Cryptography Notes

Tim DeLloyd

September 10, 2024

1 Hill Cipher

Has good diffusion since changing a single letter of the plaintext will change the entire block.

2 Ciphertext

- only viable attack options are difficult

- if the blocksize is small we can brute force or use frequency analysis of digrams (two letters) or trigrams (three letters)

- most common digram in English is ”th”, second most common is a tie between ”he” and ”er”

3 Ring

3.1 Definition

A ring is a collection of things that we can add, subtract, and multiply while staying within the collection

3.2 Properties

- Usual laws of arithmetic apply

- (observations: we need to have a zero element (additive identity) and a one element (multiplicative identity)

3.3 Examples

- Set of the integers ($\mathbb{Z}$)

- Set of the reals ($\mathbb{R}$)

- Set of the rations ($\mathbb{Q}$)

- Set of complex numbers ($\mathbb{C}$)

- Polynomials, e.g., $\mathbb{Z}_n$, $\mathbb{R}_n$, $\mathbb{Q}_n$

- Set of remainders when dividing by m ($\mathbb{Z}_m$)*

*Note: the set of natural numbers ($\mathbb{N}$) is **NOT** a ring.*

*If we define +, -, and $\cdot$ using modular arithmetic ($a \equiv b \pmod{m}$), if $b - a$ is divisible by m, then $\mathbb{Z}_m$ is a ring.

3.4 Division

In a ring we can do division by elements that have an inverse.
a has inverse a^{-1} if $a \cdot a^{-1} \equiv 1 \pmod{m}$.
In $\mathbb{Z}_m$, if element $a \in \mathbb{Z}_m$ and m have $\gcd(a, m) = 1$, a^{-1} exists, and we say a and m are relatively prime.
The equivalence class of all integers $\pmod{m}$ with the same remainder is called a resolve modulo m.

4 Greatest Common Divisor

We can compute GCD's very quickly even if the integers involved are huge using Euclid's Algorithm.

4.1 Euclid's Observations

- If a and b are any two integers there is always a unique remainder r when dividing a by b with $0 \leq r < b$, $a = qb + r$

- If d divides both m and n, then it also divides $m + n$, $m - n$, $am + bn$

This means if d divides a and b it also divides $a - qb = r$, and anything that divides b and r divides a

$$\gcd a, b = \gcd b, r$$

with r smaller than a and b
We can repeat this process until we get a remainder 0, then the GCD is the last nonzero remainder we get.

4.2 Example 1

Find $\gcd 119, 91$

$$119 - 91 \cdot 1 = 28$$

$$91 - 28 \cdot 3 = 7$$

$$28 - 7 \cdot 4 = 0$$

Therefore, the GCD is 7.

4.3 Example 2

Find $\gcd 77, 45$

$$77 - 45 \cdot 1 = 32$$

$$45 - 32 \cdot 1 = 13$$

$$32 - 13 \cdot 2 = 6$$

$$13 - 6 \cdot 2 = 1$$

$$6 - 1 \cdot 6 = 0$$

Therefore, the GCD is 1.

5 Extended Euclid's Algorithm

Find two numbers, x and y, such that $ax + by = d = \gcd a, b$.
Note: $ax + by$ is called a linear combination of a and b.
First we write out all of the quotient and remainder expression we found along the way using regular Euclid's Algorithm to obtain the $\gcd a, b$. Then, we combine them back together.

5.1 Example 3

Find $\gcd 77, 45$ like Example 1 above:

$$77 = 1 \cdot 45 + 32$$

$$45 = 1 \cdot 32 + 13$$

$$32 = 2 \cdot 13 + 6$$

$$13 = 2 \cdot 6 + 1$$

Next, regroup using substitution working backwards:

$$1 = 13 - 2 \cdot (6)$$

$$1 = 13 - 2 \cdot (32 - 2 \cdot 13)$$

$$1 = -2 \cdot 32 + 5 \cdot 13$$

$$1 = -2 \cdot 32 + 5 \cdot (13)$$

$$1 = -2 \cdot 32 + 5 \cdot (45 - 1 \cdot 32)$$

$$1 = 5 \cdot 45 - 7 \cdot 32$$

$$1 = 5 \cdot 45 - 7 \cdot (32)$$

$$1 = 5 \cdot 45 - 7 \cdot (77 - 1 \cdot 45)$$

$$1 = -7 \cdot 77 + 12 \cdot 45$$

Therefore, in this example, $x = -7$ and $y = 12$ if $a = 77$ and $b = 45$.