Robert Jones

Homework 5

1.

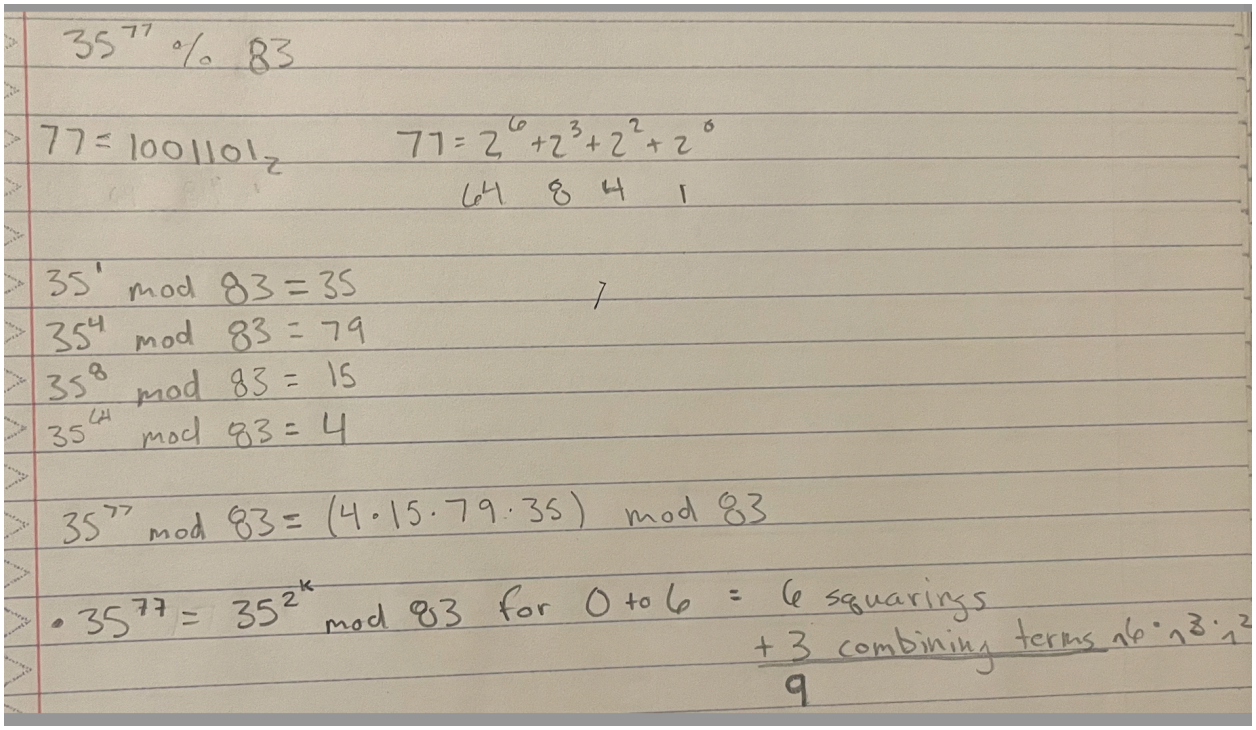
```
--------------
    1 | 426.318
    2 | 347.807
    3 | 364.343
    4 | 349.268
    5 | 299.582
    6 | 406.525
    7 | 346.854
    8 | 419.814
    9 | 380.675
   10 | 465.761
   11 | 414.671
   12 | 378.579
   13 | 425.168
   14 | 366.325
   15 | 306.071
   16 | 370.525
   17 | 419.789
   18 | 320.171
   19 | 425.232
   20 | 272.582
   21 | 255.961
   22 | 410.739
   23 | 685.564
   24 | 433.536
   25 | 347.314

Best Key: 23
Decrypted Plaintext:
WHENINTHECOURSEOFHUMANEVENTS
The program '/Users/tylerjones/Desktop/CaeserCipherDecryption/CCD' has exited with code 0 (0x00000000).
```

2. Caesar cipher is not a public system because it does not share a public/private key relationship. If k was an encryption key, it would easily lead to the decryption key through 26-k, making the public/private relationship obsolete.

3.

a.



b.

c.
```cpp
#include <iostream>
```

d.
```cpp
using namespace std;
```

e.

f.
```cpp
unsigned int dexp(unsigned int x, unsigned int y, unsigned int n) {
```

g.
```cpp
    unsigned long long result = 1;
```

h.
```cpp
    unsigned long long base = x % n;
```

i.

j.
```cpp
    while (y > 0) {
```

k.
```cpp
        if (y & 1) {
```

l.
```cpp
            result = (result * base) % n;
```

m.
```cpp
        }
```

n.

