COL-759

Tutorial Sheet - 4

2019MCS2574

VIVEK SINGH

Q1. A binary sequence which satisfies Golomb's randomness postulates is called pseudo noise sequence or pn sequence. Consider the periodic sequence $S = 0\,11\,00\,1\,000\,1111\,01$ of period $n = 15$. Is this sequence pn-sequence? Justify

Soln: $S = 0\,11\,00\,1\,000\,1111\,01$

period = 15.

To show S is a pn sequence, it must satisfy all 3 rules of golomb's postulates

R1:- $|\#1's - \#0's| \leq 1$

$\#1's = 8$

$\#0's = 7$

$\therefore$ R1 is satisfied

R2: Total Run in sequence = 8

1 length Run = 4

2 length Run = 2

3 length Run = 1

4 length Run = 1

$\therefore$ R_2 is satisfied

R3: Autocorrelation function $C(\tau)$

$C(0) = 1$

$C(\tau) = -1/15$ for $1 \leq \tau \leq 14$

$\therefore$ R3 is satisfied

Since 'S' follows all golomb's postulates Hence it is 'pn- Sequence".

Q2: The So called S-box ..... $x \in GF(2^8) \rightarrow x^{-1} \in GF(2^8)$
i.e 8 bit I/p bits are mapped to 8 bit o/p bit.
What is total number of possible mapping one can specify for function S?

Since $f \in GF(2^n)$ can be represented as Polynomial.

$$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots a_1 x + a_0$$

∴ ~~Input~~: where $a_i \in GF(2)$
$a_i \in \{0,1\}$

inputs: $\underbrace{2 \times 2 \times 2 \cdots}_{n \text{ time}} = 2^n$

For each I/p there is a corresponding mapping in $GF(2^n)$
as $f: GF(2^n) \longrightarrow GF(2^n)$

o/p:- 2^n

∴ Total mapping for function S =

$$\underbrace{2^n * 2^n * 2^n \cdots * 2^n}_{2^n \text{ times}}$$

$= (2^n)^{2^n}$.

Q3 In crypto & computer security, man-in-the middle attack (MITM), is an attack where the attacker secretly relays and possibly alters communication b/w two parties, who believe that they are directly communicating with each other.

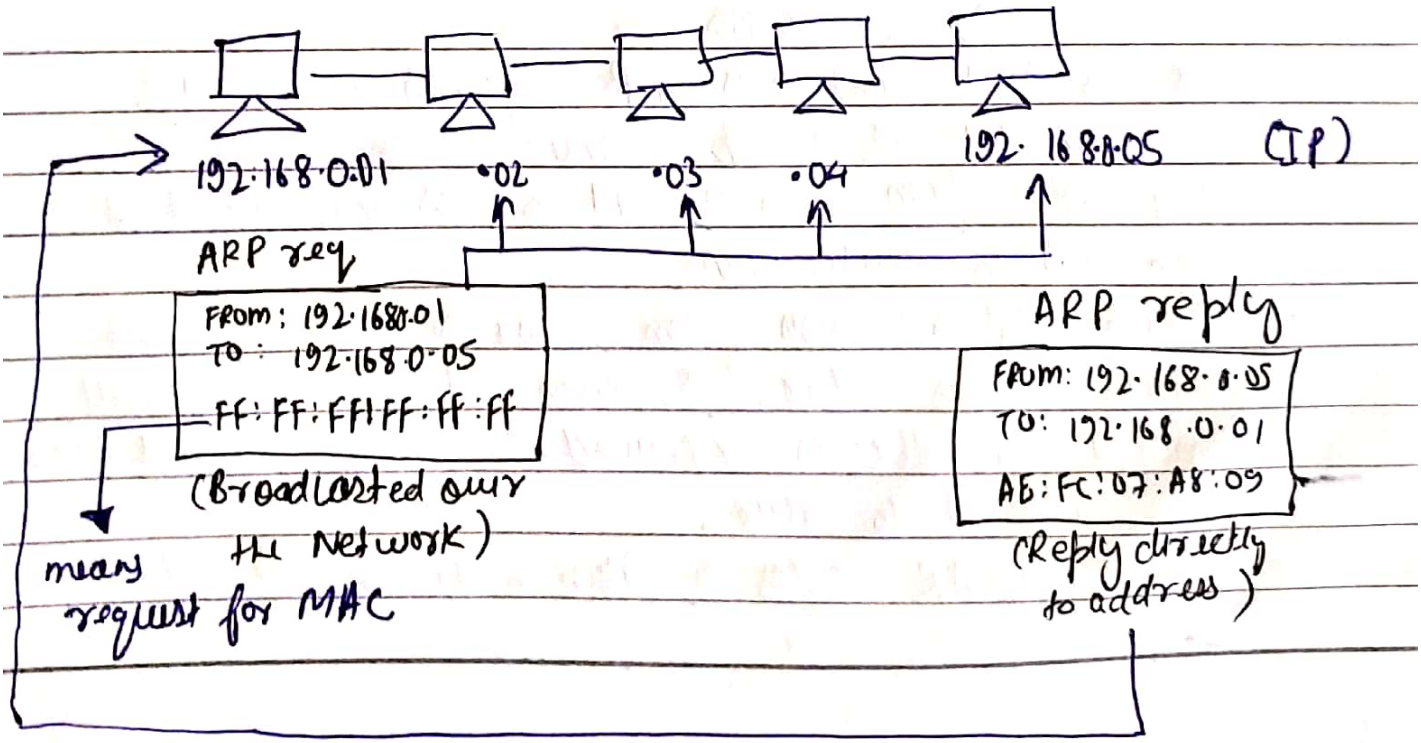
(i) Describe how MITM attack may be performed on a WI-FI N/w and the consequences of such an attack.

