CRYPTO1 - 05/12/2023

TUE	05/12	CRYPTO I — STREAM CIPHERS
WED	06/12	PROF TARICCO
TUE	12/12	DR. MAIOLINI — BLOCK CIPHERS - AES
WED	13/12	TUTORING ON STREAM CIPHERS
FRI	15/12	ZOOM TUTORING ? (TO BE CONFIRMED)
TUE	18/12	PQC - MCELIECE
WED	20/12	END OF MCELIECE + TUTORING
FRI	22/12	ZOOM TUTORING

TUE	09/01	TUTORING
WED	10/01	TUTORING
FRI	12/01	ZOOM TUTORING
TUE	16/01	CANCELED
WED	17/01	CANCELED
FRI	19/01	ZOOM TUTORING

APPLICATION OF INFORMATION THEORY
CRYPTOGRAPHIC FEATURES
KERCKOFFS' PRINCIPLE
ATTACKS
SYMMETRIC AND ASYMMETRIC ENCRYPTION
SYMMETRIC ENCRYPTION SCHEME
FUNDAMENTAL ENTROPY PROPERTIES OF A SECURE SCHEME
ENTROPY OF THE KEY AND KEY LENGTH
ONE-TIME PAD
STREAM CIPHERS VS. BLOCK CIPHERS
BINARY RANDOM SEQUENCES AND THEIR PROPERTIES
LFSRS, M-SEQUENCES AND THEIR PROPERTIES
LFSRS AND STREAM CIPHERS: THE LINEARITY PROBLEM

EXERCISE 4.1

APPLICATION OF INFORMATION THEORY: CODING

SOME REDUNDANCY IS ADDED TO COUNTER NOISE AND INTERFERENCE

- ERROR DETECTION: CHECK MESSAGE INTEGRITY (≡ DETECT THE ERROR) [CRC]
- ERROR CORRECTION: CORRECT THE ERRORS (TURBO CODES, LDPC, POLAR CODES)

APPLICATION OF INFORMATION THEORY: CRYPTOGRAPHY

TO PREVENT

- UNAUTHORIZED READING OF THE MESSAGE
- CHANGING THE MESSAGE
- STEALING THE IDENTITY
- REPUDIATING A MESSAGE

CRYPTOGRAPHIC FEATURES

- CONFIDENTIALITY
- INTEGRITY
- AUTHENTICATION
- SIGNATURE (THE IDENTITY OF THE SENDER CAN BE PROVED BY A THIRD PARTY AUTHORITY)

CRYPTANALYSIS

ATTACKER WANTS TO

- READ MESSAGE
- CHANGE MESSAGE
- STEAL IDENTITY

AUTHOR WAHTS TO

- REPUDIATE MESSAGE

KERCKOFFS' PRINCIPLE

THE ATTACHER PERFECTLY KNOWS THE ENCRYPTION ALGORITHM

("THE ENEMY KNOWS THE SYSTEM"
C. SHANNON)

PROTECTION MUST BE ASSURED BY

- ALGORITHM
- KEY

TERMINOLOGY

MESSAGE ≡ PLAINTEXT

ENCRYPTED MESSAGE ≡ CIPHERTEXT

ATTACKS

CIPHERTEXT ONLY:

THE ATTACHER HAS ACCESS TO SOME CIPHERTEXTS

KNOWN PLAINTEXT

THE ATTACKER HAS ACCESS

TO SOME

PLAINTEXT/ CIPHERTEXT PAIRS

CHOSEN PLAINTEXT

THE ATTACKER IS ABLE

TO OBTAIN THE CIPERTEXT

CORRESPONDING TO ANY

PLAINTEXT IT WANTS.

BRUTE FORCE ATTACK

THIS IS A CIPHERTEXT-ONLY ATTACK WHERE THE ATTACHER TRIES ALL THE POSSIBLE KEYS.

COMPUTATIONALLY SECURE ALGORITHM

THE ALGORITHM IS ABLE TO RESIST TO AN ATTACK FOR A REASONABLE AMOUNT OF TIME

Example of brute-force attack

Check all possible keys until you guess the correct one

In order to simply flip through the possible values for a 128-bit symmetric key you need 2^{128} operations

Fastest supercomputer is about 1000 PetaFLOPS = 1000 10^{15} FLOPS = $10^{18} \cong 2^{60}$

$2^{128}/2^{60} = 2^{48}$ seconds about 9 Myears

DIFFERENTIAL CRYPTANALYSIS

CHOSEN PLAINTEXT ATTACK

WHERE THE ATTACKER

IS ABLE TO OBTAIN THE

CIPHERTEXTS

CORRESPONDING TO PLAINTEXTS

WITH SOME SPECIFIC DIFFERENCES

(E.G. CAST BYTE)

LINEAR CRYPTANALYSIS

THE ATTACKER BUILDS A LINEAR MODEL INVOLVING PLAINTEXT, KEY, CIPHERTEXT TO APPROXIMATE THE TRUE ENCRYPTION ALGORITHM LOOKING FOR SOME BIAS REVEALING PORTION OF THE PLAINTEXT OR KEY.

FOR ENCRYPTION

LINEARITY IS VERY BAD

GIVEN A PLAINTEXT/ CIPHERTEXT

PAIR WE CAN RECOVER THE

KEY AND DECODE ALL

SUCCESSIVE MESSAGES

ALL ENCRYPTION ALG. MUST

HAVE A NON-LINEAR COMPONENT

SYMMETRIC AND ASYMMETRIC ENCRYPTION

SYMMETRIC: THERE IS A SINGLE PRIVATE KEY WHICH IS USED FOR ENCRYPTION AND DECRYPTION

(THE KEY MUST BE EXCHANGED ON A SECURE CHANNEL BEFORE STARTING ENCRYPTION)

[AES]

ASYMMETRIC: THERE ARE TWO KEYS

ONE PUBLIC USED FOR ENCRYPTION

ONE PRIVATE USED FOR DECRYPTION

[RSA]

SYMMETRIC AND ASYMMETRIC SCHEMES CAN BE COMBINED TOGETHER.

FOR EXAMPLE, ASYMMETRIC ENCRYPTION CAN BE USED TO EXCHANGE THE PRIVATE KEY THEN SYMMETRIC ENCRYPTION FOR EXCHANGING MESSAGES.

