دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

عنوان: تکلیف دوم درس مبانی رمزنگاری

نام و نام خانوادگی: علیرضا ابره فروش

شماره دانشجویی: ۹۸۱۶۶۰۳

نیم سال تحصیلی: بهار ۱۴۰۱/۱۴۰۲

مدرّس: دکتر سیدمحمد دخیل علیان

دستیاران آموزشی: گلاره عودی قدیم

۱

”One-time pad is a cryptographic encryption technique that uses a random key that is as long as the message itself. The key is used only once, and both the sender and receiver must have a copy of the same key to encrypt and decrypt messages. Here are some pros and cons of one-time pad:
Pros:

1. Security: One-time pad encryption is considered to be unbreakable if used correctly, as it provides perfect secrecy. The encryption key used is completely random and cannot be guessed or predicted, making it virtually impossible for an attacker to break.
2. Simplicity: One-time pad encryption is simple to understand and implement, as it involves only the use of a random key and the XOR operation. It does not require complex algorithms or mathematical computations, making it a preferred choice for encrypting short messages.
3. Privacy: One-time pad encryption ensures complete privacy, as it does not reveal any information about the original message, even if an attacker intercepts the ciphertext.

Cons:

1. Key distribution: One-time pad encryption requires both the sender and the receiver to have a copy of the same key. This can be challenging in practice, especially if the keys need to be distributed securely over long distances.
2. Key management: The one-time pad key can be used only once and must be discarded after use, making key management a challenge. Generating a truly random key that is as long as the message itself can also be difficult.
3. Size limitations: One-time pad encryption requires a key that is as long as the message, which can make it impractical for encrypting large amounts of data.
4. Vulnerable to certain attacks: One-time pad encryption is vulnerable to certain attacks, such as key reuse or guessing attacks, which can compromise the security of the encryption.”

۲

۱.۲

1. LFSRs which generate a maximum-length sequence. These LFSRs are based on primitive polynomials.
2. LFSRs which do not generate a maximum-length sequence but whose sequence length is independent of the initial value of the register. These LFSRs are based on irreducible polynomials that are not primitive. Note that all primitive polynomials are also irreducible.
3. LFSRs which do not generate a maximum-length sequence and whose sequence length depends on the initial values of the register. These LFSRs are based on reducible polynomials.

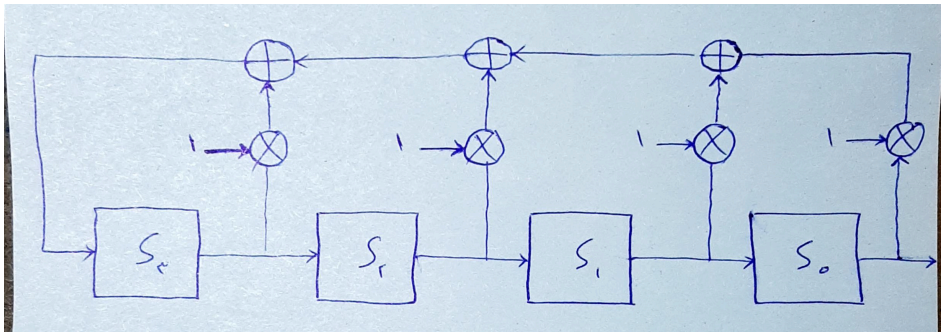
۲.۲

۱.۲.۲

$P(x) = x^4 + x^3 + x^2 + x + 1$

$m = 4$

$p_3 = p_2 = p_1 = p_0 = 1$



شکل ۱

از آنجایی که این چندجمله‌ای را نمی‌توان به چندجمله‌ای غیر ۱ای تجزیه کرد پس irreducible است. پس این reducible LFSR نیست. برای بررسی اینکه آیا primitive است باید بررسی کنیم که آیا طول بزرگترین دنباله‌ای که تولید می‌کند ماکسیمم $(2^4 - 1)$ هست یا نه. طبق جدول زیر تناوب طولانی‌ترین دنباله ساخته شده توسط این LFSR برابر ۵ است که کمتر از ۱۵ است. پس این primitive LFSR نیست. در نتیجه این LFSR بر پایه‌ی primitive polynomial است.

