Nama : Arya Pratama
Nim : 122140156

Plainteks : Hello world
IV : 0011
Kunci : LFSR 4-bit, seed 1010
Bit 1 XOR Bit 3

* Konversi Plainteks ke biner dan blok 4 bit
↳ H (ASCII : 104) -> Biner : 0110 1000 → 0110
→ 1000

↳ e (Ascii : 101) -> Biner : 0110 0101 → 0110
→ 0101

↳ l (ASCII : 108) -> Biner : 01101100 → 0110
→ 1100

↳ L (ASCII : 108) -> Biner : 01101100 → 0110
→ 1100

↳ o (ASCII : 111) -> Biner : 01101111 → 0110
→ 1111

↳ w (ASCII : 119) -> Biner : 01110111 → 0111
→ 0111

↳ o (ASCII : 111) -> Biner : 01101111 → 0110
→ 1111

↳ r (ASCII : 114) -> Biner : 01110010 → 0111
→ 0010

↳ L (Ascii : 108) -> Biner : 01101100 → 0110
→ 1100

↳ D (ASCII : 100) -> Biner : 01100100 → 0110
→ 0100

Date

Fold

Blok 4-Bit (20 blok)

0110, 1000, 0110, 0101, 0110, 1100, 0110, 1111, 0111, 0111, 0110, 1111, 0110,
0010, 0110, 1100, 0110, 0100

* Pembangkitan kunci LFSR 4-bit

↳ 1010 = 1 ⊕ 1 = 0 : 0101
↳ 0101 = 0 ⊕ 0 : 0 : 0010
↳ 0010 = 0 ⊕ 1 : 0 1 : 1001
↳ 1001 : 1 ⊕ 0 : 1 : 1100
↳ 1100 : 1 ⊕ 0 : 1 : 1110
↳ 1110 : 1 ⊕ 1 : 0 : 0111
↳ 0111 : 0 ⊕ 1 : 1 : 1011
↳ 1011 : 1 ⊕ 1 : 0 : 0101
↳ 0101 : 0 ⊕ 0 : 0 : 0010
↳ 0010 : 0 ⊕ 1 : 1 : 1010

↳ 1010 = 1 ⊕ 1 = 0 = 0101
↳ 0101 : 0 ⊕ 0 : 0 = 0010
↳ 0010 = 0 ⊕ 1 = 1 = 1001
↳ 1001 : 1 ⊕ 0 : 1 = 1100
↳ 1100 : 1 ⊕ 0 : 1 : 1110
↳ 1110 : 1 ⊕ 1 = 0 : 0111
↳ 0111 : 0 ⊕ 1 : 1 : 1011
↳ 1011 : 1 ⊕ 1 : 0 : 0101
↳ 0101 : 0 ⊕ 0 : 0 : 0010
↳ 0010 : 0 ⊕ 1 : 1 : 1010

* Proses CBC 4-Bit

↳ P_1 : 0110 ⊕ 0011 : 0101 ⊕ 1010 : 1111 (hex : f)
↳ P_2 : 1000 ⊕ 1111 : 0111 ⊕ 0101 : 0010 → 1000 (hex : 8)
↳ P_3 : 0110 ⊕ 1000 : 1110 ⊕ 1001 : 0111 → 1101 (hex : d)
↳ P_4 : 0101 ⊕ 1101 : 1000 ⊕ 1001 : 0001 → 0100 (hex : 4)
↳ P_5 : 0110 ⊕ 0100 : 0010 ⊕ 1100 : 1110 → 1011 (hex : b)
↳ P_6 : 1100 ⊕ 1011 : 0111 ⊕ 1110 : 1001 → 0110 (hex : 6)
↳ P_7 : 0110 ⊕ 0110 : 0000 ⊕ 0111 : 0111 → 1101 (hex : d)
↳ P_8 : 1100 ⊕ 1101 : 0001 ⊕ 1011 : 1010 → 1010 (hex : a)
↳ P_9 : 0110 ⊕ 1010 : 1100 ⊕ 0101 : 1001 → 0110 (hex : 6)
↳ P_{10} : 1111 ⊕ 0110 : 1001 ⊕ 1001 : 0000 → 0000 (hex : 0)
↳ P_{11} : 0111 ⊕ 0000 : 0111 ⊕ 1001 : 1110 → 1011 (hex : b)