[EX. TLS / SSL PROTOCOL]

ALPHABETS

A

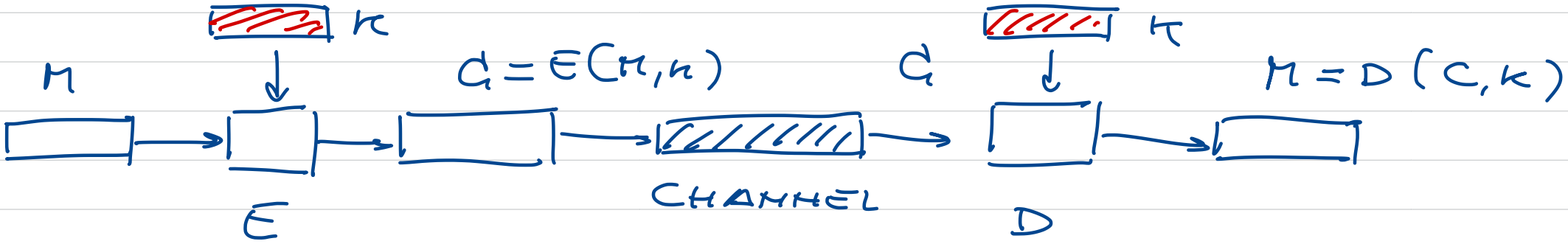
PLAINTEXT MESSAGE $M \in A^{N_n}$

(VECTORS OF N_n SYMBOLS TAKEN FROM A)

KEY $K \in A^{N_k}$

CIPHERTEXT $C \in A^{N_c}$

SYMMETRIC ENCRYPTION SCHEME



E ≡ ENCRYPTION ALGORITHM

D ≡ DECRYPTION ALGORITHM

ENTROPY AND INFORMATION GAIN

$H(X)$ ≡ ENTROPY ≡ MEASURE OF UNCERTAINTY ABOUT X

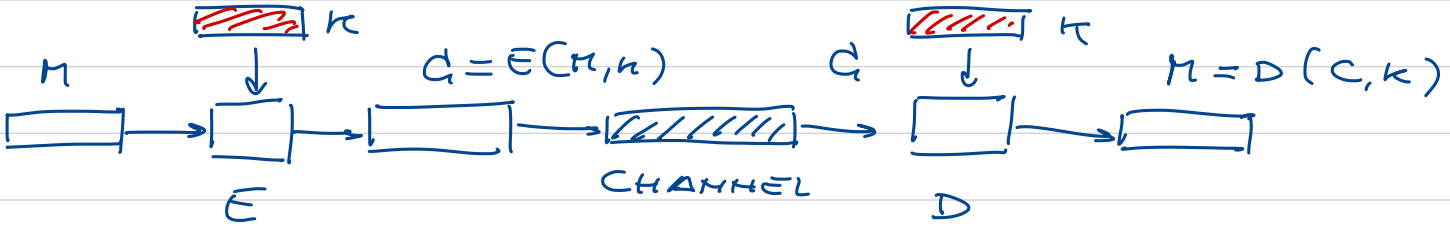
$H(X,Y)$ ≡ JOINT ENTROPY $H(X,Y) = H(X|Y) + H(Y)$

$H(X|Y)$ ≡ CONDITIONAL ENTROPY ≡ RESIDUAL UNC. ABOUT X AFTER Y IS OBSERVED

$I(X;Y) = H(X) - H(X|Y)$ ≡ INFORMATION GAIN

≡ REDUCTION OF UNCERTAINTY ABOUT X WHEN Y IS OBSERVED

FUNDAMENTAL ENTROPY PROPERTIES OF A SECURE SCHEME



① $H(M|C) = H(M)$ $\qquad I(M;C) = 0$

② $H(M|C,K) = 0$

THESE ARE THE FUNDAMENTAL PROPERTIES OF A COMPLETELY SECURE SYMMETRIC ENCRYPTION SCHEME

ENTROPY OF THE KEY

$$H(K) \geq H(K|C) = H(K,C) - H(C) = (*)$$

$$H(K,C,M) = \underbrace{H(M|K,C)}_{0} + H(K,C)$$

$$(*) = H(K,C,M) - H(M,C) = H(K|C,M)$$

$$- H(C) + H(M,C) + H(M|C)$$

$$= H(K|C,M) + H(M|C) \geq H(M|C) = H(M)$$

$$\geq 0$$

$$H(K) \geq H(M)$$

FINAL RESULT

$$H(k) \geq H(n)$$

KEY LENGTH

SUPPOSE THAT BOTH MESSAGE AND KEY ARE MADE BY RANDOM SYMBOLS FROM ALPHABET A

$$H(K) = N_K \; H(A)$$

$$H(M) = N_M \; H(A)$$

$$\rightarrow \quad N_K \geq N_M$$

$N_K \geq N_n$

TO HAVE A COMPLETELY SECURE ENCRYPTION SCHEME

THE KEY SHOULD BE AT LEAST AS LONG AS THE MESSAGE

ONE-TIME PAD

$A = \{0, 1\}$ $\oplus$ BINARY SUM

$+$	0	1
0	0	1
1	1	0

M OF N BITS

K OF N BITS

$$C = E(M, K) = M \oplus K$$

$$M = D(C, K) = C \oplus K$$

$$\begin{array}{r} 1011 \\ 1011 \\ \hline 0000 \end{array}$$

expl. $C \oplus K = M \oplus \underbrace{K \oplus K}_{0} = M$

THIS IS COMPLETELY SECURE

BUT

- THE KEY HAS SAME LENGTH OF THE MESSAGE
- CANNOT BE REUSED

(IF WE REUSE IT TWICE, IT'S EQUIVALENT TO USE A KEY OF N BITS FOR A MESSAGE OF 2N BITS)

DISCUSSION

IN PRACTICAL THE KEY LENGTH IS ALWAYS SMALLER THAN THE MESSAGE LENGTH

STREAM CIPHERS VS. BLOCK CIPHERS

STREAM CIPHERS: WE START FROM THE KEY,
WE GENERATE A LONG PSEUDO-RANDOM SEQUENCE
AND WE ENCRYPT OUR MESSAGE BY A
SYMBOL BY SYMBOL
BINARY SUM

