No.

Date / /

作业04.

1. 状态. 输出位.

1000 → 0

1100 → 0

1110 → 0

1111 → 1

0111 → 1

1011 → 1

0101 → 1

1010 → 0

1101 → 1

0110 → 0

0011 → 1

~~1001~~ → 1

~~0100~~ → 0

~~0010~~ → 0

~~0001~~ → ~~0~~ 1

~~0001 → 1~~

1000 → 0

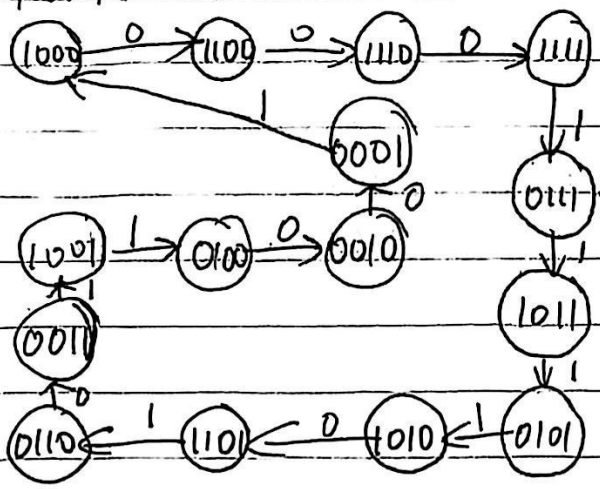
~~0100 → 0~~

~~0010 → 0~~

输出: 0001 1110 1011 0010 ……

周期为 15.

状态转换图.



2. 状态　输出　　输出序列：1101 11 …

1011 → 1　　周期：5.

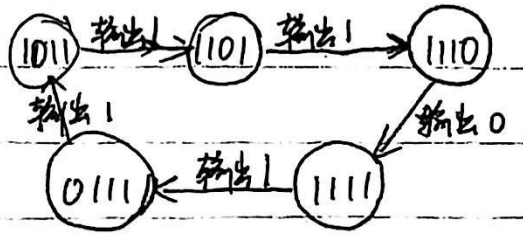
1101 → 1　　状态转换图：

1110 → 0

1111 → 1

0111 → 1

1011 → 1



3. 密钥流：1010110110 ⊕ 0100010001 = 1110100111 = k.

设 $f(b_3, b_2, b_1) = c_3b_3 \oplus c_2b_2 \oplus c_1b_1$.

$$\begin{pmatrix} k_4 \\ k_5 \\ k_6 \end{pmatrix} = \begin{pmatrix} k_1 & k_2 & k_3 \\ k_2 & k_3 & k_4 \\ k_3 & k_4 & k_5 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} \quad 即 \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

解得 $\begin{cases} c_1 = 1 \\ c_2 = 0 \\ c_3 = 1 \end{cases}$　　即 $f(b_3, b_2, b_1) = b_3 \oplus b_1$.

4. 由定理可知若特征多项式 $p(x)$ 为 5 阶本原多项式，输出序列为 m-序列.

∵ $1 + x^3 + x^5$ 为 5 阶本原多项式.

∴ 反馈函数为 $f(b_5, b_4, b_3, b_2, b_1) = b_5 \oplus b_3$.

5. ZUC算法是中国自主设计的流密码算法，简洁高效。

三层结构：1. LFSR层（16级）：由16个31bit寄存器组成，在GF($2^{31}-1$)中进行操作，用于生成随机序列。

~~初始化模式~~

L反馈多项式 $s_{16}\equiv(2^{15}\cdot s_{13}+2^{17}\cdot s_{10}+2^{21}\cdot s_4+2^{20}\cdot s_0+(2^8+1)\cdot s_0) \bmod (2^{31}-1)$.

L分两个模式：

①初始化模式：由 $V=(2^{15}\cdot s_{15}+\cdots+(2^8+1)s_0) \bmod (2^{31}-1)$

由 $s_{16}=(u+v) \bmod (2^{31}-1)$.

由若 $s_{16}=0$，则置 $s_{16}=2^{31}-1$.

由 $(s_0,s_1,\cdots,s_{16})\Rightarrow(s_0,s_1,\cdots s_{15})$.

其中u为F的输出舍弃最低bit位得到的序列。

②工作模式：由 $s_{16}=(2^{15}\cdot s_{15}+\cdots+(2^8+1)\cdot s_0) \bmod (2^{31}-1)$.

由若 $s_{16}=0$，置 $s_{16}=2^{31}-1$.

由 $(s_1,s_2\cdots s_{16})\Rightarrow(s_0,s_1\cdots s_{15})$

初始化目的在于使LFSR状态随机化。

2. BR层：从LFSR层抽128 bit组成4个32bit的字($X_0\sim X_3$)。

$$\begin{cases} X_0=S_{15H}\|S_{14L} \\ X_1=S_{11L}\|S_{9H} \\ X_2=S_{7L}\|S_{5H} \\ X_3=S_{2L}\|S_{0H} \end{cases}$$

（其中L取低16位，H取高16位）

⇒用于破坏LFSR的线性结构。

3. 非线性函数F层（由表示模2^{32}加法）。

$F(X_0,X_1,X_2)=$ {①$W=(X_0\boxplus R_1)\boxplus R_2$；②$W_1=R_1\boxplus X_1$；

③$W_2=R_2\boxplus X_2$；④$R_1=S(L_1(W_{1L}\|W_{2H}))$；

⑤$R_2=S(L_2(W_{2L}\|W_{1H}))$}.

其中，R_1、R_2为32位存储单元；S盒由4个并置8进8出盒构成，

即 $S=(S_0, S_1, S_2, S_3)$ 且 $S_0=S_2$，$S_1=S_3$；

$L_1(X)=X\oplus(X<<<2)\oplus(X<<<10)\oplus(X<<<18)\oplus(X<<<24)$.

$L_2(X)=X\oplus(X<<<8)\oplus(X<<<14)\oplus(X<<<22)\oplus(X<<<30)$.

~~LFSR~~特色与优势：~~从~~在有限域 $GF(2^{31}-1)$ 上运算，增加复杂度且硬件实现效率极高，同时考虑安全性与运算效率；且使用两种模式增强随机性保证安全。

具体流程：1. 密钥装入：128bit KEY，128bit IV. 扩展为16个31bit字.

利用一个240bit常量D.(16×15bit).

$[S_i=k_i\|d_i\|IV_i]$.

2. 初始化：置R_1、R_2全为0.重复为下过程32次：

① BR();

② $W=F(X_0, X_1, X_2)$;

③ LFSR With Initial Mode(u);

3. 工作：首先，执行初始化重复过程1次，丢掉W，(变为工作模式)

然后，依次执行以下流程，生成一个32bit字.

① BR();

② $W=F(X_0, X_1, X_2)\oplus$

③ $Z=W\oplus X_3$ → 输出.

④ LFSR With Work Mode();