HW 3

Sunday, April 5, 2020 22:16

Aaron Fox
CECS 564-01
Dr. Desoky

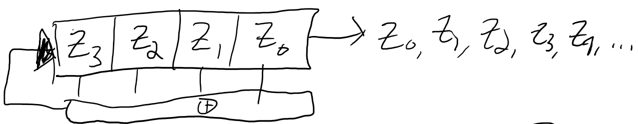
HW #3

1.18 Consider the following linear recurrence over $\mathbb{Z}_2$ of degree four:

$$z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2,$$

$i \geq 0$. For each of the 16 possible initialization vectors $(z_0, z_1, z_2, z_3) \in (\mathbb{Z}_2)^4$, determine the period of the resulting keystream.

$$Z_{i+4} = (Z_i + Z_{i+1} + Z_{i+2} + Z_{i+3}) \ \% \ 2, \quad i \geq 0$$



(0,0,0,0) → 0000] period is only 1
0000
0000
⋮

(0,0,0,1) → 0001
1000
1100
0110
0011
0001
1000
period = 5

(0,1,1,0) → 0110
0011
0001
1000
1100
0110
period = 5

(0,1,1,1) → 0111
1011
1101
1110
1111
0111
period = 5

(0,0,1,0) → 0010
1001
0100
1010
0101
0010
period = 5

(0,0,1,1) → 0011
0001
1000
1100
0110
0011
period = 5

(1,0,0,0) → 1000
1100
0110
0011
0001
1000
period = 5

(0,1,0,0) → 0100
1010
0101
0010
1001
0100
period = 5

(1,0,0,1) → 1001
0100
1010
0101
0010
period = 5

1001
0100

(0,1,0,1) → 0101
0010
1001
0100
1010
0101
period = 5

1010
0101
0010
1001
period = 5

(1,0,1,0) → 1010
0101
0010
1001
0100
1010
period = 5

(1,0,1,1) → 1011
1101
1110
1111
0111
1011
period = 5

(1,1,0,0) → 1100
0110
0011
0001
1000
1100
period = 5

(1,1,0,1) → 1101
1110
1111
0111
1011
1101
period = 5

(1,1,1,0) → 1110
1111
0111
1011
1101
1110
period = 5

(1,1,1,1) → 1111
0111
1011
1101
1110
1111
period = 5

$\therefore$ (0,0,0,0) has a period of 1 and all other initialization vectors have a period of 5

1.19 Redo the preceding question, using the recurrence

$$z_{i+4} = (z_i + z_{i+3}) \bmod 2,$$

$i \geq 0$.

The following code was used to print out cycles of every possible initialization vector:

```python
# Prototype Linear-Feedback Shift Register method that will
# be replaced by the generator method below it
# INPUT: taps: The equivalent primitive polynomial used (e.g. for polynomial x^
15 + x + 1, taps=[15, 1])
#        seed: Seed of LSFR to be used in binary, e.g. 40 bit key of '00011001111
0011000000011010000000000001100'
# OUTPUT: None (just prints)
def LFSR(taps, seed):
    print("With initialization vector (" + seed[0] + ", " + seed[1] + ", " + seed
[2] + ", " + seed[3] + "):")
    s = seed
    xor_output = 0
    init_pass = 0
    cycle_length = 0
    print(s)
    while (s != seed or init_pass == 0):# and cycle_length < 5:
        cycle_length = cycle_length + 1
        init_pass = 1
        for tap in taps:
            # print("int(s[len(s)-tap]) == " + str(int(s[len(s)-tap])))
            xor_output = xor_output + int(s[len(s)-tap])
            # xor_output = xor_output + int(s[tap-1])

        if xor_output % 2 == 0.0:
            xor_output = 0
        else:
            xor_output = 1
        s = str(xor_output) + s[0:len(s) - 1]
        xor_output = 0
        print(s)
    # Print out final seed also to show cycle
    print(s)
    print("Cycle length: " + str(cycle_length))
LFSR([4, 1], '0000')
LFSR([4, 1], '0001')
...
```

```
With initialization vector (0, 0, 0, 0):
0000
0000
0000
Cycle length: 1
```

```
With initialization vector (0, 0, 0, 1):
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
0100
0010
0001
0001
Cycle length: 15
```

```
With initialization vector (0, 0, 1, 0):
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
0100
0010
0010
Cycle length: 15
```

```
With initialization vector (0, 0, 1, 1):
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
0011
Cycle length: 15
```

```
With initialization vector (0, 1, 0, 0):
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
0100
0100
Cycle length: 15
```

```
With initialization vector (0, 1, 0, 1):
0101
1010
1101
0110
0011
1001
0100
0010
```

```
0100
0100
Cycle length: 15
```

```
With initialization vector (0, 1, 1, 0):
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0110
Cycle length: 15
```

```
With initialization vector (1, 0, 0, 0):
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
0100
0010
0001
1000
1000
Cycle length: 15
```

```
With initialization vector (1, 0, 1, 0):
1010
1101
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1010
Cycle length: 15
```

```
With initialization vector (1, 1, 0, 0):
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
0100
0010
0001
1000
1100
1100
Cycle length: 15
```

```
With initialization vector (1, 1, 1, 0):
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
```

```
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
0101
Cycle length: 15
```

```
With initialization vector (0, 1, 1, 1):
0111
1011
0101
1010
1101
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
0111
Cycle length: 15
```

```
With initialization vector (1, 0, 0, 1):
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
0110
0011
1001
1001
Cycle length: 15
```

```
With initialization vector (1, 0, 1, 1):
1011
0101
1010
1101
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
1011
Cycle length: 15
```

```
With initialization vector (1, 1, 0, 1):
1101
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
0111
1011
0101
1010
1101
1101
Cycle length: 15
```

```
With initialization vector (1, 1, 1, 1):
1111
0111
1011
0101
```

```
1010
1101
0110
0011
1001
0100
0010
0001
1000
1100
1110
1110
Cycle length: 15
```

```
With initialization vector (1, 1, 1, 1):
1111
0111
1011
0101
1010
1101
0110
0011
1001
0100
0010
0001
1000
1100
1110
1111
1111
Cycle length: 15
```

