Day 2 Notes

Lucas Brehm

January 31st 2024

1 Caesar Cipher

Encryption Function: $E_k(x) \equiv x + k$

Decryption Function $D_k(x) \equiv x - k$

With English alphabet, 26 possible keys, brute forcing (trying all possible keys) takes only a few seconds

2 Modular Arithmetic

We say that $a \equiv b \pmod{m}$
"a is congruent to b modulo m"
if a and b have the same remainder when divided by m

Alternatively, $a \equiv b \pmod{m}$ if m divides $(a - b)$.

Example: $5 \equiv 31 \equiv -25 \pmod{26}$

Addition, subtraction, and multiplication are always valid in modular arithmetic. (No fractions allowed! Also no non-integers.)

3 Affine Cipher

Pick a key (a,b)
- b can be anything (mod 26)
- a must have an inverse on mod m
(there are 312 possible keys)

Encryption function: $E(x) \equiv ax + b \pmod{26}$
Example: a = 3, b = 11
$E(x) = 3x + 11 \pmod{26}$

Let's encrypt "it" (i = 8, t = 19)
I: $E(8) \equiv 3(8) + 11 \equiv 36 \equiv 9 \pmod{26}$
T: $E(19) \equiv 3(19) + 11 \equiv 68 \equiv 16 \pmod{26}$
"IT" encrypts to "JQ"

Decryption: We need to subtract b from both sides and then 'divide' by a. However, we can't actually divide so we instead multiply both sides by the inverse of a.
The inverse of a, $a^{-1} \pmod{26}$ (if it exists) is a number where $a * a^{-1} \equiv 1 \pmod{26}$

Decryption function:
$D(y) \equiv a^{-1}(y - b) \pmod{26}$
$D(y) \equiv a^{-1}y - a^{-1}b) \pmod{26}$

Example: Find decryption function for $E(x) \equiv 3x + 11 \pmod{26}$
$y - 11 \equiv 3x \pmod{26}$
$3^{-1} \equiv 9 \pmod 2 6$
(since $3 * 9 \equiv 27 \pmod{26}$)
$9(y - 11 \equiv 9(3x) \equiv x \pmod{26})$
$D(y) = 9y + 5 \pmod{26}$

Decrypt "JQ" (9, 16)
$D(9) \equiv 9(9) + 5 \equiv 8 \pmod{26}$ (this is i)
$D(9) \equiv 9(16) + 5 \equiv 19 \pmod{26}$ (this is t)
In affine ciphers, you cannot use 2 for the a portion of the key