Affine Cipher 8/26/2020

Wednesday, August 26, 2020 11:36 AM

Quick Review:

Treat the letters A to Z as numbers from 0 to 25.

Shift Cipher: $f(x, k) = (x + k) \bmod 26$
$= (x + k)\%26$ (Encrypt)

Decrypt $f^{-1}(y, k) = (y - k) \bmod 26$
$= (y - k + 26)\%26$

```
Plaintext:   C  A  T
             2  0  19
Key = 10  10 10 10
          ------------
          12, 10, 29 % 26 = 3
          MKD

Decrypt   12  10  3
          -10 -10 -10
          ---------------
           2    0   (-7 + 26)%26 =19
           C    A                  T
```

# of possible keys = 26

This function kind of looks like a line (a linear function), but the shift cipher has a "slope" of 1. What if we allowed different slopes?

Affine Cipher

Two keys: a and b
$f(x, a, b) = (ax + b) \bmod 26$

Example: a = 5, b = 20

Plaintext: HOUSE
f(H) = (5*7 + 20)%26 = 55 % 26 = 3 (D)
f(O) = (5*14 + 20)%26 = 90 % 26 = 12 (M)
f(U) = (5*20 + 20)%26 = 120 % 26 = 16 (Q)
f(S) = (5*18 + 20)%26 = 110 % 26 = 6 (G)
f(E) = (5*4 + 20)%26 = 40 % 26 = 14 (O)

It's less obvious how to decrypt this function!
For shift, it was clear that to undo the adding, we would have to subtract, but for a cipher to work, we need to be able to undo the operation of encryption.

What is a prerequisite for this to be a valid set of keys?

What about this function?

a = 13, b = 2, f(x) = (13x + 2) % 26

Does this look like a good function for encryption???

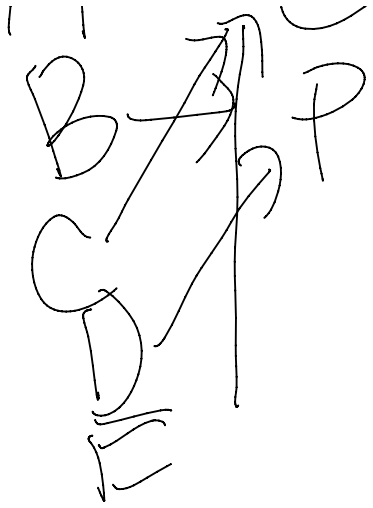
f('A') = 13*0 + 2 = 2
f('B') = 13*1 + 2 = 15
f('C') = (13*2 + 2) % 26 = 28 % 26 = 2
f('D') = (13*3 + 2) % 26 = 41 % 26 = 15

Couple issues:

1) Two different plaintexts mapped to the ciphertext, so it's impossible to figure out what was the original plaintext given the ciphertext only.
2) C $^{\text{ecrypted}}$ as C, this seems like a bad idea.

In order for encryption to work, the function it induces must be invertible.

For example, if f(x) = 2x + 4, then $f^{-1}(x) = (x-4)/2$.



function

To be invertible, we need a one-to-one function.

For what values of a and b, does the function f(x) = (ax+b) % 26 produce a one to one function?

Try a few examples…

f(x) = (5x + 20)%26 this is okay.
f(x) = (13x + 2)%26 this is bad.
f(x) = (2x + 5)% 26 --> Are there two different inputs that create the same output, if so what? Answer: 0, 13

f(0) = (2*0 + 5) = 5
f(13) (2*13 + 5) % 26 = 31 % 26 = 5

26 + 5 equivalent 0 + 5 mod 26

if that product is ever a multiple of 26, then we'll have a repeat.

f(x) = (6x + 3) % 26
Again, try x = 0, x = 13, note that 6*13 = 78 which is 0 mod 26.

Bad values of a are 2, 6, 13. Which other ones are bad?

Two integers are relatively prime if they share no common factors.

We will define a function gcd(a, b) = greatest common divisor of two integers a and b.

Two integers a and b are relatively prime iff (if and only if) gcd(a, b) =

1.

If a and 26 share a common factor, then the function will not be one to one.

So, if a = a' x common factor
Then a x (26/common factor) = multiple of 26

6 = 3 x 2
26 = 2 x 13

6 x (26/2) = (6/2) x (26) = 3 x 26

The affine cipher keys are valid iff gcd(a, 26) = 1. The valid values of a are:

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 and 25

Thus, the total number of valid keys for the affine cipher are

12 x 26 = 312

f(x) = (5x + 20) % 26

How do I decrypt? find the inverse function…

x = (5y + 20) mod 26

(x - 20) = 5y mod 26, **When you get here, you have to multiply the whole equation through by the modular inverse, in this case 5^{-1} mod 26 = 21.**

In regular math, we would divide by 5…but in mod math, dividing isn't allowed! (Only ints allowed under mod but dividing might create non integer values)

21(x - 20) = 21(5y) mod 26
21x - 420 = 105y mod 26

Mod Rule:

if a = b mod 26, then we can replace each occurrence of a in a function with b and vice versa without changing its value under mod, so long as the terms are additive or multiplicative. (Can't do this with exponents though.)

Since 105 = 1 mod 26 (a = b mod n if and only if n | (a - b). That vertical bar is divisibility.

Also since -420 = 22 mod 26, we can replace -420 with 22 in the equation above.

a | b - "b is divisible by a" means there exists some integer c such that b = ac. So, 6 | 48, 12 | 12, 107 | 0, 13 | 39 are all true.

21x - 420 = 105y mod 26
21x + 22 = 1y mod 26

$f^{-1}(x) = (21x + 22) \bmod 26$

5 x 21 = 1 mod 26 (so that's why 21 is the "magic" value to multiply by).

Let's quickly test this out:

$f^{-1}(D) = (21*3 + 22) = 85 \% 26 = 7$ (H)
$f^{-1}(M) = (21*12 + 22) = 274 \% 26 = 14$ (O)
$f^{-1}(Q) = (21*16 + 22) = 358 \% 26 = 20$ (U)
$f^{-1}(G) = (21*6 + 22) = 148 \% 26 = 18$ (S)
$f^{-1}(O) = (21*14 + 22) = 316 \% 26 = 4$ (E)

For any number a, if

$a \times b \equiv 1 \bmod 26$, then we say that $b = a^{-1} \bmod 26$

For today I have a list of modular inverse mod 26.