(ii) Explain how a MITM attack on WIFI can be defeated.

Soln 3

(i) Man in the middle attack can be performed over WIFI N/w using ARP spoofing.

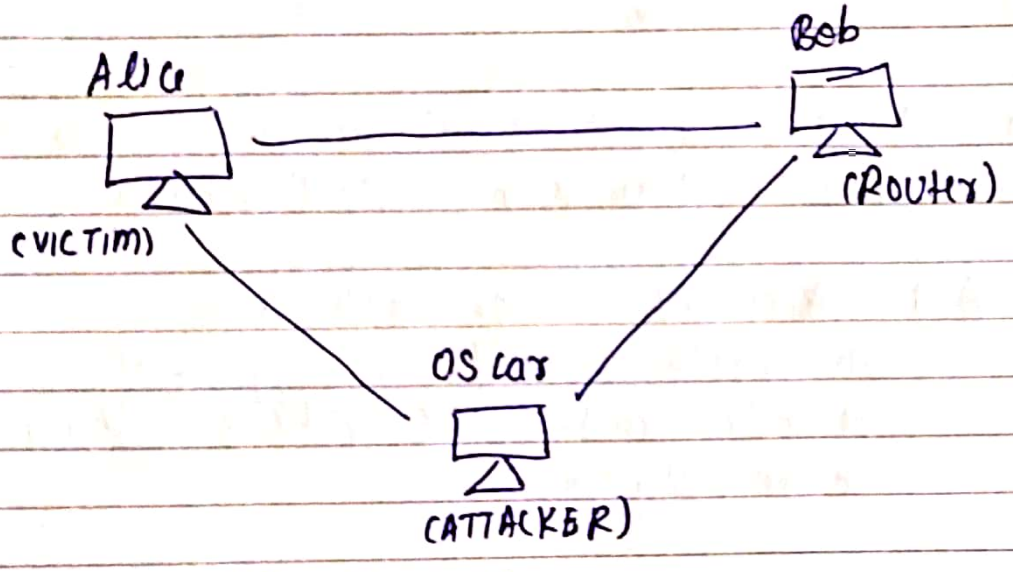
ARP: Address Resolution protocol.
This protocol helps in mapping of IP addr. with MAC address of devices in the network.



So ARP protocol is based on Request and Response b/w a computer and a router in the Network.

Due to broadcast of ARP request a computer can receive response from any other system in network.

The Flaw is used in MITM attack over Wi-Fi N/w.



ARP SPOOFING.

- Alice is sent continous ARP responses by OSCAR claiming that it is bob. Hence due to which all ARP req from Alice is sent to OSCAR. which is then sent to Router (bob).
- Again ARP response from oscar to bob is sent claim it as Alice. So, Now all ARP responses meant for Alice is received to OSCAR., which then forwards it to Alice.
- Hence OSCAR does a Man-in-the-middle attack.

consiquences of MITM attack:

- As intruder dewc b/w VICTIM and ROUTER OSCAR can listen to all packets received.
- It can contain login credential over HTTP.
- Attacker can also modify packets received.

