Cryptography — Part 1

Modular Arithmetic & Basic Ciphers

04.14.2026

Autumn Luzovich (they/them/theirs)

Quick Preface

Cryptography is hard!

1 Modular Arithmetic

Addition

$1 + 5 \equiv 6 \bmod 10$

$1 + 9 \equiv 0 \bmod 10$

$50 + 50 \equiv 0 + 0 \bmod 10$

$12 + 15 \equiv 6 \bmod 7$

Subtraction

$14 - 2 = 12 \equiv 2 \bmod 10$

$0 - 7 \equiv -3 \bmod 4 \equiv 1 \bmod 4$

$1 - 2 \equiv 0 \bmod 1$

$6 - 7 \equiv 1 \bmod 2$

Multiplication

$0 \times 1 = 0 \equiv 0 \bmod x \mid x \in \mathbb{Z}^+$

$1 \times 8 \equiv 1 \bmod 7$

$2 \times 4 \equiv 2 \bmod 3$

$\equiv 2 \bmod 6$

$12 \times 12 = 144 \equiv 1 \bmod 13$

Multiplicative Inverse

$2 \times 5 = 10 \equiv 4 \bmod 6$

How do we get 2 back? We multiply by the "inverse" of 5 in $\mathbb{Z}/6\mathbb{Z}$.

- Essentially an undo operation: $4 \times 5^{-1} \equiv 2 \bmod 6$

  $5 \times 5^{-1} \equiv 1 \bmod 6$

  $5^{-1} \equiv 5 \bmod 6$

Not all numbers have inverses!

- Being a unit (e.g., invertible) means having no common factors.
- 2 has a common factor with 6; 2. Therefore, it has no inverses.

Multiplicative Inverse (ii)

Euclidean Algorithm

Solve systems of equations that follow the form: $ax + by = 1$.

So to get the inverse from the previous example: $5x + 6y = 1$.

$a, b \in \mathbb{Z}^+ \qquad b > a$

$b = aq_1 + r_1$[1]

$a = r_1 q_2 + r_2$

$r_1 = r_2 q_3 + r_3$

$5, 6 \in \mathbb{Z}^+ \qquad 6 > 5$

$6 = 5(1) + 1$

$5 = 1(5) + 0$

We stop when our remainder is 0.

$1 = 6 - 5(1) = 5(-1) + 6(1)$

$-1 \equiv 5 \bmod 6 \qquad 5 \times 5 \equiv 1 \bmod 6$

[1] q is our quotient, r is our remainder

2 Basic Ciphers

Shift Cipher

Simple translation within the modulo n; $x + B$.

Encrypt

Relatively easy.

Decrypt

Also pretty easy.

Affine Cipher

Multiplication under the modulo n with an additional optional shift $Ax + B$.

Encrypt

Little hard but still easy.

Decrypt

A bit harder with multiplicative inverse calculation. Make sure A is invertible under $\mathbb{Z}/n\mathbb{Z}$!

$$\begin{aligned} N &\equiv Ax + b \\ N - b &\equiv Ax \\ (N - b)A^{-1} &\equiv x \end{aligned}$$

3 Looking Ahead

Diffie-Hellman Key Exchange

Agree on a mutual "unit"[2] g of some prime ring $\mathbb{Z}/p\mathbb{Z}$

Bob: $g^a \equiv A \bmod p$

- Shares A with Alice

Alice: $g^b \equiv B \bmod p$

- Shares B with Bob

Bob: $A^b \equiv K \bmod p$

Alice: $B^a \equiv K \bmod p$

Neither know their partner's secret number but can still get K!

[2] Units allow us to cover the entirety of the ring with just powers of itself; $\{g^0, g^1, \ldots, g^{p-1}\} = \mathbb{Z}/p\mathbb{Z}$

ElGamal Cryptosystem

Amalgamation of multiplicative inverses and Diffie-Hellman.

We do it in a prime number space, which makes finding units easy.

Let's say Bob wants to send a message m to Alice:

Alice shares A with Bob: $g^a \equiv A \bmod p$

Bob shares B and C with Alice:

$$g^b \equiv B \bmod p$$
$$mA^b \equiv C \bmod p$$

Alice computes the message m by multiplying C with the inverse of B^a:

$$m \equiv CB^{-a} \bmod p \equiv mA^b B^{a^{-1}} \bmod p$$