Based on the above LFSR simulations, the initialization vector of (0,0,0,0) has a period of 1 while all other initialization vectors have a period of 15.

Class Problem #1 — Baye's Theorem Probabilistic Security

Crypto System $e(k,p)$

	a	b	c
k_1	A	B	C
k_2	C	A	B
k_3	B	C	A

$K = \{k_1, k_2, k_3\}$, $P = \{a, b, c\}$, $C = \{A, B, C\}$

$Pr\{a\} = \frac{1}{4}$, $Pr\{b\} = \frac{1}{2}$, $Pr\{c\} = \frac{1}{4}$

$Pr\{k_1\} = \frac{1}{2}$, $P\{k_2\} = \frac{1}{4}$, $Pr\{k_3\}$ 1/4

Compute the following:

1. Marginal pdf of C
2. Use Baye's Theorem to Compute $Pr\{P \mid C\}$
3. Discuss the security of the given System

(1) Marginal pdf of C

$Pr(C) = ?$

		1/4	1/2	1/4
		a	b	c
$\frac{1}{2}$	K_1	A	B	C
$\frac{1}{4}$	K_2	C	A	B
1/4	K_3	B	C	A

$$Pr(C = 'A') = Pr(P=a) \cdot Pr(K=K_1) + Pr(P=b) \cdot Pr(K=K_2) + Pr(P=c) \cdot Pr(K=K_3)$$

$$= \frac{1}{4}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{4} + \frac{1}{4}\cdot\frac{1}{4} = \frac{5}{16} = 0.3125$$

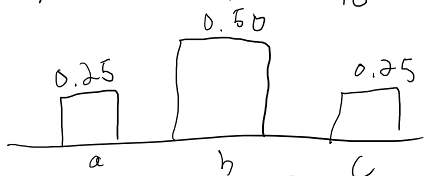
$$Pr(C = \text{'B'}) = Pr(p=b)\cdot Pr(p=k_1) + Pr(p=c)\cdot Pr(p=k_2) + Pr(p=a)\cdot Pr(k=k_3)$$

$$= \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{4}\cdot\frac{1}{4} + \frac{1}{4}\cdot\frac{1}{4} = \frac{3}{8} = 0.375$$

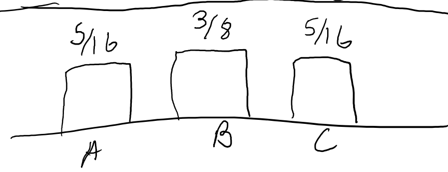
$$Pr(C = \text{'C'}) = Pr(P=c)\cdot Pr(P=k_1) + Pr(P=a)\cdot Pr(p=k_2) + Pr(P=b)\cdot Pr(P=k_3)$$

$$= \frac{1}{4}\cdot\frac{1}{2} + \frac{1}{4}\cdot\frac{1}{4} + \frac{1}{2}\cdot\frac{1}{4} = \frac{5}{16} = 0.3125$$