(ii) To prevent ARP spoofing

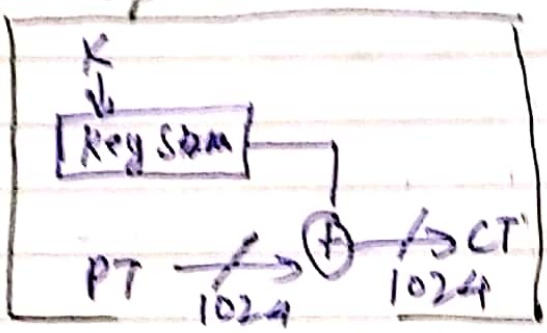
a) Static ARP
If two system communicate regularly, a static ARP entry in cache will help avoiding spoofing by OSCAR.

b) Use strong encryption.
A will encrypted and authentication process over network will reduce chances of spoofing

c) Use packet filtering.
Oscar generates multiple ARP response ~~which~~ with victim IP address.
So using packet filtering to discard such malicious packets & filtering can ensure a safe environment in the network.

Q4. Consider a PT of size 1024 bit, has a probability of 0.7 for producing a '0' and LFSR sequence has exactly 60% 0's. Find the approximate number of 0's in the resulting cipher.

Soln



		XOR
0	0	0
0	1	1
1	0	1
1	1	0

CT is XOR opn" b/w Keystream and Plain-text
So, to get '0' in cipher text,
either PT and Keystream are both 0
or PT and Keystream are both 1.

Probability (PT & Keystream = 0) = 0.7 * 0.6
= 0.42

Probability (PT & Keystream = 1) = 0.3 * 0.4
= 0.12

∴ Total Probability of CT having 0's = 0.54

∴ ~~Expect~~ Approx #0's in CT = 0.54 * 1024
= 552.96

≈ 553 0's in CT.

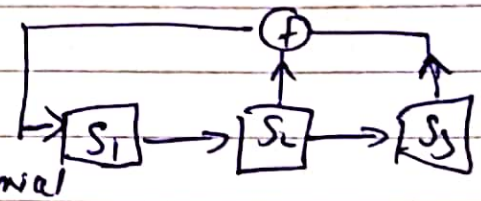
Q5. Show that any m-sequence is G-random?

- A LFSR generates m-sequence iff, it visits all possible non-zero state in one cycle.

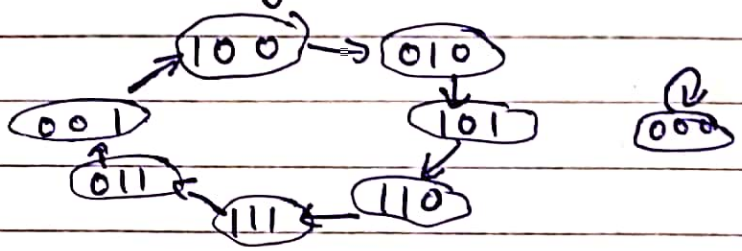
  i.e the period of sequence is $2^r - 1$ for r flip flop in the LFSR!

- A polynomial generates m-sequence iff it is a primitive polynomial.

eg. $g(x) = 1 + x^2 + x^3$
↳ Primitive polynomial



State diagram



R1. $|\#0's - \#1's| \leq 1$

Since period is $2^r - 1$ only state with all zero's is not included

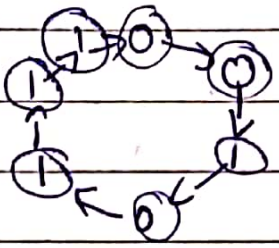
$\therefore \#1 = 2^{r-1}$

$\#0 = 2^{r-1} - 1$ (except all zeros)

$\therefore$ R_1 is satisfied.

R_2: For any m-sequence, there are 2^{n-1} runs

relative freq for runs of length l is $\begin{cases} \frac{1}{2^l} & l < n \\ \frac{1}{2^{l-1}}, & l = n \end{cases}$

eg. 

0 0 1 0 1 1 1

runs = 4

3 length = 1

2 length = 1

1 length = 2.

