C201091_Mohammed Main Uddin

Additional

Block Ciphers and the Data Encryption Standard

The Feistel Structure for Block Ciphers:

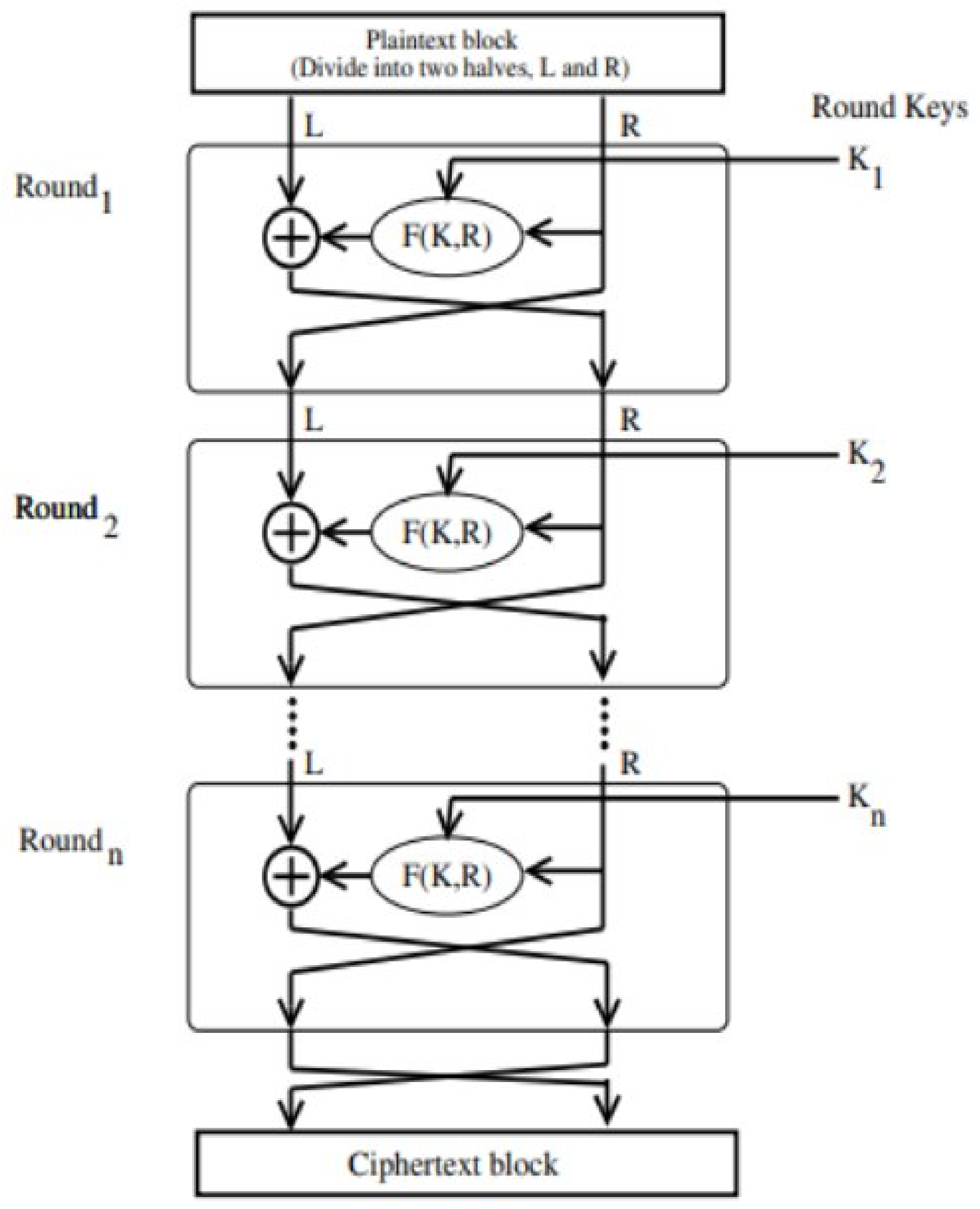

Figure 2: *The Feistel Structure for symmetric key cryptography*

A cryptographic system based on Feistel structure uses the same basic algorithm for both encryption and decryption. As shown in Figure 2, the Feistel structure consists of multiple rounds of processing of the plaintext, with each round consisting of a substitution step followed by a permutation step.

