1. Let k=5. Assume a cache with initial contents 1,2,3,4,5 and with at least one item not in the cache. Give an example sequence of length at least 6 of cache requests and a sequence of random choices by the Marker algorithm so that its competitiveness on this sequence with these choices would be greater than H5.

Q1 K = 5

cache has initial contents $\boxed{1 \mid 2 \mid 3 \mid 4 \mid 5}$

let there K+1 length = 6.

let the request sequence be.

2, 3, 2, 5, 6, 4, 1, 4, 6, 3, 2, 5, 1

Marker Algorithm

	2	3	2	5	6	4			1	4	6	3	2			5	1
0	0	0	0	0	1	1	R	0	1	1	1	1	1	R	0	1	1
0	1	1	1	1	1	1	E	0	0	0	1	1	1	E	0	0	1
0	0	1	1	1	1	1	S	0	0	0	0	1	1	S	0	0	0
0	0	0	0	0	0	1	E	0	0	1	1	1	1	E	0	0	0
0	0	0	0	1	1	1	T	0	0	0	0	0	1	T	0	0	0

initial cache						
1	6	1	1	1	5	5
2	2	2	6	6	6	1
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	2	2	2

- evict the lowest indexed cache
- when all the cache pages are marked it resets all to unmarked
- There are 6 cache misses

MIN algorithm

cache $\boxed{1\ 2\ 3\ 4\ 5}$

✓ → no cache miss

X → cache miss, evict the item farthest in future

2	3	2	5	6	4	1	4	6	3	2	5	1
✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓	X	✓

1	1
2	5
3	3
4	4
6	6
evict 5	evict 2

- number of misses is 2

The length of the request sequence $N = 13$

MIN can have $\frac{N}{K}$ misses in the worst case

$\frac{N}{K} = \frac{13}{5} = 2.6$

For our request sequence MIN faults 2 times.

For the same request sequence Marker Algorithm faults 6 times

- We call an item stale if it is unmarked, but was marked in the previous round and clean if its neither marked nor is it stale.
- Let m be the number of requests to clean items in a round.

$C_{H_5} = 2$ [MIN] $C_{MA} = 6$. [Marker Algorithm]

$\therefore$ competitivesness of Marker Algorithm is greater than H_5.

$C_{H_5} < C_{MA}$

or $\boxed{C_{MA} > C_{H_5}}$

2. Use the extended Euclidean algorithm to find the multiplicative inverse of 26mod1155. Solve 9x≡6mod33 for all solutions.

```
Extended-Euclid(a,b)
if b = 0 then return (a, 1, 0)
(d', x', y') = Extended-Euclid(b, a mod b)
(d, x, y) = (d', y', x' - floor(a/b)*y')
return (d, x, y)
```

Q2

Part 1

EE (26, 1155)

$(d, x', y') = EE(1155, 26)$

$(d, x', y') = EE(26, 11)$

$(d, x', y') = EE(11, 4)$

$(d, x', y') = EE(4, 3)$

$(d, x', y') = EE(3, 1)$

$(d, x', y') = EE(1, 0)$

$(d, x, y) = (1, 1, 0)$

$(d, x, y) = (1, 0, 1)$

$(d, x, y) = (1, 1, -1)$

$(d, x, y) = (1, -1, 3)$

$(d, x, y) = (1, 3, -7)$

$(d, x, y) = (1, -7, 311)$

$(d, x, y) = (1, 311, -7)$

$EE(26, 1155) = (1, 311, -7)$

where $d = 1$ $x = 311$ $y = -7$.