BLOCK CIPHERS: WE USE THE KEY
WE ENCRYPT OUR MESSAGE
BLOCK BY BLOCK
BY A COMPLEX ALGORITHM

STREAM CIPHERS

MESSAGE M OF n_n BITS

KEY K OF $n_k < n_n$ BITS

K IS USED TO GENERATE A PSEUDO. RANDOM

SEQUENCE S OF n_n BITS

ENCRYPTION:

$C = M \oplus S$ BINARY SUM

DECRYPTION:

SAME K IS USED TO GENERATE S

$\rightarrow M = C \oplus S$

ADVANTAGES OF STREAM CIPHERS

TYPICALLY VERY FAST

ENCRYPTION IS THE BINARY SUM

WITH A LONG PSEUDO-RANDOM
SEQUENCE

DIFFICULT TO GENERATE

SECURE PSEUDO-RANDOM SEQUENCES

(FOR SOME APPLICATIONS, BLOCK CIPHERS

ARE CONSIDERED MORE SECURE)

RANDOM BINARY SEQUENCES

STREAM CIPHERS:

WE NEED A LONG PSEUDO. RANDOM BINARY SEQUENCE
TO ENCRYPT OUR MESSAGES

MATH.
PROPERTIES OF A BINARY RANDOM SEQ.

BITS
- STATISTICALLY IND.
- EQUI. PROBABLE

IF WE OBSERVE A BINARY RANDOM SEQUENCE

WE HAVE THESE PROPERTIES;

LENGTH N LONG ENOUGH

$$N_0 = N_1 = \frac{N}{2}$$

N_0: # OF ZEROS

N_1: # OF ONES

RUN OF LENGTH i IS A SEQUENCE

OF i CONSECUTIVE EQUAL SYMBOLS

$$\underset{1}{1}\,\underset{1}{0}\,\underset{2}{11}\,\underset{2}{00}\,\underset{3}{111}\,0$$

$N_T \equiv$ TOTAL NUMBER OF RUNS $= \frac{N}{2}$

$N_i \equiv$ NUMBER OF RUNS OF LENGTH i $= \frac{N_T}{2^i}$

$N_i(0) = N_i(1)$ [# RUNS OF ZEROS OF LENGTH i

= # RUNS OF ONES OF LENGTH i]

AUTO. CORRELATION

1 0 1 1 — $\underline{v}$ BINARY SEQUENCE

1 1 0 1

= ≠ ≠ = — $\underline{v}'$ BIPOLAR SEQUENCE

$1 \to +1$

$0 \to -1$

$$R(\tau) = \sum_{i=0}^{N-1} v'(i)\, v'(i-\tau)$$

$$0 \le \tau \le N-1$$

1 −1 1 1

1 1 −1 1

1 −1 −1 1 = 0

WE VIEW THE SEQUENCE AS PERIODIC WITH PERIOD N

$0 \le z \le N-1$

$z = 0$

$1 \quad 1 \quad 0 \quad 1$

$\downarrow$

$1 \quad 1 \quad -1 \quad 1$

$1 \quad -1 \quad 1 \quad 1$

$1 \quad 1 \quad 1 \quad 1 \quad = 4$

N

$z = 1$

$1 \quad 1 \quad -1 \quad 1$

$1 \quad -1 \quad 1 \quad 1$

$z = 2$

$1 \quad 1 \quad 1 \quad -1$

$1 \quad -1 \quad 1 \quad 1$

FOR A BINARY RANDOM SEQUENCE

$$R(\tau) = \begin{cases} \tau = 0 & R(\tau) = N \\ \tau \neq 0 & R(\tau) = 0 \end{cases}$$

WE NOW INTRODUCE AN ALGORITHM

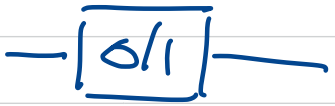
THAT STARTING FROM A SEED

GENERATES A PSEUDO-RANDOM

BINARY SEQUENCE

WITH NEARLY OPTIMAL PROPERTIES

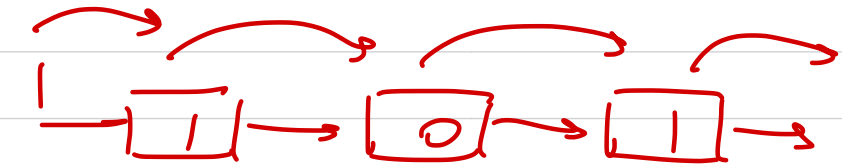
SHIFT REGISTERS



CELL

SHIFT REGISTER

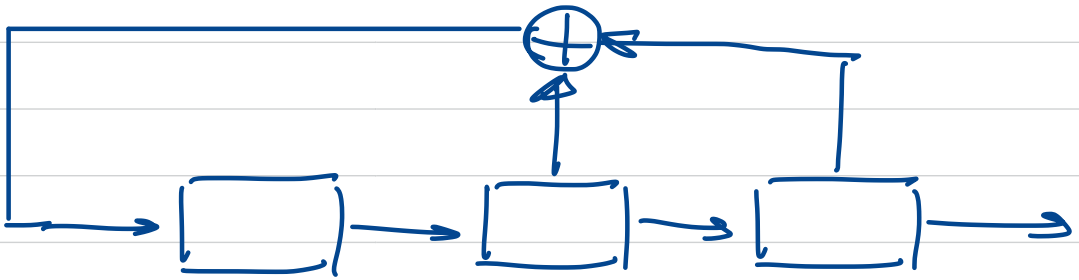
M CELLS



TIME IS SLOTTED

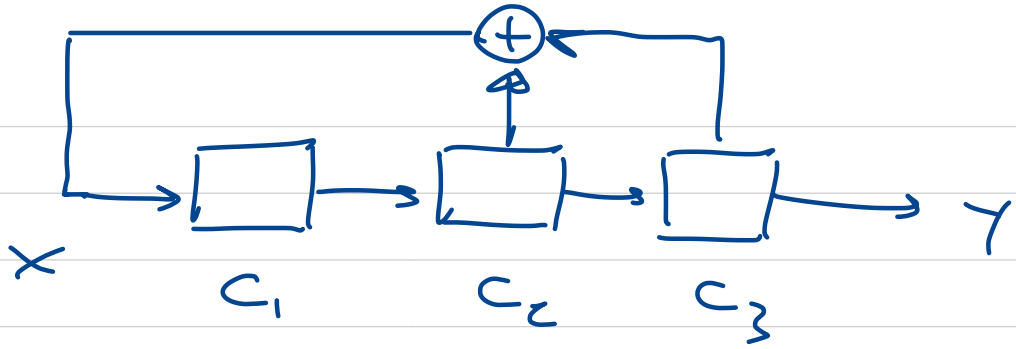
BITS MOVE LEFT TO RIGHT

LINEAR FEEDBACK SHIFT REGISTER (LFSR)



