Chapter 1: Introduction

1.1 Overview of Number Theory

The Division Algorithm

Given any positive integer *n* and any nonnegative integer *a*, if we divide *a* by *n*, we get an integer quotient *q* and an integer remainder *r* that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor \qquad (1)$$

where $\lfloor x \rfloor$ is the largest integer less than or equal to *x*. (qn ≤ a)

Example:

a= 70 ; n = 15; 70 = (4 * 15) + 10

a= 11 ; n = 7; 11 = (1 * 7) + 4

a= -11 ; n = 7; -11 = (-2 * 7) + 3

THE EUCLIDEAN ALGORITHM

Greatest Common Divisor

Recall that nonzero *b* is defined to be a divisor of *a* if *a* = *mb* for some *m*, where *a*, *b*, and *m* are integers. We will use the notation gcd(*a*, *b*) to mean the **greatest common divisor** of *a* and *b*. The greatest common divisor of *a* and *b* is the largest integer that divides both *a* and *b*. We also define gcd(0, 0) = 0.

Because we require that the greatest common divisor be positive, gcd(*a*, *b*) = gcd(*a*, -*b*) = gcd(-*a*, *b*) = gcd(-*a*, -*b*). In general, gcd(*a*, *b*) = gcd($|a|$, $|b|$).

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943434	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

gcd(*a*, *b*) = gcd(*b*, *a* mod *b*) (2)

MODULAR ARITHMETIC

11 mod 7 = 4; -11 mod 7 = 3

[(*a* mod *n*) + (*b* mod *n*)] mod *n* = (*a* + *b*) mod *n*

$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

$[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

The Extended Euclidean Algorithm

$$ax + by = d = \gcd(a, b) \qquad (3)$$

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
⋮	⋮	⋮	⋮
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-1} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_n \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

Example a= 1759; b=550

i	r_i	q_i	x_i	y_i
−1	1759		1	0
0	550		0	1
1	109	3	1	−3
2	5	5	−5	16
3	4	21	106	−339
4	1	1	−111	355
5	0	4		

Result: $d = 1; x = -111; y = 355$

$$q_i = \lfloor r_{i-2}/r_{i-1} \rfloor;\; r_i = r_{i-2} \bmod r_{i-1}$$

$$x_i = x_{i-2} - q_i \times x_{i-1};\; y_i = y_{i-2} - q_i \times y_{i-1} \qquad (4)$$

Euler’s Totient Function

Before presenting Euler’s theorem, we need to introduce an important quantity in number theory, referred to as **Euler’s totient function**. This function, written $\phi(n)$, is defined as the number of positive integers less than n and relatively prime to n. By convention, $\phi(1) = 1$.

DISCRETE LOGARITHMS

For the prime number 19, its primitive roots are 2, 3, 10, 13, 14, and 15.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

1.2 RSA Algorithm

The Rivest-Shamir-Adleman (RSA) scheme has since 1977 is the most widely accepted and implemented general-purpose approach to public-key encryption.

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

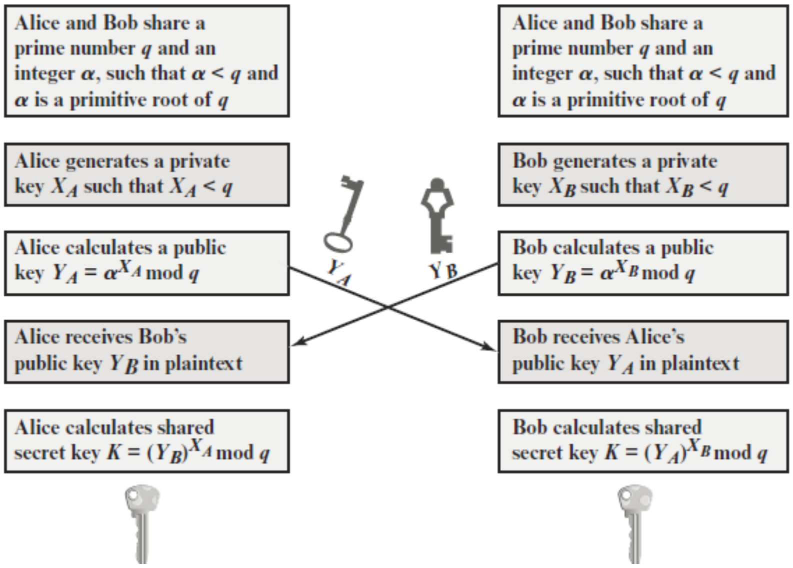
Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Example:

P=17; q=11 Find public and private keys? Find the cipher M=88?

1.3 DIFFIE–HELLMAN KEY EXCHANGE



Example:

q= 353; a=3; XA=97; XB=233; find the shared key ?

1.4 ELGAMAL CRYPTOGRAPHIC SYSTEM

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice	
Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$\{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

Thus, K functions as a one-time key, used to encrypt and decrypt the message.

For example, let us start with the prime q = 19. It has primitive roots {2, 3, 10, 13, 14, 15}. We choose a = 10. Alice generates a key pair as follows:

1. Alice chooses XA = 5.
2. Then $YA = a^{XA} \bmod q = a^5 \bmod 19 = 3$
3. Alice's private key is 5 and Alice's public key is {q, a, YA} = {19, 10, 3}.

Suppose Bob wants to send the message with the value M = 17. Then:

1. Bob chooses k = 6.
2. Then $K = (YA)^k \bmod q = 3^6 \bmod 19 = 729 \bmod 19 = 7$.
3. So

   $C1 = a^k \bmod q = a^6 \bmod 19 = 11$

   $C2 = KM \bmod q = 7 * 17 \bmod 19 = 119 \bmod 19 = 5$
4. Bob sends the ciphertext (11, 5).

For decryption:

1. Alice calculates $K = (C1)^{XA} \bmod q = 11^5 \bmod 19 = 161051 \bmod 19 = 7$.
2. Then K^{-1} is $7^{-1} \bmod 19 = 11$.
3. Finally, $M = (C2K^{-1}) \bmod q = 5 * 11 \bmod 19 = 55 \bmod 19 = 17$.