$26 \times 311 - 1155 \times 7$

$8086 - 8085 = 1$ $[\because ax + by = d]$

$\boxed{ax = 1 \bmod b}$

Here x is the multiplicative inverse of 26 mod 1155

$\boxed{x = 311}$ is multiplicative inverse of 26 mod 1155

Part 2

Solve $9x \equiv 6 \mod 33$

$ax = b \mod n$

$EE(9, 33)$

$(d, x', y') = EE(33, 9)$

$(d, x', y') = E(9, 6)$

$(d, x', y') = EE(6, 3)$

$(d, x', y') = EE(3, 0)$

$(d, x, y) = (3, 1, 0)$

$(d, x, y) = (3, 0, 1)$

$(d, x, y) = (3, 1, -1)$

$(d, x, y) = (3, -1, 4)$

$(d, x, y) = (3, 4, -1)$

Now executing Modular-Linear-Equation-Solver (a, b, n)

for $9x \equiv 6 \mod 33$

$a = 9 \quad b = 6 \quad n = 33$

$x_0 = x(b/d) \mod n$

$= 4(6/3) \mod 33$

$\boxed{x_0 = 8}$

Now executing the for loop $i = 0$ to $d-1$

$i = 0$ to 2

on $x_i = x_0 + i * (b/d) \mod n$

$i = 0 \quad x_0 = 8$

$i = 1 \quad x_1 = (8 + 1 * 33/3) \mod 33 = (8 + 11) \mod 33$

$x_1 = 19$

$i = 2 \quad x_2 = (8 + 2 * \frac{33}{3}) \mod 33 = (8 + 22) \mod 33$

$x_2 = 30$

So the solutions are $\underline{8, 19, 30}$

3. Using the Chinese Remainder theorem, determine a number xmod1155 that satisfies x≡2mod3, x≡3mod5, and x≡4mod7, and x≡5mod11.

Q3

x mod 1155 that satisfies

$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 5$
$x \equiv 4 \bmod 7$
$x \equiv 5 \bmod 11$

Calculate m_i

$m_1 = \frac{1155}{3} = 385$

$m_2 = \frac{1155}{5} = 231$

$m_3 = \frac{1155}{7} = 165$

$m_4 = \frac{1155}{11} = 105$

Calculate t_i

$t_i = (m_i)^{-1} \bmod n_i$

For $i = 1$

EE (385, 3)

$(d, x', y') = EE(3, 1)$

$(d, x', y') = EE(1, 0)$

$(d, x, y) = (1, 1, 0)$

$(d, x, y) = (1, 0 1)$

$(d, x, y) = (1, 1, -128)$

This tells us $385 \times 1 - 3 \times 128 = 1$

$\equiv 385 \times 1 = 1 \bmod 3$

$t_1 = 1 \bmod 3$

For t_i when $i = 2$

$EE(231, 5) = (1, 1, -46)$

$d = 1$, $x = 1$, $y = -46$

which gives us $231 \times 1 - 5 \times 46 = 1$

$\equiv 231 \times 1 = 1 \bmod 5$

$t_2 = 1 \bmod 5$

when $i = 3$

$EE(165, 7) = (1, 2, -47)$

$d = 1$ $x = 2$ $y = -47$

which gives us $165 \times 2 - 7 \times 47 = 1$

$\equiv 165 \times 2 = 2 \bmod 7$

$t_3 = 2 \bmod 7$

when $i = 4$

$EE(105, 11) = (1, 2, -19)$

we get $105 \times 2 - 11 \times 19 = 1$

$\equiv 105 \times 2 = 2 \bmod 11$

$t_4 = 2 \bmod 11$

Calculate c_i

$c_1 = m_1 t_1$
$= 385 \times 1$
$= 385$

$c_2 = m_2 t_2$
$= 231 \times 1$
$= 231$

$c_3 = m_3 t_3$
$= 165 \times 2$
$= 330$

$c_4 = m_4 t_4$
$= 105 \times 2$
$= 210$

$x = a_1 c_1 + a_2 c_2 + a_3 c_3 + a_4 c_4$
$= (2 * 385) + (3 * 231) + (4 * 330) + (5 * 210)$
$= 770 + 693 + 1320 + 1050$
$= 3833$

Now substituting x in $x \bmod 1155$

we get $\boxed{3833 \bmod 1155 = 365}$

$x \bmod 3 = 368 \bmod 3 \equiv 2 \bmod 3$

$x \bmod 5 = 368 \bmod 5 \equiv 3 \bmod 5$

$x \bmod 7 = 368 \bmod 7 \equiv 4 \bmod 7$

$x \bmod 11 = 368 \bmod 11 \equiv 5 \bmod 11$

4. Suppose p=7, q=17. If we choose e=3, what would be a the RSA public and private keys? Show the result of encrypting with the private key, the message 89. Show the steps in decrypting it, to get the original number back.