INPUT BIT IS GENERATED BY THE CELL CONTENT

THE OUTPUT BIT IS TAKEN FROM LAST CELL



$X = C_2 \oplus C_3$	C_1	C_2	C_3	$Y = C_3$
1	0	0	1	1
0	1	0	0	0
1	0	1	0	0
1	1	0	1	1
1	1	1	0	0
0	1	1	1	1
0	0	1	1	0
		0	1	

FROM THIS POINT THE SEQUENCE IS REPEATED

OUTPUT SEQ. = 1 0 0 1 0 1 1

PERIOD

$N = 7$

$N = 2^m - 1$

THE ALL-ZERO STATE MUST BE AVOIDED: IF WE ENTER IT WE STAY THERE FOREVER

→ THE BITS GENERATED ARE ALL ZEROS

→ NOT RANDOM!

MAXIMUM PERIOD

$$N = 2^m - 1$$

NOTE:

IF WE START FROM ANOTHER

STARTING SEED

WE OBTAIN A CYCLIC SHIFT

OF THE SAME SEQUENCE

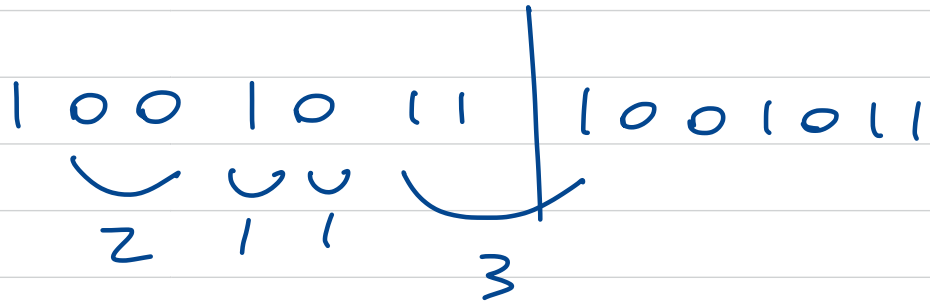
NUMBER OF ZEROS AND ONES

1 0 0 1 0 1 1

$N = 7$ $N_1 = 4$ $N_0 = 3$

$N_1 = N_0 + 1$

RUNS



- $N_1 = 2$
- $N_2 = 1$

$N_3 = 1$

$$N_i = \frac{N_T}{2^i}$$

$$N_T = N_1 + N_2 + N_3 = 4$$

AUTO-CORRELATION

$$R(\tau) = \begin{cases} N & \tau = 0 \\ 0 & \tau \neq 0 \end{cases}$$

IDEAL

$$R(\tau) = \begin{cases} N & \tau = 0 \\ -1 & \tau \neq 0 \end{cases}$$

LFSR SEQUENCE

1001011

1 −1 −1 1 −1 1 1

1 1 −1 −1 1 −1 1

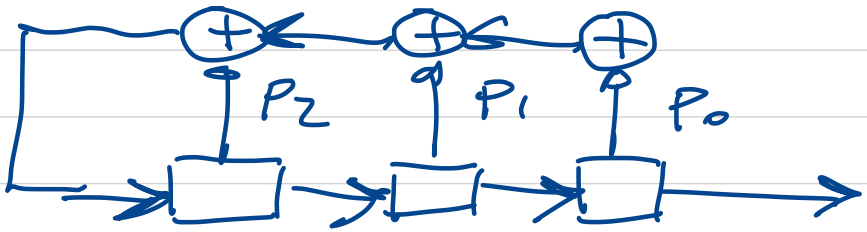
1 −1 1 −1 −1 −1 1 = −1

WITH m CELLS

AN LFSR GENERATES A BINARY SEQUENCE WITH PERIOD $N = 2^m - 1$

IF THE FEEDBACK IS PROPERLY CHOSEN

POLYNOMIAL DESCRIPTION



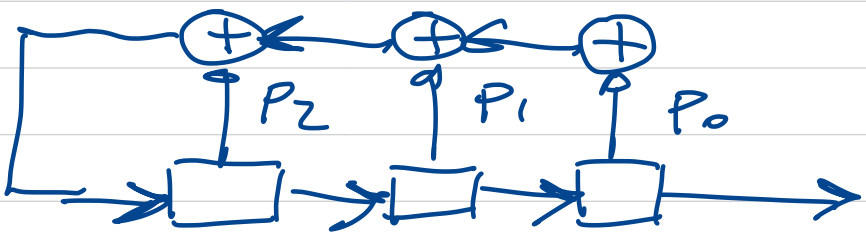
$p_i \begin{cases} 0 \\ 1 \end{cases}$

$$p(D) = D^3 + p_2 D^2 + p_1 D + p_0$$

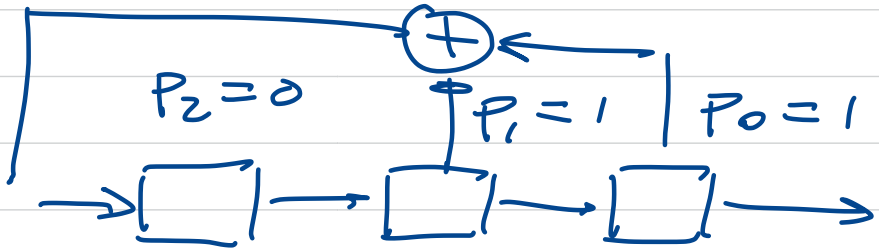
↑ INDETERMINATE

POLYNOMIAL DESCRIPTION

$p_i \begin{cases} 0 \\ 1 \end{cases}$



$$p(D) = D^3 + p_2 D^2 + p_1 D + p_0$$



$$D^3 + D + 1$$

PRIMITIVE POLYNOMIAL

WHEN THE POLYNOMIAL IS

PRIMITIVE

THE PERIOD IS MAXIMUM

$$N = 2^m - 1$$

AND THE BINARY SEQUENCE

IS CALLED

AN M-SEQUENCE

↑

MAXIMAL

PERIOD

LFSR AND STREAM CIPHERS

IN PRINCIPLE WE COULD USE AN LFSR FOR A STREAM CIPHER:

- WE START FROM A KEY OF N_K BITS
- WE USE IT AS THE STARTING SEED OF AN LFSR WITH $m = N_K$ CELLS
- WE GENERATE THE M-SEQUENCE S OF $N = 2^{N_K} - 1$ BITS
- WE ENCRYPT OUR MESSAGE AS A STREAM CIPHER $C = M \oplus S$

THE LINEARITY PROBLEM

UNFORTUNATELY THERE IS A PROBLEM!