pdf(p) =



$\therefore$ pdf(C) =



② Use Bayes' Theorem to compute

$$Pr\{P \mid C\}$$

$$Pr(P \mid C) = \frac{P(C \mid P)\cdot P(P)}{Pr(C)}$$

First, $p(C \mid P) = \sum_{e(k,p)=C} Pr(K)$

$Pr(C \mid P) = C$

	a	b	c
A	1/2	1/4	1/4
B	1/4	1/2	1/4
C	1/4	1/4	1/2

$\therefore$

$Pr(P \mid C) =$

	A	B	C
a	2/5	1/6	1/5
b	2/5	2/3	2/5
c	1/5	1/6	2/5

$$Pr(a \mid A) = \frac{Pr(A \mid a)\cdot Pr(a)}{Pr(A)} = \frac{\frac{1}{2}\cdot\frac{1}{4}}{5/16} = \frac{2}{5} = .4$$

$$Pr(a|A) = \frac{Pr(A|a) \cdot Pr(a)}{Pr(A)} = \frac{\frac{1}{2} \cdot \frac{1}{4}}{5/16} = \frac{2}{5} = .4$$

$$Pr(b|A) = \frac{Pr(A|b) \cdot Pr(b)}{Pr(A)} = \frac{1/4 \cdot 1/2}{5/16} = \frac{2}{5} = .4$$

$$Pr(c|A) = \frac{Pr(A|c) \cdot Pr(c)}{Pr(A)} = \frac{1/4 \cdot 1/4}{5/16} = \frac{1}{5} = .2$$

$$Pr(a|B) = \frac{Pr(B|a) \cdot Pr(a)}{Pr(B)} = \frac{\frac{1}{4} \cdot 1/4}{3/8} = \frac{1}{6} = 0.1\overline{6}$$

$$Pr(b|B) = \frac{Pr(B|b) \cdot Pr(b)}{Pr(B)} = \frac{\frac{1}{2} \cdot 1/2}{3/8} = \frac{2}{3} = 0.\overline{6}$$

$$Pr(c|B) = \frac{Pr(B|c) \cdot Pr(c)}{Pr(B)} = \frac{1/4 \cdot 1/4}{3/8} = \frac{1}{6} = 0.1\overline{6}$$

$$Pr(a|C) = \frac{Pr(C|a) \cdot Pr(a)}{Pr(C)} = \frac{1/4 \cdot 1/4}{5/16} = \frac{1}{5} = 0.2$$

$$Pr(b|C) = \frac{Pr(C|b) \cdot Pr(b)}{Pr(C)} = \frac{1/4 \cdot 1/2}{5/16} = \frac{2}{5} = 0.4$$

$$Pr(c|C) = \frac{Pr(C|c) \cdot Pr(c)}{Pr(C)} = \frac{1/2 \cdot 1/4}{5/16} = \frac{2}{5} = 0.4$$

See $Pr(P|C)$ above

(3) Discuss the security of the given system.

Here, a posteriori dist $= Pr(P|C) =$

	A	B	C
a	2/5	1/6	1/5
b	2/5	2/3	2/5
c	1/5	1/6	2/5

and a priori dist $= Pr(P) =$

A cryptosystem is perfectly secure iff

$Pr(P|C) = Pr(P)$ for any cipher message C.

Since $\Pr(P|C) \neq \Pr(P)$ in this system,
this system is <u>NOT</u> perfectly secure and
is vulnerable to easy attacks.

```
>> p=[.25 .5 .25];
>> pk=[.5 .25 .25];
>> e=[1 2 3; 3 1 2; 2 3 1];
>> [q pgc]=Bayes(p,pk,e)

q =

   0.3125   0.3750   0.3125


pgc =

   0.4000   0.1667   0.2000
   0.4000   0.6667   0.4000
   0.2000   0.1667   0.4000
```

<u>not</u> equal

Conditions of perfect security

1.) $|P| = |K| = |C|$

2.) keys are randomly generated w/ equal probability
$P(K_1) = P(K_2) = P(K_3)$

3.) $\Pr(P|C) = \Pr(P)$

Here #2 is violated since $K_1 = \frac{1}{2} \neq K_2 = 1/4$
as is #3 as illustrated above.

The system is thus <u>not</u> perfectly secure
like OTP and can be
easily attacked.

Class #2 Which of the following 2nd order polynomials are irreducible in $GF(2^2)$

x^2 , x^2+1 , x^2+x , x^2+x+1

Irreducible polynomials are polynomials of order ≥ 2
w/ coefficients in $GF(2)$ or 0 or 1
s.t. it can't be reduced or factored

x^2 is not irreducible b/c $(0)^2 = 0$ so 0 is a root

• x is <u>NOT</u> ...

• x^2+1 is <u>NOT</u> irreducible b/c $(1)^2+1 \% 2=0$ so 0 is a root

• x^2+x is <u>NOT</u> irreducible b/c $(0)^2+(0)=0$ & $(1)^2+(1)=0$, so 0 & 1 are roots

• x^2+x+1 <u>is</u> irreducible of 2^{nd} order

b/c $(0)^2+0+1 \% 2=1$

and $(1)^2+(1)+1 \% 2=1$

∴ x^2+x+1 the only irreducible polynomial of the order 2 polynomials listed above.

