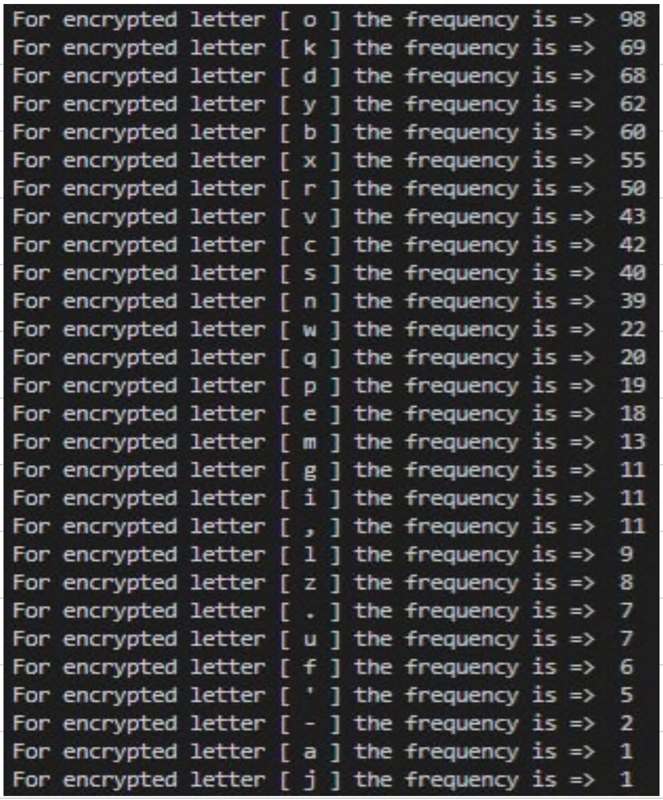
1. A python file was coded in order to answer the following questions:

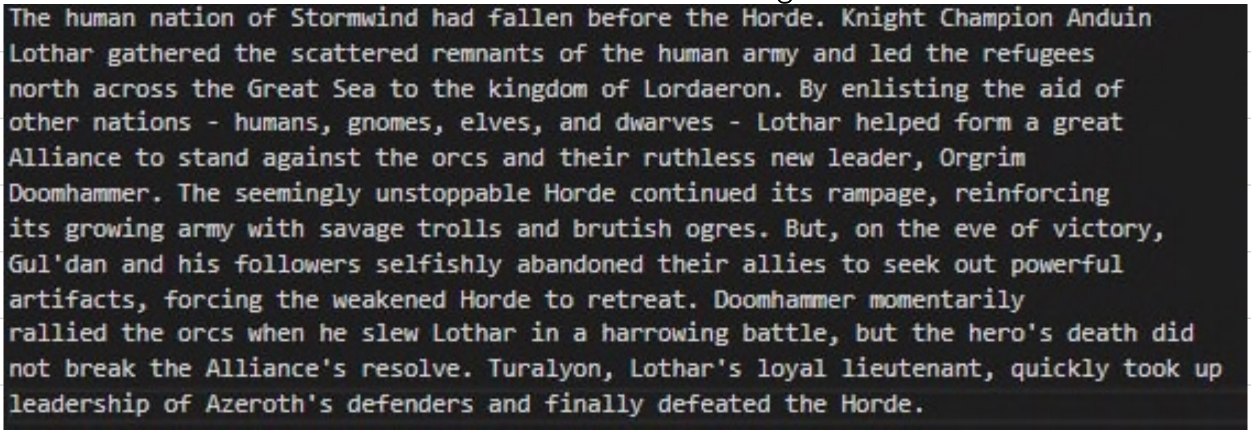
a).



```
For encrypted letter [ o ] the frequency is =>  98
For encrypted letter [ k ] the frequency is =>  69
For encrypted letter [ d ] the frequency is =>  68
For encrypted letter [ y ] the frequency is =>  62
For encrypted letter [ b ] the frequency is =>  60
For encrypted letter [ x ] the frequency is =>  55
For encrypted letter [ r ] the frequency is =>  50
For encrypted letter [ v ] the frequency is =>  43
For encrypted letter [ c ] the frequency is =>  42
For encrypted letter [ s ] the frequency is =>  40
For encrypted letter [ n ] the frequency is =>  39
For encrypted letter [ w ] the frequency is =>  22
For encrypted letter [ q ] the frequency is =>  20
For encrypted letter [ p ] the frequency is =>  19
For encrypted letter [ e ] the frequency is =>  18
For encrypted letter [ m ] the frequency is =>  13
For encrypted letter [ g ] the frequency is =>  11
For encrypted letter [ i ] the frequency is =>  11
For encrypted letter [ , ] the frequency is =>  11
For encrypted letter [ l ] the frequency is =>  9
For encrypted letter [ z ] the frequency is =>  8
For encrypted letter [ . ] the frequency is =>  7
For encrypted letter [ u ] the frequency is =>  7
For encrypted letter [ f ] the frequency is =>  6
For encrypted letter [ ' ] the frequency is =>  5
For encrypted letter [ - ] the frequency is =>  2
For encrypted letter [ a ] the frequency is =>  1
For encrypted letter [ j ] the frequency is =>  1
```

'O' was found to have the highest letter frequency.