∴ R_2 is satisfied

R_3: Autocorelation function (τ)

$C(0) = 1$. ∴ in-phase autocorrelation is 1

S_t = 0 0 1 0 1 1 1

S_{t+1} = 1 0 0 1 0 1 1 $\quad C(1) = \frac{3-4}{7} = -\frac{1}{7}$

S_{t+2} = 1 1 0 0 1 0 1 $\quad C(2) = \frac{3-4}{7} = -\frac{1}{7}$

∴ $C(\tau) \quad 1 \le \tau < P$ is constant

∴ R_3 is also satisfied

Hence m-sequence is G-random as it satisfies all 3 Golomb's postulates.

Q6. Prove that out-of-phase autocorrelation function of an m-sequence with period 2^n-1 is $\frac{-1}{2^n-1}$.

We know that m-sequence follows Golomb's postulate.

for n stab LFSR

Period of m-sequence $= 2^n-1$

also # Runs $= 2^{n-1}$

length 1 =	$1/2$
length 2 =	$1/4$
⋮	⋮
length ℓ	$1/2^\ell$

For every shift :- length 1 get disaggrement
one of length 2 get disaggrement
one of length 3 get disaggrement
⋮

Similarly for next shift: all length 1 get aggrement

So: Total we get $= 2^{n-1}-1$ aggrement for each (τ)
and 2^{n-1} disaggrement for each (τ)

$\therefore C(\tau) = \frac{A-D}{P} = \frac{2^{n-1}-1-(2^n-1)}{2^{n-1}}$

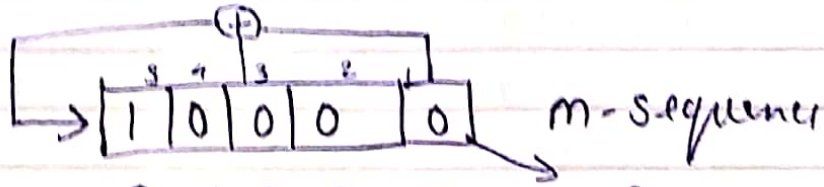
$= \frac{-1}{2^n-1}$.

Q.7 Suppose we wish to construct an m-sequence of length 31. Using polynomial $(45)_8$. Write the resulting m-sequence by LFSR with initial sequence (1, 0, 0, 0, 0)

Soln $31 \leq 2^5 - 1$ (satisfied) (Period bound by LFSR)

$(45)_8 = 100101 = (37)_{10}$

$P(x) = 1 + x + x^3 + x^5$



0 1 0 0 0	0
0 0 1 0 0	0
1 0 0 1 0	0
0 1 0 0 1	0
1 0 1 0 0	1
1 1 0 1 0	0
0 1 1 0 1	0
0 0 1 1 0	1
1 0 0 1 1	0
1 1 0 0 1	1
1 1 1 0 0	1
1 1 1 1 0	0
1 1 1 1 1	0
0 1 1 1 1	1
0 0 1 1 1	1
0 0 0 1 1	1
1 0 0 0 1	1
1 1 0 0 0	1
0 1 1 0 0	0

1	0	1	1	0	0
1	1	0	1	1	0
1	1	1	0	1	1
0	1	1	1	0	1
1	0	1	1	1	0
0	1	0	1	1	1
1	0	1	0	1	1
0	1	0	1	0	1
0	0	1	0	1	0
0	0	0	1	0	1
0	0	0	0	1	0
Repeated ⟹ 1	0	0	0	0	1

∴ The Generated 31 length m-sequence is

0 0000 1 00 1 0 11 00 11111 000
11 0 111 0 1 0 1.

Q3. Let S be a periodic binary sequence with period p. Let K be the number of entries 1 in one period of S and μ is the number of pairs $(S_i, S_{i+\tau}) = (1,1)$ for a fixed $\tau < p$, $0 \le i \le p$. Then prove that the autocorrelation coefficients $C(\tau)$ is:

$$C(\tau) = 1 - \frac{4(K-\mu)}{p}$$

Given: For a sequence S,

$(S_i, S_{i+\tau}) \rightarrow (1,1) = \mu$

Period = p

Autocorrelation $C(\tau) = \frac{A-D}{p}$

A: #Aggrement ie (0,0) || (1,1)
D: #Disagrement ie (0,1) || (1,0)

'K' :- No of 1's in 'S'

So # (0,1) = (K−μ) } as both S_i & $S_{i+\tau}$ will have K 1's as $S_{i+\tau}$ is just shifted seq of S_i
(1,0) = (K−μ)

we know that

$p = \#(0,0) + \#(1,1) + \#(0,1) + \#(1,0)$
$p = \#(0,0) + \mu + 2(K-\mu)$
$\#(0,0) = p + \mu - 2K$

$$\therefore \quad C(C) = \frac{A - D}{P}$$

$$= \frac{\left(\mu + [p + \mu - 2k]\right) - \left(2(k - \mu)\right)}{P}$$

$$= \frac{P - 4(k - \mu)}{P}$$

$$= 1 - \frac{4(k - \mu)}{P}$$

Hence Proved.