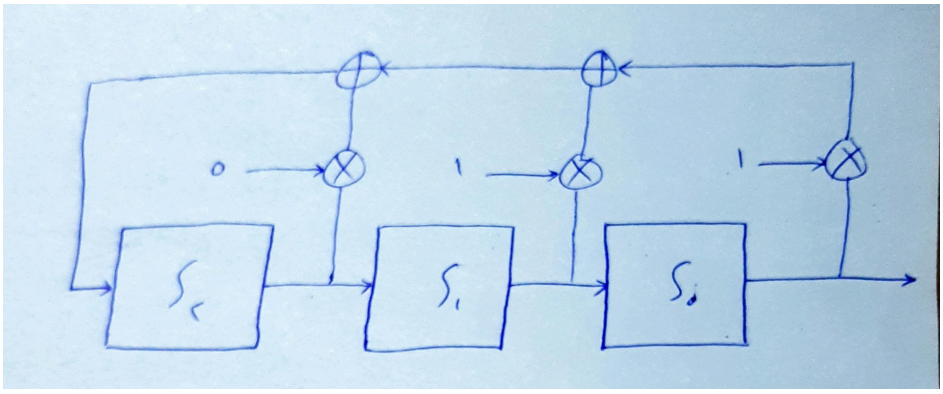
1	0	1	0	1
2	0	0	1	0
3	1	0	0	1
4	0	1	0	**0**
5	1	0	1	0
6	0	1	0	1

۲.۲.۲

$P(x) = x^3 + x + 1$

$m = 3$

$p_2 = 0, p_1 = p_0 = 1$



شکل ۲

از آنجایی که این چندجمله‌ای را نمی‌توان به چندجمله‌ای غیر ۱ای تجزیه کرد پس irreducible است. پس این reducible LFSR نیست. برای بررسی اینکه آیا primitive است باید بررسی کنیم که آیا طول بزرگترین دنباله‌ای که تولید می‌کند ماکسیمم $(2^3 - 1)$ هست یا نه. طبق جدول زیر تناوب طولانی‌ترین دنباله ساخته شده توسط این LFSR برابر ۷ است. پس این primitive LFSR است.

1	1	0	1
2	1	1	0
3	1	1	1
4	0	1	**1**
5	0	0	1
6	1	0	0
7	0	1	0
8	1	0	1

۳

$y_i \equiv x_i + s_i \mod 2$

$\Rightarrow s_i \equiv y_i - x_i \equiv y_i + x_i \mod 2$

$\Rightarrow$

x_i	1	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1	0	0	1	0	0	1	0	0	1	1	0
y_i	1	0	1	1	1	1	0	0	0	0	1	1	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	1
s_i	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1

۱.۳

با فرض primitive بودن LFSR، و با توجه به اینکه دنباله‌ی به طول هفتِ ۰۰۱۰۱۱۱ چهار بار تکرار شده است، احتمالا LFSR تولید کننده‌ی این key stream از درجه‌ی $\log_2 (7 + 1) = 3$ است.

۲.۳

مقدار اولیه‌ی LFSR با توجه به قسمت قبل برابر سه بیت اول دنباله است که برابر است با ۰۰۱.

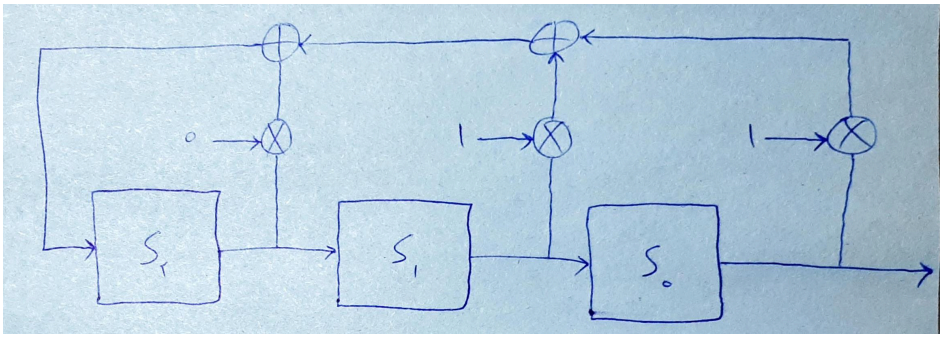
۳.۳

$$\begin{bmatrix} s_2 & s_1 & s_0 \\ s_3 & s_2 & s_1 \\ s_4 & s_3 & s_2 \end{bmatrix} \begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix} = \begin{bmatrix} s_3 \\ s_4 \\ s_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} s_2 & s_1 & s_0 \\ s_3 & s_2 & s_1 \\ s_4 & s_3 & s_2 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

۴.۳



شکل ۳

$$s_{i+1} \equiv s_{i-2} + s_{i-3} \mod 2$$

1	1	0	0
2	0	1	0
3	1	0	1
4	1	1	0
5	1	1	1
6	0	1	1
7	0	0	1
8	1	0	0

با توجه به جدول بالا درست است.

منابع