THE LFSR IS LINEAR → IF WE OBSERVE

2M CONSECUTIVE BITS OF AN

M-SEQUENCE S WE CAN COMPUTE

THE LFSR POLYNOMIAL COEFFICIENTS

→ STARTING FROM THIS POINT WE

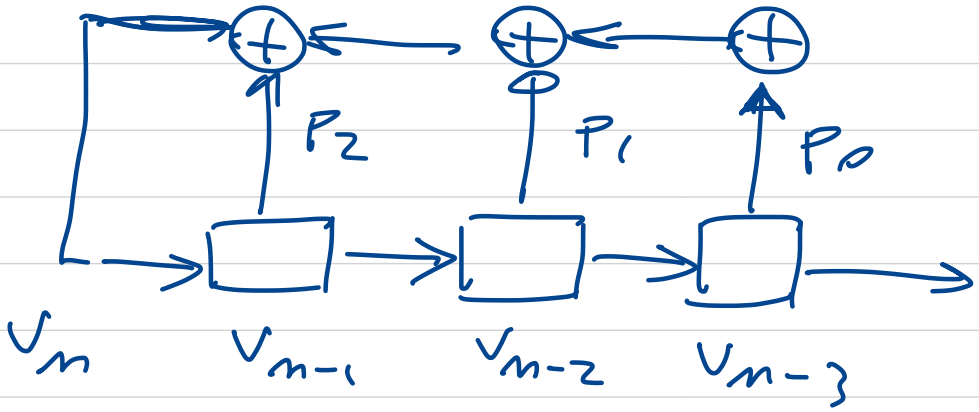
ARE ABLE TO GENERATE ALL

SUCCESSIVE BITS OF THE SEQUENCE S

THEN WE CAN DECRYPT THE

CIPHERTEXT !

How To Break A Linear LFSR



$v_{n-3}\ v_{n-2}\ v_{n-1}\ v_n \ldots$

Given this binary sequence we want to determine $p_2\ p_1\ p_0$

$$v_n = p_2 v_{n-1} + p_1 v_{n-2} + p_0 v_{n-3}$$

Sequence: $v_0\ v_1\ v_2\ v_3\ v_4\ v_5$ (2m bits)

$$v_3 = p_2 v_2 + p_1 v_1 + p_0 v_0$$
$$v_4 = p_2 v_3 + p_1 v_2 + p_0 v_1$$
$$v_5 = p_2 v_4 + p_1 v_3 + p_0 v_2$$

$$\rightarrow \begin{bmatrix} v_5 \\ v_4 \\ v_3 \end{bmatrix} = \begin{bmatrix} v_4 & v_3 & v_2 \\ v_3 & v_2 & v_1 \\ v_2 & v_1 & v_0 \end{bmatrix} \begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix}$$

$\rightarrow$ Solve for $\begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix}$

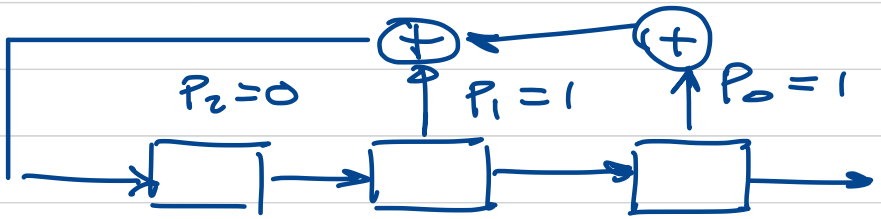
$v_0\ v_1\ v_2\ v_3\ v_4\ v_5$

$1\ 0\ 0\ 1\ 0\ 1$ ✗

$$\begin{bmatrix} v_5 \\ v_4 \\ v_3 \end{bmatrix} = \begin{bmatrix} v_4 & v_3 & v_2 \\ v_3 & v_2 & v_1 \\ v_2 & v_1 & v_0 \end{bmatrix} \begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix}$$

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

$p_1 = 1$
$p_2 = 0$
$p_0 = 1$



NOTE THAT WE CAN OBTAIN A SEGMENT OF 2M CONSECUTIVE BITS OF THE SEQUENCE S BY A KNOWN PLAINTEXT ATTACK ON A PORTION OF THE MESSAGE

$$C_i = M_i \oplus S_i \rightarrow S_i = M_i \oplus C_i$$

NON-LINEARITY

TO HAVE A SECURE STREAM CIPHER

WE MUST ADD SOME NON-LINEARITY

TO THE LFSR

→ THIS WAY EVEN IF WE

ARE ABLE TO INTERCEPT

A PORTION OF THE SEQUENCE Σ

WE ARE NOT ABLE TO

COMPUTE THE POLYNOMIAL COEFFICIENTS

AND BREAK THE SYSTEM

Assignment 4

Draft version 0.1 04/12/2023

Politecnico di Torino - Master of Science in Data Science and Engineering

Information Theory for Data Science
Prof. Roberto Garello
roberto.garello@polito.it