The input block to each round is divided into two halves that I have denoted L and R for the left half and the right half. In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. The operation carried out on the left half L is referred to as the Feistel Function.

The permutation step at the end of each round consists of swapping the modified L and R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round. The next two subsection present important properties of the Feistel structure. As you will see, these properties are invariant to our choice for the Feistel Function.

Mathematical Description of Each Round in the Feistel Structure:

Let LEi and REi denote the output half-blocks at the end of the i th round of processing. The letter 'E' denotes encryption.

In the Feistel structure, the relationship between the output of the i th round and the output of the previous round, that is, the (i − 1)th round, is given by LEi = REi−1. REi = LEi−1 ⊕ F(REi−1, Ki). where ⊕ denotes the bitwise EXCLUSIVE-OR operation. The symbol F denotes the operation that "scrambles" REi−1 of the previous round with what is shown as the round key Ki in Figure 2. The round key Ki is derived from the main encryption key as will be explained later.F is referred to as the Feistel function, after Horst Feistel naturally.

Assuming 16 rounds of processing (which is typical), the output of the last round of processing is given by LE16 = RE15 RE16 = LE15 ⊕ F(RE15, K16)

Groups, Rings, Fields:

Watch this Video: https://youtu.be/oBL-Cb5GxA0

(20109)

Modular Arithmetic

তারিখ: ....../....../......

* Congruent modulo n, if $a \bmod n = b \bmod n$.

or we can express $a \equiv b \pmod n$

Example: [redacted] find congruences of modulo 3: OR proof that if modulo n maps $\{0, 1, 2 \dots n-1\}$.

** ইংলিশে answer এইটা হবে **.

Ans: 3 এর জন্য, $n = -5$ $\therefore$ $-5 \bmod 3 = 1$

$n = 5$ $\therefore$ $5 \bmod 3 = 2$

$n = 6$ $\therefore$ $6 \bmod 3 = 0$

so, formula অনুযায়ী $5 \equiv 2 \pmod 3$

... 0 1 2 0 1 2 0 1 2 0 1 2 0 ...

... -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 ...

upper line = modulo 3 output.

lower line = আমার নিজের দেওয়া কিছু random value.

so, আমার modulo 3 এর congruence এর মান এই ক্ষেত্রে (3 mod) এর value 0 - 2 হবে means $n-1$ $(3-1)$.

$\therefore$ set $\{0, 1, 2\} = \{0, 1, n-1\}$ satisfied.

☐ Modulo Addition and Modulo Multiplication Over Z_n.

Let assume. $n = 8$.

$\therefore Z_8 = (0-7)$.

Z_8 :	0	1	2	3	4	5	6	7
Additive inverse :	0	7	6	5	4	3	2	1
Multiplacitive inverse :	-	1	-	3	-	5	-	7

* additive inverse হওয়ার rules = $w + x = 0 \mod n$

here, $w \in Z_8$, $x \in Z_8$.

যেমন, $w = 2$ হলে, $(2 + 6 = 0 \mod 8)$. $6 \in Z_8$.

* multiplicative inverse হওয়ার rules = $w \times x = 1 \mod n$

here, $w \in Z_8$, $x \in Z_8$.

যেমন, $w = 3$ হলে, $(3 \times 3 = 1 \mod 8)$. $3 \in Z_8$.

আবার, $w = 4$ " . $(4 \times \boxed{x} = 1 \mod 8)$. এই জন্য 4 এর কোনো multiplicative inverse নাই।

C২৩।০৩।

তারিখ: ..../.........../......

∴ multiplicative inverse হতে হলে $\mathbb{Z}_8$ এর value গুলো relatively prime হতে হবে।

———————— × ————————

⊡ Euclid's GCD Algorithm :

Example : GCD (70, 38) ⟶ 38) 70 (1
38
32

= GCD (38, 32)

= GCD (32, 6) ⟶ 6) 32 (5
30
2

= GCD (6, 2)

= GCD (2, 0) ⟶ 0) 2 – not possiple

↳ answer.

∴ gcd (70, 38) = 2.