By following the letter frequency, 'e' is the most used letter in the English lang. Thereby substi. 'o' for 'e' we get a division of 16 from the right. Following the trend gives the following decrypted ans:



```
The human nation of Stormwind had fallen before the Horde. Knight Champion Anduin
Lothar gathered the scattered remnants of the human army and led the refugees
north across the Great Sea to the kingdom of Lordaeron. By enlisting the aid of
other nations - humans, gnomes, elves, and dwarves - Lothar helped form a great
Alliance to stand against the orcs and their ruthless new leader, Orgrim
Doomhammer. The seemingly unstoppable Horde continued its rampage, reinforcing
its growing army with savage trolls and brutish ogres. But, on the eve of victory,
Gul'dan and his followers selfishly abandoned their allies to seek out powerful
artifacts, forcing the weakened Horde to retreat. Doomhammer momentarily
rallied the orcs when he slew Lothar in a harrowing battle, but the hero's death did
not break the Alliance's resolve. Turalyon, Lothar's loyal lieutenant, quickly took up
leadership of Azeroth's defenders and finally defeated the Horde.
```

2. ASIC checking speed = $5 \cdot 10^{8}$ keys / sec

a) Budget = \$1,000,000

1 AISC = \$100

$\therefore$ Total AISC $= \dfrac{1000000}{100}$

$\Rightarrow 10,000$

$\therefore$ 10,000 AISC can run in parallel.

Avg. key search = ?

$\Rightarrow$ key length = 128 bits.

$\therefore$ keys $= 2^{127}$

$\therefore$ 2^{127} x checking sp. x total AISC

$\Rightarrow 2^{127} \times (5 \cdot 10^{8}) \times 10,000$

$\Rightarrow 2^{127} \times 5 \cdot 10^{8} \times 10^{4} = 2^{127} \times 5 \cdot 10^{12}$ sec thus longer than the universe.

$= 1.08 \times 10^{18}$ years ;

b) According to Moore's law, computer power doubles every 18 months. assuming 'k' as Moore's iteration.

24 hours = 1 day.

1 year = 365 days

$\therefore 1 \text{ day} = \dfrac{1.08 \times 10^{18} \text{ years} \times 365}{2^{i}} = 2^{i} = 1.08 \times 10^{18}$ years $\times 365$

$\therefore i = 68.42$ iterations.

$i \approx 69$ iterations.

$\therefore 1.5$ years $\times 69 = 103.5$ years.

3. password = 8 letters

a) Since there are 7 bits per character, each character will represent 2^7 keys

$\therefore$ 8 letters $\Rightarrow (2^7)^8 = 2^{56}$ keys

$\therefore$ size of key space = 2^{56} keys

b) key length = num (characters) x bit/character

$\Rightarrow 8 \times 7 = 56$ bits

c) Bits per character = celing $(\log(26)) = 5$

$\therefore$ key length = $5 \times 8 = 40$ bits

d)

i) $128/7 = 18.28$ characters

≈ 19 characters

ii) From question 3(c) we found the bits/char for 26 lowercase letters

= 5 bits/char.

$\therefore \frac{128}{5} = 25.6$ characters $\approx$ 26 characters.

4.

a) $15 \cdot 29 \mod 13$

$\Rightarrow 15 \mod 13 \qquad 29 \mod 13$

$2 \qquad 3$

$\therefore 2 \cdot 3 = 6$

$\Rightarrow 6 \mod 13 = 6$

b) $2 \cdot 39 \mod 13$

$2 \mod 13 \qquad 39 \mod 13$

$2 \qquad 0 \qquad \therefore 2 \cdot 0 = 0 \quad \therefore 0 \mod 13 = 0$

c) $2 \cdot 8 \bmod 13$

$2 \bmod 13 \qquad 8 \bmod 13$

$2 \qquad 8$

$\therefore\ 2 \cdot 8 = 16$

$16 \bmod 13 = 3$

d) $-11 \cdot 4 \bmod 13$

$-11 \bmod 13 \qquad 4 \bmod 13$

$2 \qquad 4$

$\therefore\ 2 \cdot 4 = 8$

$\Rightarrow 8 \bmod 13 = \underline{\underline{8}}$

5.

a) $1/5 \bmod 13$

$\Rightarrow 5^{-1} \bmod 13$

$\Rightarrow 5x = 1 \bmod 13 \quad \therefore\ x = 8$

$\therefore\ 1/5 \bmod 13 = \underline{\underline{8}}$

b) $1/5 \bmod 7$

$\Rightarrow 5^{-1} \bmod 7 \Rightarrow 5x = 1 \bmod 7 \Rightarrow x = 3$

$\therefore\ 1/5 \bmod 7 = \underline{\underline{3}}$

c) $4 \cdot 2/5 \bmod 7$

$4 \cdot 2 \cdot 1/5 \bmod 7 \qquad 1/5 \bmod 7$

$\Rightarrow 8 \bmod 7 \qquad 3$

$1 \qquad \therefore\ 1 \cdot 3 = 3 \Rightarrow 3 \bmod 7 = \underline{\underline{3}}$

d) $9^{2021} \bmod 80$

$9 \cdot 9^{2020} \bmod 80 \Rightarrow 9 \bmod 80 \qquad 9^{2020} \bmod 80$

$9 \qquad \Rightarrow (9^2)^{1010} \bmod 80 \Rightarrow (81)^{1010} \bmod 80$

$\Rightarrow (1)^{1010}$ $[81 \bmod 80 = 1]$
$= 1$

$\therefore 9 \cdot 1 = 9$ $\therefore 9 \bmod 80 = 9$

Addition table for Z_5

6.
a)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication table for Z_5

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Addition table for Z_6

b)

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplication table for Z_6

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

c) 0, 2, 3, 4

d) 5 is a prime no. and all the non-zero elements in Z_5 are smaller than 5.