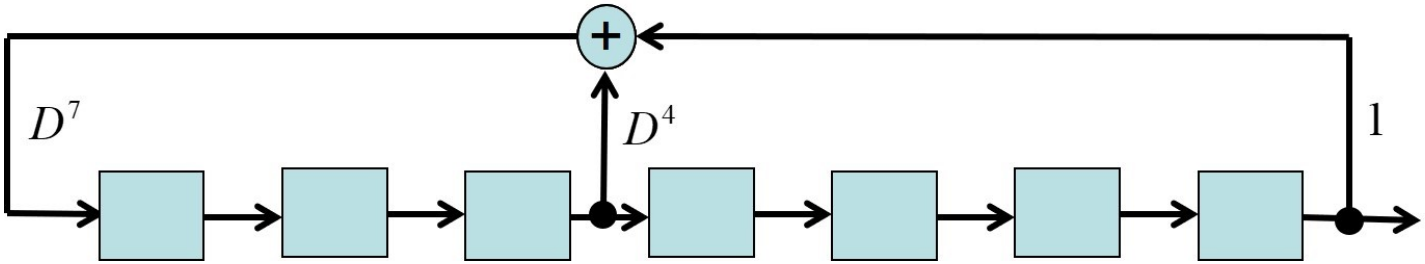
Assignment 4

- Exercise 1 - Stream Ciphers - pt. XX

Exercise 1 - Stream Ciphers - pt. XXX

Exercise 1 - LFSR M-sequences

Study the M-sequence generated by this Linear Feedback Shift Register (LFSR):



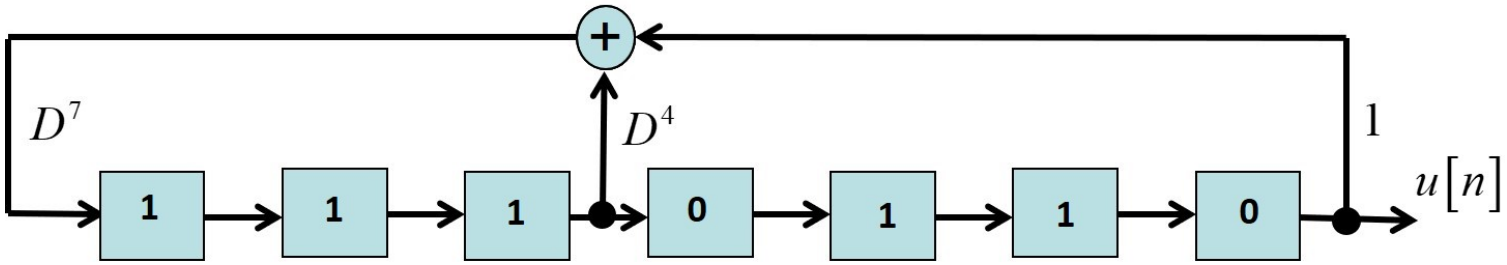
The LFSR is characterized by;

- m=7 cells
- polynomial $D^7 + D^4 + 1$

(The association between the feedback connections and the polynomial coefficients is not unique, the reverse order is used too. The proposed one is the association used by Matlab in its functions.)

Starting seed

Use the starting seed 1110110



The polynomial is primitive then the LFSR generates an m-sequence with

- period $N = 2^m - 1 = 127$ bits
- first bits = 0110111100...

Denote the binary sequence by $v(n)$ and the corresponding bipolar sequence $(0 \to -1,\ 1 \to +1)$ by $v'(n)$, for $0 \leq n \leq N-1$.
When needed, consider them as the principal periods of periodic sequences.

0/1

1. (pt. XXX) Generate the 127-bit M-sequence $v(n)$, compute the values of N_1 and N_0 (number of bits equal to 1 or 0 in $v(n)$), check if $N_1 = N_0 + 1$.
2. (pt. XXX) Prove that for an M-sequence we always have $N_1 = N_0 + 1$.

Runs

$$\frac{N_T}{2^i}$$

3. (pt. XXX) Write a table with the values of $NR_0(i)$ and $NR_1(i)$ (number of runs of i consecutive 0 or 1 symbols in $v(n)$).
4. (pt. XXX) Compare the values of $NR(0)$ and $NR(1)$ against the run properties of an ideal binary random sequence.
5. (pt. XXX) Prove that we cannot have a run of m zeros, or a run of $m+1$ ones.

Autocorrelation

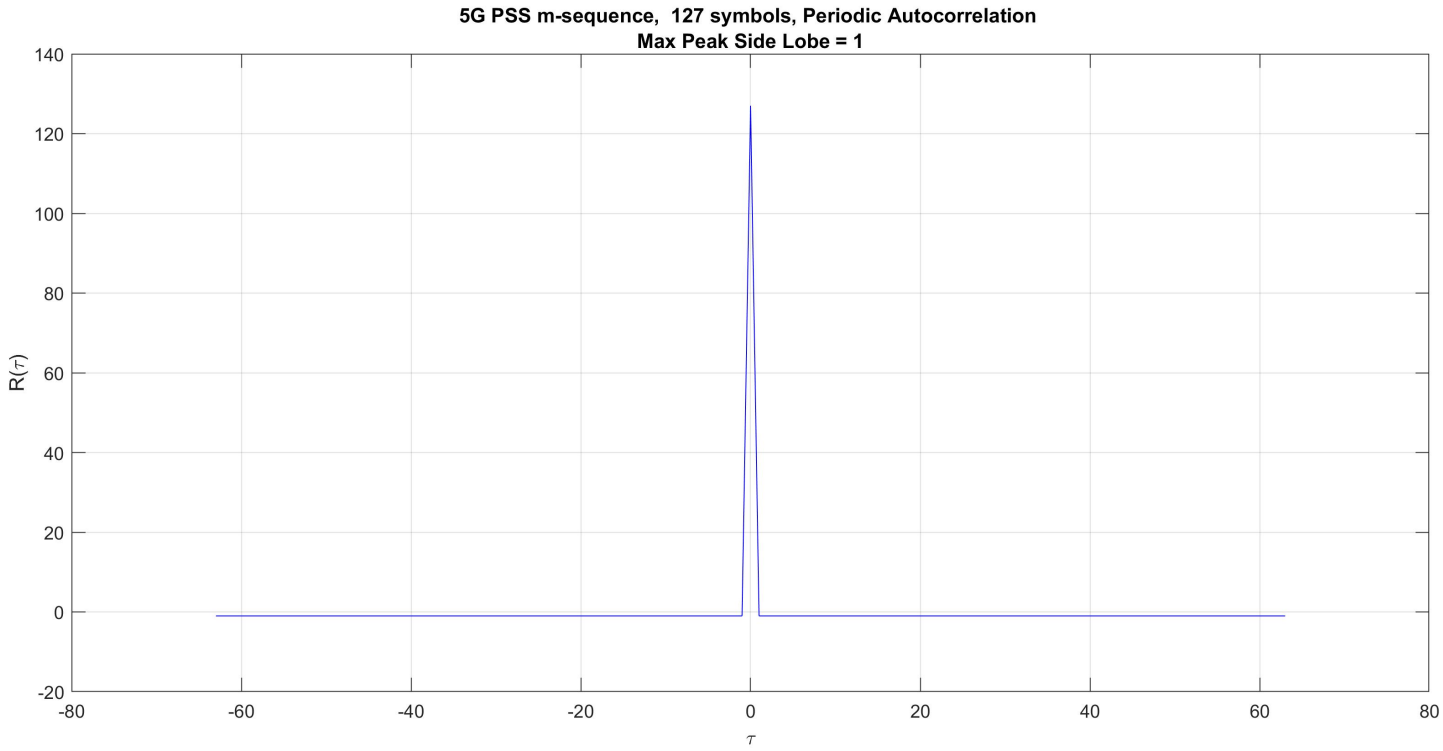
5. (pt. 0.5) Compute and plot the periodic autocorrelation function