1. *Select two large prime numbers p and q such that $p \neq q$. (For instance, the primes might be 512 bits each.)*
2. *Compute $n = pq$.*
3. *Select a small odd integer e that is relatively prime to $\varphi(n) = (p-1)(q-1)$.*
4. *Compute the multiplicative inverse d of $e \bmod \varphi(n)$.*
5. *Publish the pair $P = (e, n)$ as the RSA public key.*
6. *Keep secret the pair $S = (d, n)$ as the RSA secret key.*

Q4

Step 1: p and q are both primes and $p \neq q$

Step 2: $n = p * q$
$= 7*17 = 119$

Step 3: $\phi(n) = (p-1)(q-1) = 6*16 = 96$, we have $e = 5$
$\therefore$ $\phi(n)$, e are relatively prime.
$\gcd(5, 96) = 1$

Step 4 compute multiplicative inverse d of $e \bmod \phi(n)$

when $\gcd(a, n) = 1$ (Special case) we have $b = 1$.

$\therefore$ $ax \equiv b \pmod n$ $[a = 5,\ b = 1,\ n = 96]$

we have.

$5x \equiv 1 \bmod 96 \longrightarrow$ (eq 1)

We solve the above using Modular Linear equation Solver

MLES (a, b, n)

EE (a, n)

EE (5, 96)

$(d, x', y') = EE(96, 5)$

$(d, x', y') = EE(5, 1)$

$(d, x', y') = EE(1, 0)$

$(d, x, y) = (1, 1, 0)$

$(d, x, y) = (1, 0, 1)$

$(d, x, y) = (1, 1, -19)$

$(d, x, y) = (1, -19, 1)$

$x_0 = (x(b/d)) \bmod n$
$= -19 \bmod 96$
$= 77$

$\therefore$ $\boxed{d = 77}$.

Step 5: public key $P = (e, n) = (5, 119)$

Step 6: Secret key $S = (d, n) = (77, 119)$

Encryption of Message M=89 with private key

To apply a key to a message $0 \leq M < n$, we compute either $P(M) = M^e \bmod n$ or $S(C) = C^d \bmod n$

For our encryption we use $P(M) = M^e \bmod n$

Here $M = 89$ $e = 5$ $n = 119$

substituting the values to the above equation

$$P(M) = 89^5 \bmod 119$$
$$= 5584059449 \bmod 119$$
$$= 38$$

Decryption steps to get M=89

we solve this using Exp-Mod(a, x, n) algorithm..

$$38^{77} \bmod 119$$

R1 : Exp-Mod (38, 77, 119)

C = (Exp-Mod (38, 38, 119))^2 mod 119

R2 : Exp-Mod (38, 38, 119)

C = (Exp-Mod (38, 19, 119))^2 mod 119

R3: Exp-Mod (38, 19, 119)

C = (Exp-Mod (38, 9, 119))^2 mod 119

R4: Exp-Mod (38, 9, 119)

C = (Exp-Mod (38, 4, 119))^2 mod 119

R5: Exp-Mod (38, 4, 119)

C = (Exp-Mod (38, 2, 119))^2 mod 119

R6 : Exp-Mod (38, 2, 119)

$c = (\text{Exp-Mod}(38, 1, 119))^\wedge 2 \mod 119$

R7 : Exp-Mod (38, 1, 119)