Q9.: An affine block cipher .... $C = Am + t$
.... C, A and m all over GF(2).
Find the number of affine block ciphers

Soln

$C, A, m \in GF(2)$

$GF(2) = \{0, 1\}$

$A = \begin{bmatrix} & \\ & \end{bmatrix}_{3\times3}$ Total A's possible 2^9

But for Decryption we need

$m = A^{-1}(C - t)$

so, A must be non-singular.

#Total Affine cipher: # Distinct non-singular A * # Distinct t

Distinct non-singular A =

(i) R_1 = $(2^3 - 1)$ except (0,0,0)

(ii) R_2 = $(2^3 - 1) - 1$ except (0,0,0) and R_1

(iii) R_3 = $(2^3 - 1) - 2 - 1$

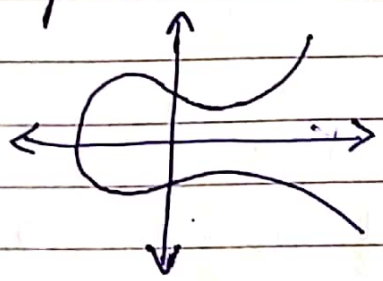
(0,0,0) | R_1, R_2 | any linear combination of R_1 and R_2

Affine cipher: $(7 * 6 * 4) * (2^3)$
$= 1344$

Q 10) Each of the following points has finite order on the given elliptic curve over Q. In each case find order of P.

a) ~~P = (0, 16)~~

General elliptic curve $y^2 = x^3 + ax + b \bmod p$



Order = n P = $\mathcal{O}$ (Identity)
↓
smallest (+ve) integer.

a) $P = (0, 16)$ on $y^2 = x^3 + 256$

$a = 0$

(Point doubling) $P + P = 2P$

slope $m = \frac{3x_1^2 + a}{2y_1}$

$m = 0$

$x_3 = m^2 - x_1 - x_2 = 0$

$y_3 = m(x_1 - x_3) - y_1 = -16$

$2P = (0, -16)$

$2P = -P$ (inverse)

$3P = 2P + P$

$(-P) + (P) = \mathcal{O}$ (Identity)

∴ order of $P = 3$.

b) $P = (\frac{1}{2}, \frac{1}{2})$ on $y^2 = x^3 + (\frac{1}{4})x$

$$a = \frac{1}{4}$$

$$m = \frac{3 \cdot \frac{1}{4} + \frac{1}{4}}{2 \times \frac{1}{2}} = \frac{1}{1} = 1.$$

$$a_3 = 1 - \frac{1}{2} - \frac{1}{2} = 0$$

$$y_3 = 1\left(\frac{1}{2} - 0\right) - \frac{1}{2} = 0$$

$$2P = (0, 0)$$

$4P = 2P + 2P$ ~~$m = \frac{3 \cdot 0 + \frac{1}{4}}{0}$~~

since $P \neq -P$

$\therefore$ order $\neq 2$

$\therefore 4P = 2P + 2P =$

$= 2(2P)$

$= 0$

So, order is 4.

(c) $P = (3, 8)$ on $y^2 = x^3 - 43x + 166$

$a = -43$

$m = \frac{3 * 9 - 43}{2 \times 8} = -1$

$2P = P + P$

$x_3 = 1 - 3 - 3 = -5$

$y_3 = -1(3 + 5) - 8 = -16$

$2P = (-5, -16)$

$4P = 2P + 2P$

$m = \frac{3 * 25 - 43}{2 * (-16)} = -1$

$x_3 = 1 + 5 + 5 = 11$

$y_3 = 16 - 1(-5 - 11) = 32$

$4P = (11, 32)$

$8P = 4P + 4P$

$m = \frac{3 * 121 - 43}{2 * (32)} = 5$

$x_3 = 25 - 11 - 11 = 3$

$y_3 = 5(11 - 3) - 32 = 8$

$\therefore 8P = (3, 8)$

Hence $8P = P$

$\therefore 7P + P = 8P$

$\therefore 7P = O$

Hence order = 7

(1) $P = (0,0)$ on $y^2 + y = x^3 - x^2$

Idea: make eqn in form $y^2 = x^3 + ax + b$

$y \to y - 1/2$
$x \to x + 1/3$ } replace

$$\left(y - \frac{1}{2}\right)^2 + \left(y - \frac{1}{2}\right) = \left(x + \frac{1}{3}\right)^3 - \left(x + \frac{1}{3}\right)^2$$

