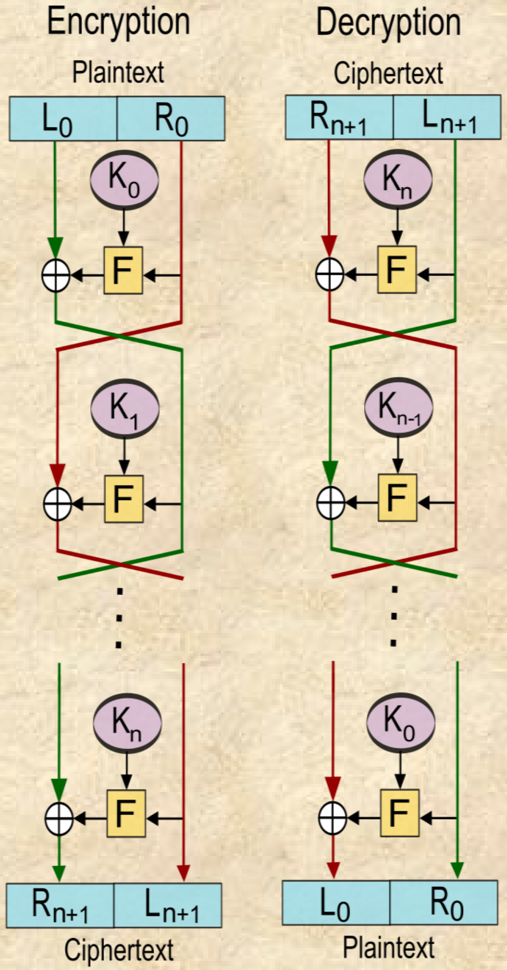
For each round i:

$Li = Ri$

$1Ri = Li \oplus f$

Repeated **32 rounds**.





Function f in GOST

The function f consists of 4 main steps:

Step 1: Modular Addition

Add the right is combined with the subkey:

2^{32}R+Ki mod 232

Step 2: S-Box Substitution

- Split result into eight 4-bit chunks.
- Each chunk enters a different S-box.
- Each S-box is a permutation of numbers 0–15.
- S-boxes are secret (considered additional key material).

Example S-box:

Input → Output

0 → 7

1 → 10

2 → 2

Step 3: Recombine Output

Recombine into 32-bit word.

Step 4: 11-bit Left Circular Shift

Rotate left by 11 bits.

Final result is XORed with the left half.

Key Schedule

The 256-bit key is divided into:

k1,k2,...,k8k_1, k_2, ..., k_8k1,k2,...,k8

Each is 32 bits.

Rounds use subkeys in sequence:

- Rounds 1–24: k1 → k8 repeated three times
- Rounds 25–32: k8 → k1 (reverse order)

Decryption = same algorithm with reversed key order.

comparison with DES

Feature	DES	GOST
Key Size	56-bit	256-bit
Rounds	16	32
S-box Input	6-bit	4-bit
S-box Output	4-bit	4-bit
Permutation	P-box	11-bit rotation
Key Schedule	Complex	Simple

Strengths

- Very large key (256-bit)
- 32 rounds
- Resistant to brute-force
- Strong against differential & linear cryptanalysis
- Secret S-boxes increase resistance

Weaknesses

- No expansion permutation (unlike DES)
- Weaker avalanche effect
- Needs 8 rounds for full diffusion (DES needs 5)

However:

GOST has double the rounds of DES.

If brute force is the only attack → GOST is extremely secure

Lecture questions

1. What does GOST stand for?
2. GOST was developed in which region?
3. The official standard number of the GOST cipher is:
4. GOST is classified as:
5. The block size of GOST is:
6. The key size used in GOST is:
7. The structure used in GOST is:
8. How many rounds does the GOST algorithm use?
9. The plaintext in GOST is divided into:
10. How many S-boxes are used in GOST?
11. The output size of each GOST S-box is:
12. The modular addition in GOST is performed modulo:
13. Which attack becomes difficult due to the large key size?
14. GOST designers increased security by:
15. GOST is considered secure mainly because:

Conclusion

GOST 28147-89 is a Soviet-era block cipher that uses a **64-bit block size**, a **256-bit key**, and a **32-round Feistel structure**.

It applies **modular addition, S-box substitutions, and bit rotation**, providing strong resistance against classical cryptanalysis.

thank you