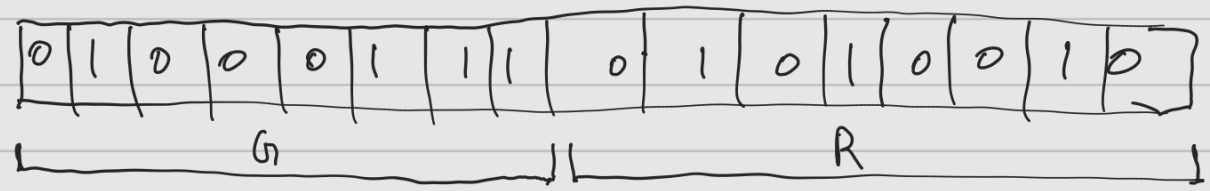
09/01/22.

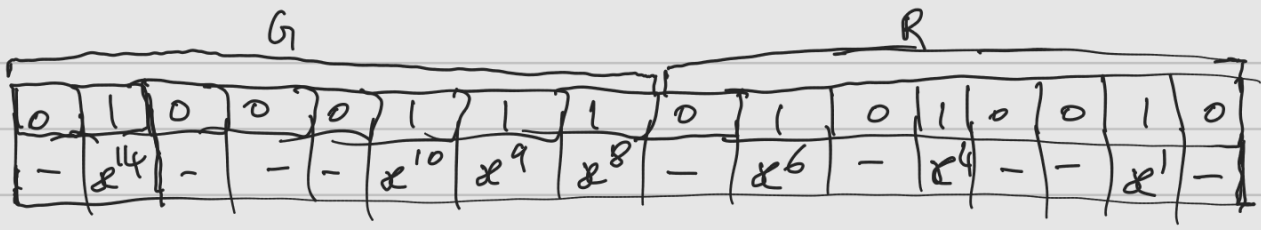
HOME WORK-2.

1.

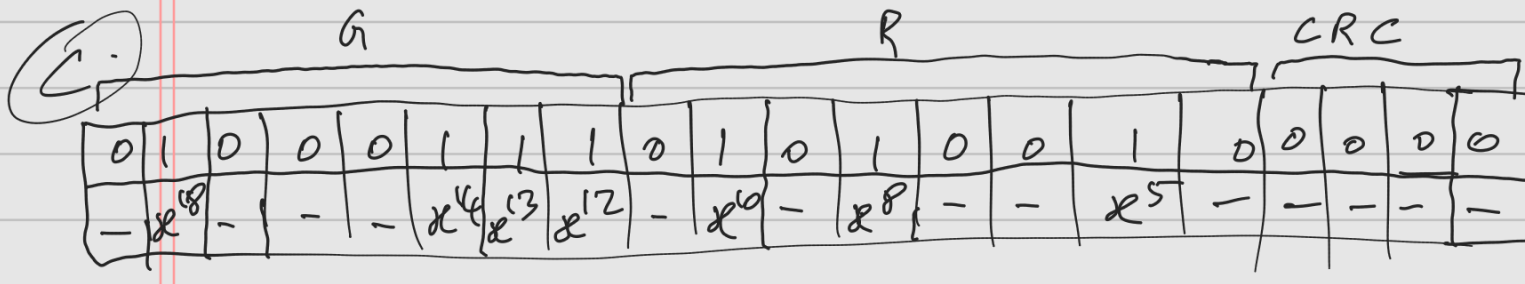
(a) My Initials are GR.

(b)





(c)



∴ The Message Polynomial is,

$x^{18} + x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^5$.

(d) Polynomial is, 0x13.
Polynomial in binary is, 1 0 0 1 1.

Polynomial in Exponential is, $x^4 - x^1 x^0$.

∴ The Polynomial in Exponential is,

$x^4 + x + 1$.

(c) $x^4+x+1 \;\overline{)\; x^{18}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^5}$

(x^{14}) $x^{18}+x^{15}+x^{14}$

$x^{15}+x^{13}+x^{12}+x^{10}+x^8+x^5$

(x^{11}) $x^{15}+x^{12}+x^{11}$

$x^{13}+x^{11}+x^{10}+x^8+x^5$

(x^9) $x^{13}+x^{10}+x^9$

$x^{11}+x^9+x^8+x^5$

(x^7) $x^{11}+x^8+x^7$

$x^9+x^7+x^5$

(x^5) $x^9+x^6+x^5$

x^7+x^6

(x^3) $x^7+x^4+x^3$

$x^6+x^4+x^3$

(x^2) $x^6+x^3+x^2$

x^4+x^2

(x^0) x^4+x+1

$x^2+x+1 \rightarrow$ Remainder.