$x = 1$ so return $38 \mod 119. = 38$

Recursing back to R1

R6 : $C = 38^\wedge 2 \mod 119 = 16$

x is even so return c

R5 : $c = 16^\wedge 2 \mod 119 = 18$

x is even so return c

R4 : $c = 18^\wedge 2 \mod 119 = 86$

x is odd so return $a * c \mod n$

$38 * 86 \mod 119 = 55$

return 55

R3 : $c = 55^\wedge 2 \mod 119 = 50$

x is odd. so return $(38 \times 50) \mod 119 = 115$

R2 : $c = 115^\wedge 2 \mod 119 = 16$

x is even so return c

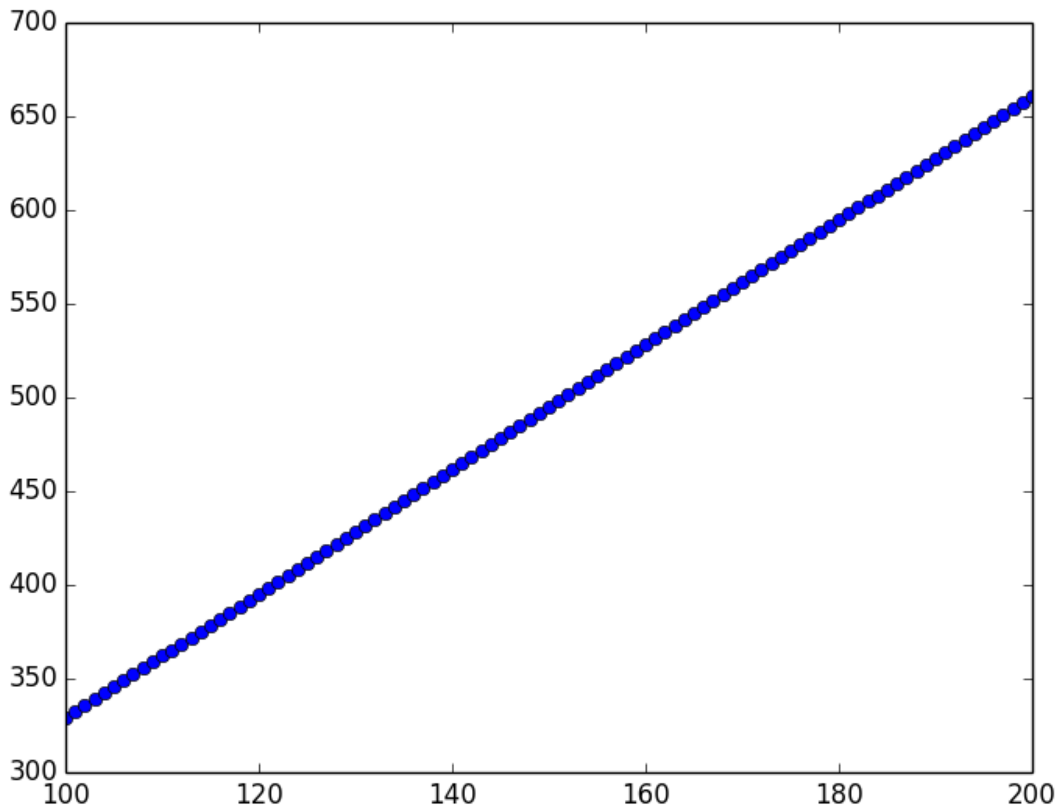
R1 : $16^\wedge 2 \mod 119 = 18$

x is odd so return $(38 \times 18) \mod 119 = \underline{89}$

So the message is decrypted and we get back.

$\boxed{M = 89}$.

Coding Question:
By Sylvester's Theorem, we know there is always a prime in this range. For 0.5pts of your coding points described below, plot $\log_2\left(x-2^{n-1}\right)$ vs n where x is your output for values n between 100 and 200. Say what you observe.



From the above graph we can say that $\log_2\left(x-2^{n-1}\right)$ linearly increases as n increases. So its O(n).