o.
```cpp
        base = (base * base) % n;
```

p.
```cpp
        y >>= 1;
```

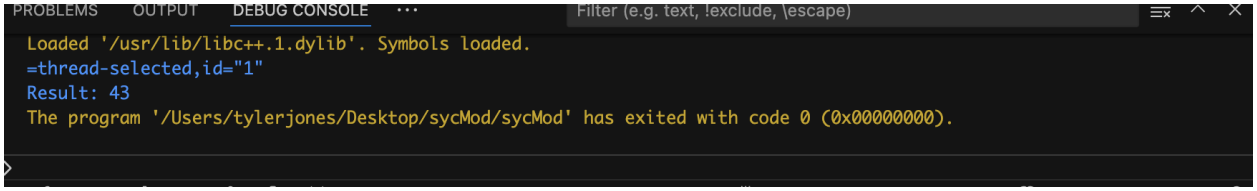
q.
```cpp
    }
```

r.
```cpp
return static_cast<unsigned int>(result);
```

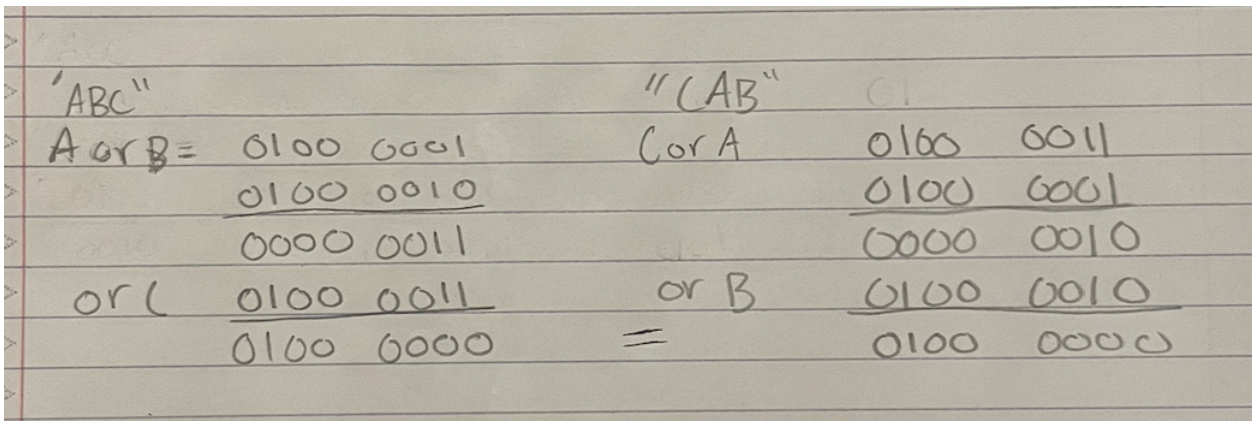
s.
```cpp
}
```

```
t.
u.  int main() {
v.      unsigned int x = 35;
w.      unsigned int y = 77;
x.      unsigned int n = 83;
y.      unsigned int answer = dexp(x, y, n);
z.      cout << "Result: " << answer << endl;
aa.     return 0;
bb. }
```

C.

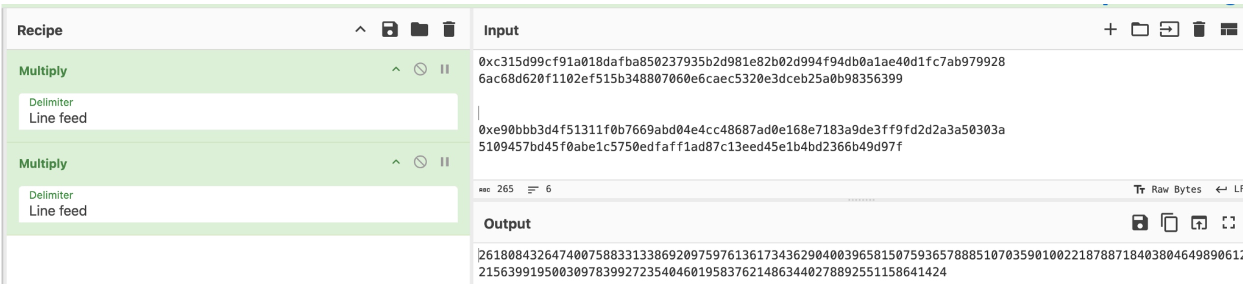


4.



XOR is not a secure hash function. It is too easy to replicate and backtrack hash's with so few options. Similarly the lack of options creates too many possibilities for collisions. The hashes also dont change enough when altered, easily tracked decyphered when making alterations.

5.



6. 200111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111

179820433

7.

$Files_T = 10{,}000$
Viruses = 50
$Files_c = 9{,}950$
FPR = 0.5%
FNR = 1%
TNR = 99%
TPR = 99.5%

a.)
$TNR = \frac{TN}{N}$ $TN = (.99)(9{,}950)$
$TN = 9850$
$FNR = \frac{FN}{P}$ $FN = (1\%)(50)$
$FN = .5$

Clean = 9851   True = 9850

b.)
$TPR = \frac{TP}{P}$ $TP = (99.5\%)(50)$
$TP = 49.75$
$FPR = \frac{FP}{N}$ $FP = (0.5\%)(9{,}950)$
$FP = 49.75$

flagged = 99.5   Clean = 49.75

c.)
$acc = \frac{TP + TN}{Total} = \frac{49.75 + 9850}{10{,}000} = .989 \approx 99\%$

d.) $prec = \frac{TP}{TP + FP} = \frac{49.75}{49.75 + 49.75} = .5$ 50%

e.) $recall = \frac{TP}{TP + FN} = \frac{49.75}{49.75 + .5} = .99 \approx 99\%$

f.) This system is good for detecting viruses but has low precision.