6 mm

Date

Fold

↳ P_{12} : 0110 ⊕ 0000 : 0110 ⊕ 1110 : 1000 → 0010 (hex : 2)

↳ P_{13} : 0110 ⊕ 1011 : 1100 ⊕ 1100 : 0000 → 0000 (hex : 0)

↳ P_{14} : 1111 ⊕ 0010 : 1101 ⊕ 0111 : 1010 → 1010 (hex : a)

↳ P_{15} : 0111 ⊕ 1010 : 1101 ⊕ 1011 : 0110 → 1001 (hex : 9)

↳ P_{16} : 0010 ⊕ 1001 : 1011 ⊕ 0101 : 1110 → 1011 (hex : b)

↳ P_{17} : 0110 ⊕ 1011 : 1101 ⊕ 1001 : 0100 → 0001 (hex : 1)

↳ P_{18} : 1100 ⊕ 0001 : 1101 ⊕ 1001 : 0100 → 0001 (hex : 1)

↳ P_{19} : 0110 ⊕ 0001 : 0111 ⊕ 1100 : 1011 → 1110 (hex : c)

↳ P_{20} : 0100 ⊕ 1110 : 1010 ⊕ 1110 : 0100 → 0001 (hex : 1)

* Process CFB 4-Bit

↳ S_1 : 0011 ⊕ 1010 : 1001 → 0110 ⊕ 0110 : 0000 (hex : 0)

↳ S_2 : 0000 ⊕ 0101 : 0101 → 0101 ⊕ 1000 : 1101 (hex : d)

↳ S_3 : 1101 ⊕ 1001 : 0100 → 0001 ⊕ 0110 : 0111 (hex : 7)

↳ S_4 : 0111 ⊕ 1001 : 1110 → 1011 ⊕ 0101 : 1110 (hex : e)

↳ S_5 : 1110 ⊕ 1100 : 0010 → 1000 ⊕ 0110 : 1110 (hex : e)

↳ S_6 : 1110 ⊕ 1110 : 0000 → 0000 ⊕ 1100 : 1100 (hex : c)

↳ S_7 : 1100 ⊕ 0111 : 1011 → 1110 ⊕ 0110 : 1000 (hex : 8)

↳ S_8 : 1000 ⊕ 1011 : 0011 → 1100 ⊕ 1100 : 0000 (hex : 0)

↳ S_9 : 0000 ⊕ 0101 : 0101 → 0101 ⊕ 0110 : 0011 (hex : 3)

↳ S_{10} : 0011 ⊕ 1001 : 1010 → 1010 ⊕ 1111 : 0101 (hex : 5)

↳ S_{11} : 0101 ⊕ 1001 : 1100 → 0011 ⊕ 0111 : 0100 (hex : 4)

↳ S_{12} : 0100 ⊕ 1100 : 1000 → 0010 ⊕ 0111 : 0101 (hex : 5)

↳ S_{13} : 0101 ⊕ 1110 : 1011 → 1110 ⊕ 0110 : 1000 (hex : 8)

↳ S_{14} : 1000 ⊕ 0111 : 1111 → 1111 ⊕ 1111 : 0000 (hex : 0)

↳ S_{15} : 0000 ⊕ 1011 : 1011 → 1110 ⊕ 0111 : 1001 (hex : 9)

↳ S_{16} : 1001 ⊕ 0101 : 1100 → 0011 ⊕ 0010 : 0001 (hex : 1)

↳ S_{17} : 0001 ⊕ 1001 : 1000 → 0010 ⊕ 0110 : 0100 (hex : 4)

Date

Fold

↳ S_{18} : 0100 ⊕ 1001 = 1101 → 0111 ⊕ 1100 = 1011 (hex = b)

↳ S_{19} = 1011 ⊕ 1100 = d11 → 1101 ⊕ 0110 = 1011 (hex = b)

↳ S_{20} : 1011 ⊕ 1110 = 0101 → 0101 ⊕ 0100 = 0001 (hex = 1)

Maka :

* Gabungan hasil CBC = f8375d3185e57fceaf5f

* Gabungan hasil CFB = 0d9507b6d010d5c4f50f