$0\ 1\ 1\ 1 \rightarrow CRC$

6.

G								R								CRC				
0	1	0	0	0	1	1	1	0	1	0	1	0	0	1	0	0	1	1	1
–	x^{18}	–	–	–	x^{14}	x^{13}	x^{12}	–	x^{10}	–	x^8	–	–	x^5	–	–	x^2	x^1	x^0

∴ The Full binary message we will send including CRC is, $x^{18}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^5+x^2+x^1+x^0$

verification:-

x^4+x+1) $x^{18}+x^{14}+x^{13}+x^{12}+x^{10}+x^8+x^5+x^2+x^1+x^0$

(x^{14}) $x^{18}+x^{15}+x^{14}$

$x^{15}+x^{13}+x^{12}+x^{10}+x^8+x^5+x^2+x^1+x^0$

(x^{11}) $x^{15}+x^{12}+x^{11}$

$x^{13}+x^{11}+x^{10}+x^8+x^5+x^2+x^1+x^0$

(x^9) $x^{13}+x^{10}+x^9$

$x^{11}+x^9+x^8+x^5+x^2+x^1+x^0$

(x^7) $x^{11}+x^8+x^7$

$x^9+x^7+x^5+x^2+x^1+x^0$

(x^5) $x^9+x^6+x^5$

$x^7+x^6+x^2+x^1+x^0$

(x^3) $x^7+x^4+x^3$

$x^6+x^4+x^3+x^2+x^1+x^0$

(x^2) $x^6+x^3+x^2$

x^4+x+1

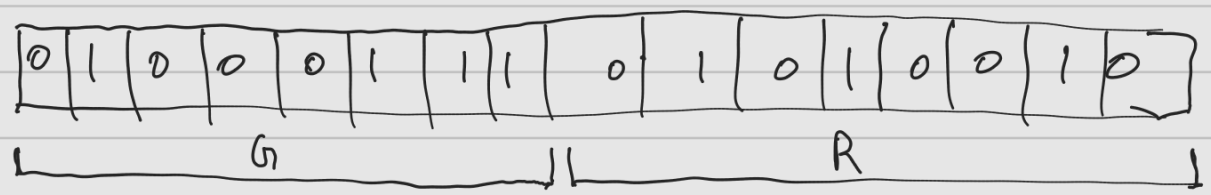
(x^0) x^4+x+1

$0 \rightarrow$ Remainder (Hence verified)

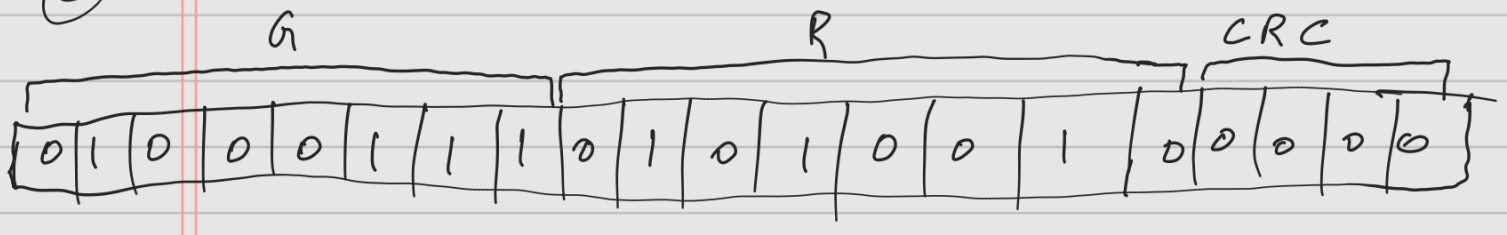
2.

(a) My Initials are GR.

(b)



(c)



Polynomial is, 0x13;
Polynomial in binary is, 1 0 0 1 1.

(d)

1 0 0 1 1 | 0 1 0 0 0 1 1 1 0 1 0 1 0 0 0 0 0

Left shift until First Bit is 1;

1 0 0 1 1 | 1 0 0 0 1 1 1 0 1 0 1 0 0 0 0 0

Now, XOR the Binary Bits with Polynomial Binary with 0's after.

