

$$5) \text{ plain} = [1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1] \\ \text{cipher} = [1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0]$$

$$\text{keystream} = \text{plain} \oplus \text{cipher}$$

$$KS = [0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1]$$

$$5 \text{ stage linear recurrence}$$

$$S_i = (C_1 \cdot S_{i-1}) \oplus (C_2 \cdot S_{i-2}) \oplus (C_3 \cdot S_{i-3}) \oplus (C_4 \cdot S_{i-4}) \oplus (C_5 \cdot S_{i-5})$$

$$S_0 = 0 \quad S_1 = 1 \quad S_2 = 0 \quad S_3 = 1 \quad S_4 = 1$$

$$S_5 = (C_1 \cdot S_4) \oplus (C_2 \cdot S_3) \oplus (C_3 \cdot S_2) \oplus (C_4 \cdot S_1) \oplus (C_5 \cdot S_0)$$

$$1 = (C_1 \cdot 1) \oplus (C_2 \cdot 1) \oplus (C_3 \cdot 0) \oplus (C_4 \cdot 1) \oplus (C_5 \cdot 0)$$

$$1 = C_1 \oplus C_2 \oplus C_4$$

$$S_6 = (C_1 \cdot S_5) \oplus (C_2 \cdot S_4) \oplus (C_3 \cdot S_3) \oplus (C_4 \cdot S_2) \oplus (C_5 \cdot S_1)$$

$$1 = (C_1 \cdot 1) \oplus (C_2 \cdot 1) \oplus (C_3 \cdot 1) \oplus (C_4 \cdot 0) \oplus (C_5 \cdot 1)$$

$$1 = C_1 \oplus C_2 \oplus C_3 \oplus C_5$$

$$S_7 = (C_1 \cdot S_6) \oplus (C_2 \cdot S_5) \oplus (C_3 \cdot S_4) \oplus (C_4 \cdot S_3) \oplus (C_5 \cdot S_2)$$

$$0 = (C_1 \cdot 1) \oplus (C_2 \cdot 1) \oplus (C_3 \cdot 1) \oplus (C_4 \cdot 1) \oplus (C_5 \cdot 0)$$

$$0 = C_2 \oplus C_3 \oplus C_4$$

$$S_8 = (C_1 \cdot S_7) \oplus (C_2 \cdot S_6) \oplus (C_3 \cdot S_5) \oplus (C_4 \cdot S_4) \oplus (C_5 \cdot S_3)$$

$$1 = (C_1 \cdot 1) \oplus (C_2 \cdot 0) \oplus (C_3 \cdot 1) \oplus (C_4 \cdot 1) \oplus (C_5 \cdot 1)$$

$$1 = C_1 \oplus C_3 \oplus C_4 \oplus C_5$$

$$S_9 = (C_1 \cdot S_8) \oplus (C_2 \cdot S_7) \oplus (C_3 \cdot S_6) \oplus (C_4 \cdot S_5) \oplus (C_5 \cdot S_4)$$

$$1 = (C_1 \cdot 1) \oplus (C_2 \cdot 1) \oplus (C_3 \cdot 0) \oplus (C_4 \cdot 1) \oplus (C_5 \cdot 1)$$

$$1 = C_1 \oplus C_2 \oplus C_4 \oplus C_5$$

★ Error
in #15

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \xrightarrow{R_2 - R_1} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow{R_4 - R_1} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \xrightarrow{R_5 - R_1} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\text{Swap } R_2, R_3 \Rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{R_4 + R_2} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow{R_1 - R_2} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{\begin{matrix} R_1 + R_3 \\ R_2 - R_3 \\ R_4 - 2R_3 \\ R_5 + R_3 \end{matrix}} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\xrightarrow{\begin{matrix} R_1 + R_4 \\ R_2 - 2R_4 \\ R_3 + R_4 \end{matrix}} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{\begin{matrix} R_1 - R_5 \\ R_2 + R_5 \\ R_3 - R_5 \end{matrix}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\Rightarrow C_1 = 1, C_2 = 0, C_3 = 0, C_4 = 0, C_5 = 0$$

Test

$$1 = C_1 \oplus C_2 \oplus C_4 = 1 \oplus 0 \oplus 0 \quad \checkmark$$

$$1 = C_1 \oplus C_2 \oplus C_3 \oplus C_5 = 1 \oplus 0 \oplus 0 \oplus 0 \quad \checkmark$$

$$0 = C_2 \oplus C_3 \oplus C_4 = 0 \oplus 0 \oplus 0 \quad \checkmark$$

$$1 = C_1 \oplus C_3 \oplus C_4 \oplus C_5 = 1 \oplus 0 \oplus 0 \oplus 0 \quad \checkmark$$

$$1 = C_1 \oplus C_2 \oplus C_4 \oplus C_5 = 1 \oplus 0 \oplus 0 \oplus 0 \quad \checkmark$$

$$S_8 = 1$$

$$S_7 = 1$$

$$S_6 = 0$$

$$S_5 = 1$$

$$S_4 = 1$$

$$S_3 = 1$$

$$S_2 = 0$$

$$S_1 = 1$$

$$S_0 = 0$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 2/3 \\ 2/3 \\ -1/3 \\ 2/3 \end{bmatrix}$$

$$Z_{i+5} = -3Z_i + 2Z_{i+1} + 2Z_{i+2} \\ + -Z_{i+3} + 2Z_{i+4} \\ \text{mod } 2$$

$$\Rightarrow Z_{i+5} = Z_i + Z_{i+3}$$