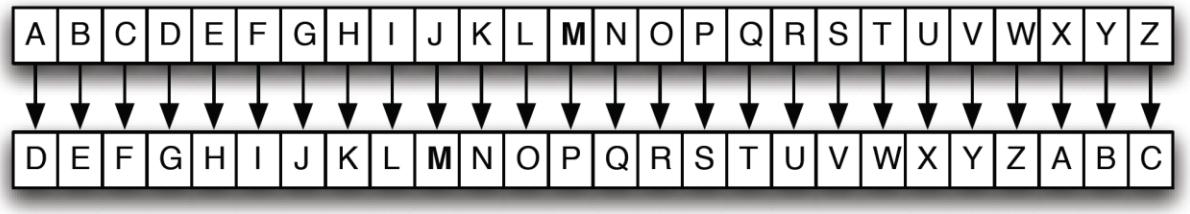
CS 3339 Encryption Homework

1. Caesar Cipher



The example Caesar Cipher above has an offset of +3.

Given the following ciphertext

wklv lv wkh phvvdjh

Figure what the plaintext is for this ciphertext

this is the message

2. Public Key Cryptography
   a. Given **p = 109**, **q = 53, e = 97**, Find **n, ϕ(n),** and **d**

      n = p * q = 5777
      ϕ(n) = (p - 1) * (q - 1) = 5616
      d = (1 (mod ϕ(n)) / e = 3937

   b. Using your result from part a, encrypt the plaintext **x=32**

      y = (32 ^ 97) mod 5777 = 3978

3. One-Time pad
   For this question, use the following encoding,

```
A=0000  B=0001  C=0010  D=0011  E=0100  F=0101  G=0110 H=0111
I=1000  J=1001  K=1010  L=1011  M=1100  N=1101  O=1110  P=1111
```

   a. Figure out the 1-time pad that encrypts this plaintext to this ciphertext

```
Plaintext: BACK   0001 0000 0010 1010
Ciphertxt: FNCG   0101 1101 0010 0110
1time-pad: ENAM   0100 1101 0000 1100
```

   b. Figure out the ciphertext that is generated by this plaintext and 1-time-pad

```
Plaintext: JOKE   1001 1110 1010 0100
1time-pad: MPDK   1100 1111 0011 1010
Ciphertxt: FBJO   0101 0001 1001 1110
```

4. Diffie-Hellman Key Exchange
Given the following information, show how Diffie-Hellman key exchange works for both the client and the server

p=2161, g=23

Client: a = 532
Server: b = 461

Some prime number p and a number g which is coprime to p-1 are chosen. The client and server each choose arbitrary secret numbers a and b. The client then computes (g ^ a) mod p and sends the result of that calculation to the server. The server does the same operation, but with its own secret number and sends the result of (g ^ b) mod p to the client. Both parties then perform the same operation, but with the result they received instead of g. The client and server should have arrived at the same number, which can be used as their shared secret key.

Key = $g^{ab} \bmod p = 1552$
Client calculation: $(g^a \bmod p)^b \bmod p$
Server calculation: $(g^b \bmod p)^a \bmod p$