$$R(\tau) = \sum_{n=0}^{N-1} v'(n)\, v'(n-\tau) \qquad -\frac{N-1}{2} \leq \tau \leq \frac{N-1}{2}$$

Verify the property:

- $R(\tau) = N$ for $\tau = 0$
- $R(\tau) = -1$ for $\tau \neq 0$

Autocorrelation plot



Matlab

LFSR

```
m=7; % number of cells
Nb=2^m-1; % period
pnSequence = comm.PNSequence('Polynomial',[7 4 0], ...
'SamplesPerFrame',Nb,'InitialConditions',[1 1 1 0 1 1 0]);
x1 = pnSequence()';
```

Matlab

Autocorrelation

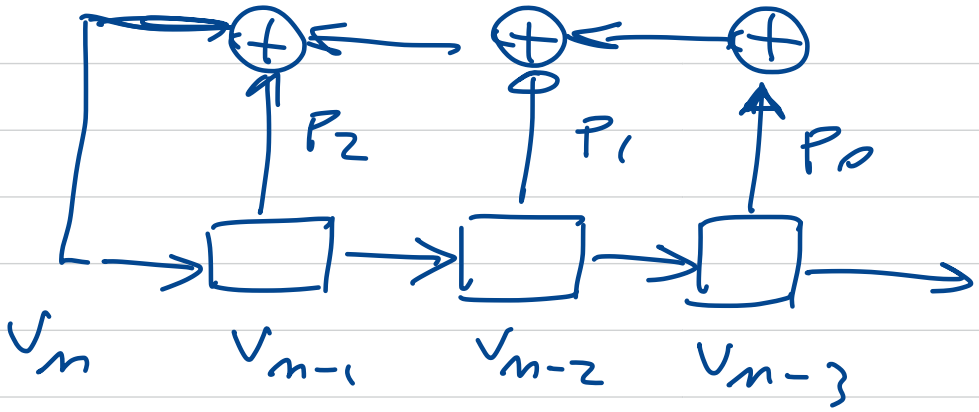
x1b=2*x1-1; % bipolar version 0 $\rightarrow$ -1 1 $\rightarrow$ +1
R=ifft(fft(x1b).*conj(fft(x1b))); % non-normalized periodic autocorr.

Breaking a linear LFSR

By a chosen plaintext attack, you manage to intercept this portion of the key: XXXXXXXXX(40 bits)

I sent the string by email to all the students who delivered Assignment 1. If you did not receive the email, contact me (roberto.garello@polito.it).

6. (pt. XXX) Compute the primitive polynomial of the LFSR
7. (pt. XXX) Generate the next 20 bits of the key



$v_{n-3}\ v_{n-2}\ v_{n-1}\ v_n \ldots$

GIVEN THIS BINARY SEQUENCE WE WANT TO DETERMINE $p_2\ p_1\ p_0$

$$v_n = p_2 v_{n-1} + p_1 v_{n-2} + p_0 v_{n-3}$$

SEQUENCE: $v_0\ v_1\ v_2\ v_3\ v_4\ v_5$

$$v_3 = p_2 v_2 + p_1 v_1 + p_0 v_0$$
$$v_4 = p_2 v_3 + p_1 v_2 + p_0 v_1$$
$$v_5 = p_2 v_4 + p_1 v_3 + p_0 v_2$$

$$\rightarrow \begin{bmatrix} v_5 \\ v_4 \\ v_3 \end{bmatrix} = \begin{bmatrix} v_4 & v_3 & v_2 \\ v_3 & v_2 & v_1 \\ v_2 & v_1 & v_0 \end{bmatrix} \begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix}$$

$\rightarrow$ SOLVE FOR $\begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix}$

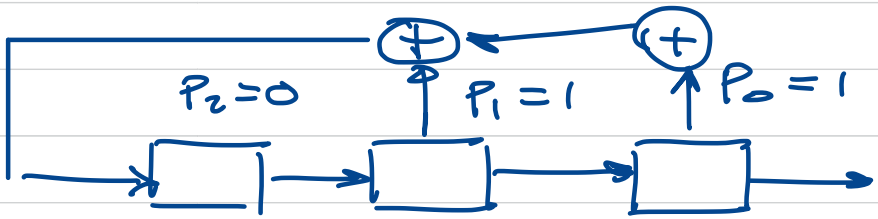
$v_0\ v_1\ v_2\ v_3\ v_4\ v_5$

$1\ 0\ 0\ 1\ 0\ 1$ ✗

$$\begin{bmatrix} v_5 \\ v_4 \\ v_3 \end{bmatrix} = \begin{bmatrix} v_4 & v_3 & v_2 \\ v_3 & v_2 & v_1 \\ v_2 & v_1 & v_0 \end{bmatrix} \begin{bmatrix} p_2 \\ p_1 \\ p_0 \end{bmatrix}$$

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

$p_1 = 1$
$p_2 = 0$
$p_0 = 1$



Matlab

How to solve equations in GF(2)

R = rank(gf(A)); % computes the rank of the binary matrix A
[x,v] = gflineq(A,b,2); % solves the binary linear equation b=Ax
(If $v = 0$ the equation has no solution.)

