DTTF/NB479: Dszquphsbqiz Day 2

- Announcements:
  - Subscribe to Angel forums
- Questions?
- Roll Call
- Today: affine ciphers

Affine ciphers

Somewhat stronger since **scale, then shift**:

$x \rightarrow \alpha x + \beta \pmod{26}$

Say $y = 5x + 3$; x = ‘hellothere’;

Then y = ‘mxggv…’

Affine ciphers: $x \rightarrow \alpha x + b \pmod{26}$

Consider the 4 attacks:

1. How many possibilities must we consider in brute force attack?

Restrictions on α

Consider y= 2x, y = 4x, or y = 13x

What happens?

Basics 1: Divisibility

Definition:

$$Given\ a, b \in Z, a \neq 0.$$

$$a \mid b\ means\ \exists k \in Z\ s.t.\ b = ka$$

Property 1:

$$\forall a \neq 0, \quad a \mid 0, \quad a \mid a, \quad 1 \mid a$$

Property 2 (transitive):

$$a \mid b\ and\ b \mid c \Rightarrow a \mid c$$

Property 3 (linear combinations):

$$a \mid b\ and\ a \mid c \Rightarrow a \mid (sb + tc) \forall s, t \in Z$$

Basics 2: Primes

- Any integer p > 1 divisible by only p and 1.
- How many are there?
- Prime number theorem:
  - Let $\pi(x)$ be the number of primes less than x.
  - Then $$\lim_{x \to \infty} \pi(x) = \frac{x}{\ln(x)}$$
  - Application: how many 319-digit primes are there?
- Every positive integer is a unique product of primes.

Basics: 3. GCD

- gcd(a,b)=$\max_j$ (j|a and j|b).
- Def.: a and b are relatively prime iff gcd(a,b)=1
- gcd(14,21) easy…

Basics 4: Congruences

- Def: a≡b (mod n) iff (a-b) = nk for some int k
- Properties

$$Consider\ a,b,c,d \in Z, n \neq 0$$
$$a \equiv b \pmod{n}\ if\ \exists k \in Z\ s.t.\ a = b + nk$$
$$a \equiv 0 \pmod{n}\ iff\ n \mid a$$
$$a \equiv a \pmod{n}$$
$$a \equiv b \pmod{n}\ iff\ b \equiv a \pmod{n}$$
$$a \equiv b, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$$

$$If\ a \equiv b, c \equiv d \pmod{n}, then$$
$$(a + c) \equiv (b + d) \pmod{n}$$
$$(a - c) \equiv (b - d) \pmod{n}$$
$$ac \equiv bd \pmod{n}$$
$$If\ \gcd(a,n) = 1\ and\ ab \equiv ac \pmod{n}, then$$
$$b \equiv c \pmod{n}$$

- You can easily solve congruences ax≡b (mod n) if gcd(a,n) = 1 and the numbers are small.
  - Example: 3x+ 6 ≡ 1 (mod 7)
- If gcd(a,n) isn't 1, there are multiple solutions (next week)

Restrictions on α

Consider y= 2x, y = 4x, or y = 13x

The problem is that gcd(α, 26) != 1.

The function has no inverse.

Finding the decryption key

- You need the inverse of $y = 5x + 3$
- In *Integer (mod 26) World*, of course…
- $y \equiv 5x + 3 \pmod{26}$

Affine ciphers: x → ax + b (mod 26)

- Consider the 4 attacks:
  1. Ciphertext only:
     - How long is brute force?
  2. Known plaintext
     - How many characters do we need?
  3. Chosen plaintext
     - Wow, this is easy.
  4. Chosen ciphertext
     - Could be even easier!