1 0 0 1 1 | 1 0 0 0 1 1 1 0 1 0 1 0 0 0 0 0

⊕ 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0

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

Continue the Process;

1 0 0 1 1 | 1 0 1 1 0 1 0 1 0 0 0 0 0

⊕ 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0

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

1 0 0 1 1 | 1 0 1 1 0 1 0 0 0 0 0

⊕ 1 0 0 1 1 0 0 0 0 0 0 0 0 0

0 0 1 0 1 1 0 0 0 0 0

10011 | 1011 0000
⊕ 1001 1000 0000
0010 1000 0000

10011 | 1010 1000 0000
⊕ 1001 1 0000 0000
0011 1000 0000

10011 | 1100 0000
⊕ 1001 1 000
0100 1 000

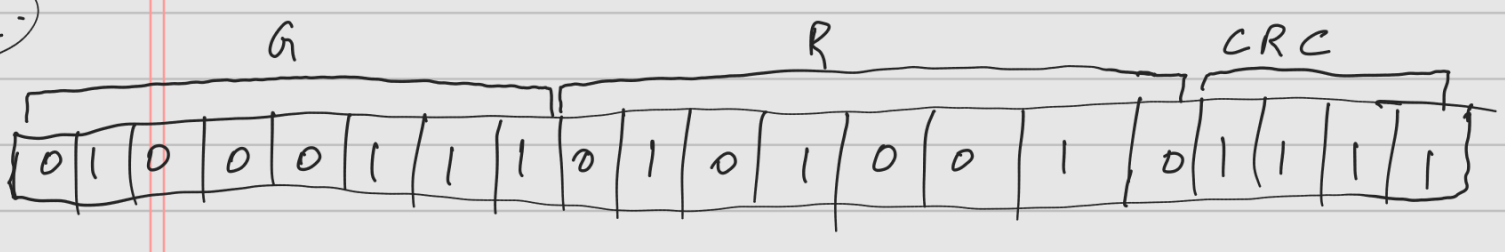
10011 | 1011 000
⊕ 1001 1 00
0010 1 00

1001 | 101 0 0
⊕ 1001 1 1
0011 1 1

1001 | 111 00
⊕ 1001 1
0111 1

1001 | 1111 → 4-bit C.R.C

(2.)



09/07/22:

(3.) 0 & $(2^m - 1)$

When, $m = 1 \Rightarrow (2^1 - 1) = 1$. → First collision

when, $m = 2 \Rightarrow (2^2 - 1) = 3$. → Second collision

when, $m = 3 \Rightarrow (2^3 - 1) = 7$. → Third collision.

∴ we have to choose a Random number between 0 & 7.

(4.) For 1st Attempt:-

0 and $(2^n - 1)$
0, 1

(0,0) ; (0,1) ; (1,0); (1,1) $\Rightarrow \frac{1}{4} = 0.25$ Probability

0 and $(2^n - 1)$
0, 3

For 2nd Attempt:-

(0,0); (0,1); (0,2); (0,3); (1,0); (1,1); (1,2); (1,3)

$\Rightarrow \frac{5}{8} = 0.625$ Probability.

For 3rd Attempt:-

0 and $(2^n - 1)$
0, $(2^3 - 1)$
0, 7

(0,0); (0,1); (0,2); (0,3); (0,4); (0,5); (0,6); (0,7);
(1,0); (1,1); (1,2); (1,3); (1,4); (1,5); (1,6); (1,7);

$\frac{13}{16} = 0.8125$ Probability.

5. → I can detect and prove if they are cheating the system, by implementing certain wait times between retries and the number of retries, as it depends upon our use call and network condition.

6. NO, we cannot assume that the device wanting to send the data to the base station is disconnected because, the device is connected to the network with multiple connections and may occour network discrepancies.

→ I can send the message now as I have the clear to send (CTS) request because we don't have to wait for a Request to send (RTS) to send the data and hence we can send it right away.

7. The DST MAC address is set as 'i2'. It tells the switch to broadcast the IP address with MAC addresses destination so that the ARP Responds with the intended IP provides the MAC address.

8. When we connect to an unsecured (open) wi-Fi, we should be careful not to send any important (or) personal details through the network if it is not encrypted, that means the data can be seen (or) accessed by anyone, hence we get a warning before connecting to this network.

As we connect to a secure Wi-Fi network, it encrypts the transmissions and hence it is secure and no can interpret the transmissions, and hence we dont get the warning.

(9.) There are multiple ways to prevent ARP poisoning, by using Encryption; VPN's.

Encryption:- when the traffic is Encrypted, the attacker would have to go to the additional step of tricking the targets browser into accepting an illegitimate certificate.

VPN's:- VPN can be a reasonable defense for individuals, but they are generally not suitable for larger organisations.

(10.) There are multiple scenarios where a switch would have to drop the frames.

1st Scenario:- when the switch reaches its maximum buffer load, then it has to drop the frames, because it can't handle more than that of the buffer.

2nd Scenario:- If both the source and the destination of the MAC address is found in the same port, then the switch will need to drop the frame.

Because a switch will never send a frame back out the same port it came in on.

→ The best way to measure a frame loss is using "ping". to send a large number of pings to the destination and look for failed responses.