- START FROM $m = 3$
- TRY TO COMPUTE b
- IF b EXISTS CHECK IF SUCCESSIVE BITS ARE CORRECT
- IF YES GENERATE NEXT 20 BITS AND STOP
- OTHERWISE $m = m+1$ AND REPEAT

SNOW

7. (pt. XXX) Consider the SNOW stream cipher (choose a version), and prepare no more than 3 slides as if you had to present them to your colleagues: scheme, high-level description, (no details,) give some info on applications and how non-linearity is achieved, list the references used.

THIS PART NOT FOR FINAL EXAM

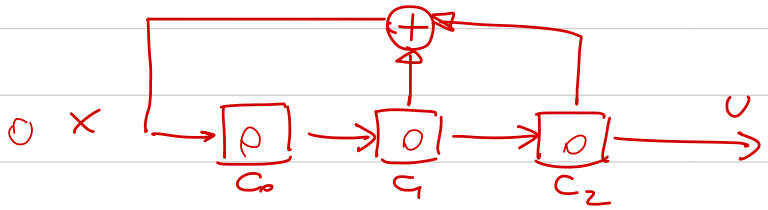
A BINARY POLYNOMIAL OF DEGREE m

IS PRIMITIVE IF AND ONLY IF

- IT IS DIVISIBLE ONLY BY 1 AND ITSELF
- IT DIVIDES $D^x + 1$ WITH $x = 2^m - 1$

  AND DOES NOT DIVIDE $D^y + 1$ WITH $y < x$

LFSR AND MATRIX REPRESENTATION · COLUMN MULTIPLICATION



SEED = INITIAL CONFIGURATION OF THE LFSR

$X = C_1 + C_2$	C_0 C_1 C_2	$U = C_2$
0	1 0 0	0
1	0 1 0	0
1	1 0 1	1
1	1 1 0	0
0	0 1 1	1
0	1 0 1	1
1	0 0 1	

CURRENT STATE → NEXT STATE

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} C_0' \\ C_1' \\ C_2' \end{bmatrix}$$

$$C_0' = C_1 \oplus C_2$$

$$C_1' = C_0$$

$$C_2' = C_1$$

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{matrix} 0 \\ 1 \\ 0 \end{matrix} \rightarrow \begin{matrix} 1 \\ 0 \\ 1 \end{matrix} \rightarrow \begin{matrix} 1 \\ 1 \\ 0 \end{matrix} \rightarrow \begin{matrix} 1 \\ 1 \\ 1 \end{matrix} \rightarrow \begin{matrix} 0 \\ 1 \\ 1 \end{matrix} \rightarrow \begin{matrix} 0 \\ 0 \\ 1 \end{matrix} \rightarrow \begin{matrix} 1 \\ 0 \\ 0 \end{matrix}$$

BINARY MATRIX × BINARY VECTOR

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$G^N = I$$

$N \equiv$ ORDER OF THE MATRIX

NOW WE SHOW THAT $p(D)$ REPRESENTING THE CFSR MUST BE A PRIMITIVE POLYNOMIAL

LFSR AND MATRIX · ROW MULTIPLICATION

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\begin{pmatrix} x_2 & x_1 & x_0 \end{pmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{matrix} 0 \\ 0 \\ 1 \end{matrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

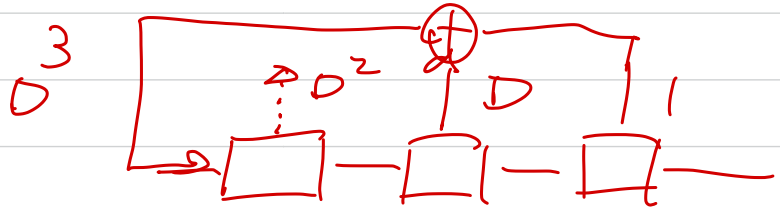
$k = 7$

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$G^{N} = I$$

$$(0\,0\,1) \rightarrow (0\,1\,0) \rightarrow (1\,0\,0) \rightarrow (0\,1\,1) \rightarrow (1\,1\,0)$$

$$\rightarrow (1\,1\,1) \rightarrow (1\,0\,1) \rightarrow (0\,0\,1)$$



$$p(D) = D^3 + D + 1$$

$$(x_2\,x_1\,x_0) \equiv x_2 D^2 + x_1 D + x_0 = x(D) \equiv \text{polynomial representation of vector } (x_2\,x_1\,x_0)$$

$$x(D) \cdot D \mod p(D)$$

ROW MULTIPLICATION CORRESPONDS TO THIS OPERATION

$(001) \rightarrow (010) \rightarrow (100) \rightarrow (011) \rightarrow (110)$

$\rightarrow (111) \rightarrow (101) \rightarrow (001)$

$(x_2 x_1 x_0) = x_2 D^2 + x_1 D + x_0 \qquad p(D) = D^3 + D + 1$

$1 \rightarrow D \rightarrow D^2 \rightarrow D^3 = D + 1 \rightarrow D^2 + D \rightarrow$

$\rightarrow D^3 + D^2 = D^2 + D + 1 \rightarrow D^3 + D^2 + D = D^2 + 1 \rightarrow$

$\rightarrow D^3 + D = 1 \rightarrow$ SINCE WE HAVE PERIOD 4

$$x(D) \cdot D^4 \bmod p(D) = x(D)$$

$$x(D) \cdot D^N \bmod p(D) = x(D)$$

$$x(D)(D^N + 1) \bmod p(D) = 0$$

$p(D)$ DIVIDES $D^N + 1$

PRIMITIVE POLYNOMIAL

CAN BE DIVIDED ONLY BY 1 AND ITSELF

+ DIVIDES $D^N + 1$ WITH

$$N = 2^m - 1$$

$$m = \text{degree}(p(D))$$

AN LFSR MUST HAVE

FEEDBACK COEFFICIENTS

CORRESPONDING TO A

PRIMITIVE POLYNOMIAL

→ THIS WAY THE PERIOD N IS

MAXIMUM $N = 2^m - 1$

AND THE BINARY SEQUENCE

HAS THE DESIRED PROPERTIES.