$$y^2 - \frac{1}{4} = x^3 + \frac{1}{27} - \frac{1}{9} - \frac{2}{3}x$$

$$\Rightarrow \boxed{y^2 = x^3 - \frac{1}{3} + \frac{19}{108}} \text{ - standard form}$$

$$a = -\frac{1}{3}$$

$P(0,0) \xrightarrow[\text{transformed do}]{\text{to}} \left(-\frac{1}{3}, \frac{1}{2}\right)$

$2P = P + P$

$$m = \frac{\left(3 * \frac{1}{9} - \frac{1}{3}\right)}{2 * \frac{1}{2}} = 0$$

$x_3 = \frac{1}{3} + \frac{1}{3} = 2/3$, $y_3 = -\frac{1}{2}$

$2P = \left(\frac{2}{3}, -\frac{1}{2}\right)$

$4P = 2P + 2P$

$$m = \frac{3 * \left(\frac{4}{9}\right) - \frac{1}{3}}{-2 * \frac{1}{2}} = -1$$

$x_3 = 1 - 2/3 - 2/3 = -1/3$

$y_3 = \frac{1}{2} - 1\left(\frac{2}{3} + \frac{1}{3}\right) = -\frac{1}{2}$

$\therefore 4P = \left(-\frac{1}{3}, -\frac{1}{2}\right)$

$\therefore 4P = -P$

$\therefore 5P = P + 4P$

$= P + (-P)$

$= 0$

$\therefore$ Order $= 5$

Q11. Consider elliptic curve over F_{2^4} (field of characteristic 2) is

$E: y^2 + xy = x^3 + g^4x^2 + 1$

where $g = (0010)$ is generator of F_{2^4}.

F_{2^4} is constructed using primitive polynomial $f(x) = x^4 + x + 1$. List all elements in $E(@F_{2^4})$

Elliptic curve over F_{2^4} = $GF(2^4)$

~~∴ This cyclic group contain~~

The finite field $GF(2^4)$ contains 16 element in the set

∴ $g = (0010)$ is the generator

Primitive polynomial = $x^4 + x + 1$

'g' generator can be expressed as

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

$g^0 = 0001$

$(g^1) = 0010$

$g^2 = 0100$

$g^3 = (1000)$

$g^4 = 0011$

$g^4 = g * g^3 = x * x^3 = x^4 \bmod f(x)$

$x^4 + x + 1 \;|\; x^4$

$x^4 + x + 1$

$x + 1 = 0011$

$g^5 = g^4 \cdot g = (x+1)\cdot(x) = x^2 + x \bmod x^4+x+1$

$g^5 = 0110$

Similarly

$g^6 = 1100$ $\quad g^9 = 1010$ $\quad g^{12} = 1111$ $\quad g^{15} = 0001$

$g^7 = 1011$ $\quad g^{10} = 0111$ $\quad g^{13} = 1101$

$g^8 = 0101$ $\quad g^{11} = 1110$ $\quad g^{14} = 1001$

Now B: $y^2 + xy = x^3 + g^4x^2 + 1$

point (g^5, g^3) satisfies the eqn

$= (g^3)^2 + g^8 = g^{15} + g^{14} + 1$

$= 1100 + 0101 = 0001 + 1001 + 0001$

$1001 = 1001$

Using (g^5, g^3) we get other points that satisfy the eqn:

$(1, g^{13})$, (g^3, g^{13}), (g^5, g^{11}), (g^6, g^{14}), (g^7, g^{13}), (g^{10}, g^{11}),

(g^{12}, g^{14}), $(1, g^6)$, (g^3, g^8), (g^5, g^7), (g^6, g^9), (g^7, g^{10}), (g^{10}, g),

$(g^{12}, 0)$, $(0, 1)$