Class # 3 Draw the multiplication table of $GF(2^3)=\{0,1,2,3,4,5,6,7\}$ using the irreducible Poly x^3+x^2+1

$GF(2^3)=\{0,1,2,3,4,5,6,7\}$

w/ irreducible polynomial x^3+x^2+1, or 13

$*_{13}$		0 0	1 1	x 2	$x+1$ 3	x^2 4	x^2+1 5	x^2+x 6	x^2+x+1 7
0	0	0	0	0	0	0	0	0	0
1	1	0	$\boxed{1}$	2	3	4	5	6	7
x	2	0	2	4	6	5	7	1	3
$x+1$	3	0	3	6	5	$\boxed{1}$	2	7	4
x^2	4	0	4	5	$\boxed{1}$	7	3	2	6
x^2+1	5	0	5	7	2	3	6	4	$\boxed{1}$
x^2+x	6	0	6	$\boxed{1}$	7	2	4	3	5
x^2+x+1	7	0	7	3	4	6	1	5	2

x^3:

x^3
x^3+x^2+1
$x^2+1=5$

x^3+x
x^3+x^2+1
$x^2+x+1=7$

$\cancel{x^3}+\cancel{x^2}$
$\cancel{x^3}+\cancel{x^2}+1$
$1=1$

$\cancel{x^3}+\cancel{x^2}+x$
$\cancel{x^3}+\cancel{x^2}+1$
$x+1=3$

$(x+1)(x+1)=x^2+\cancel{2x}+1=x^2+1=5$

$(x^2+1)(x+1)$
$=\cancel{x^3}+\cancel{x^2}+x+1$
$+\cancel{x^3}+\cancel{x^2}+1$

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

$(x^2+x)(x+1)=\cancel{x^3}+\cancel{2x^2}+x$
$+\cancel{x^3}+x^2+1$

$= x^4 + x + 1 \cdot x + 1$
$+ x^3 + x^2 \quad + 1$
x

$x^3 + x^2 + 1$
$1 = 1$

$(x^2+x)(x+1) = x^3 + 2x^2 + x$
$+ x^3 + x^2 + 1$
$x^2 + x + 1 = 7$

$(x+1)(x^2+x+1) = x^3 + \cancel{x^2} + \cancel{x} + \cancel{x^2} + \cancel{x} + 1 = x^3 + 1$
$+ x^3 + x^2 + 1$
$x^2 = 4$

$x^2 \cdot x^2 = x^4 = x^2 + x + 1 = 7$

$x^2(x^2+1) = x^4 + x^2 = \cancel{x^2} + x + 1 + \cancel{x^2} = x + 1 = 3$

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

0	1	x	x^2	x^2+1	x^2+x+1	
0	1	x	x^2	x^3	x^4	x^5

$x^2(x^2+x+1) = x^4 + x^3 + x^2$
$= x^2 + x + \cancel{1} + \cancel{x^2} + \cancel{1} + \cancel{x^2}$
$= x^2 + x = 6$

$x^3 + x^2 + 1 = 0$
$\Rightarrow x^3 = x^2 + 1$

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

$(x^2+1)(x^2+1) = x^4 + \cancel{2x^2} + 1$
$= x^2 + x + \cancel{1} + \cancel{1} = 6$

$(x^2+1)(x^2+x) = x^4 + x^3 + x^2 + x$
$= \cancel{x^2} + \cancel{x} + \cancel{1} + \cancel{x^2} + \cancel{1} + x^2 + \cancel{x} = x^2 = 4$

$(x^2+1)(x^2+x+1) = x^4 + x^3 + x^2 + x^2 + x + 1$
$= \cancel{x^2} + \cancel{x} + \cancel{1} + \cancel{x^2} + \cancel{1} + \cancel{x^2} + \cancel{x^2} + \cancel{x} + 1 = 1 = 1$

$(x^2+x)(x^2+x) = x^4 + \cancel{2x^3} + x^2 = \cancel{x^2} + x + 1 + \cancel{x^2} = 3$

$(x^2+x)(x^2+x+1) = x^4 + \cancel{x^3} + \cancel{x^2} + \cancel{x^3} + \cancel{x^2} + x = x^2 + \cancel{x} + 1 + \cancel{x} = x^2 + 1 = 5$

$(x^2+x+1)(x^2+x+1) = x^4 + \cancel{x^3} + \cancel{x^2} + \cancel{x^3} + \cancel{x^2} + \cancel{x} + x^2 + \cancel{x} + 1$
$= \cancel{x^2} + x + \cancel{1} + \cancel{x^2} + \cancel{1} = x = 2$