[Part 2]
Asymmetric-Key Encipherment

Chapter 9

Mathematics of Cryptography

Forouzan, B.A. Cryptography and Network Security (International Edition). United States: McGraw Hill, 2008.

- To introduce prime numbers and their applications in cryptography;
- To discuss some primality test algorithms and their efficiencies;
- To discuss factorization algorithms and their applications in cryptography;
- To describe the Chinese remainder theorem and its applications;
- To introduce quadratic congruence;
- To introduce modular exponentiation and logarithm.

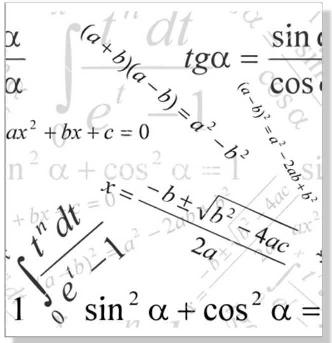
- To introduce prime numbers and their applications in cryptography;
- To discuss some prime applications including Euler's phi-function, Fermat's theorem and Euler's theorem;
- To discuss the Fermat's and Euler's theorems as the multiplicative inverse application.

Contents

Contents

9.1 Introduction

- This chapter reviews some mathematical background concept needed for understanding the asymmetric-key or public-key cryptography.
- The primes is one of the mathematical concept uses in this cryptography extensively.



https://cdn.vectorstock.com/i/composite/82,07/seamless-mathematical-pattern-vector-978207.jpg

9.1 Introduction

- Two theorems that play important roles in asymmetric-key cryptography are Fermat's and Euler's theorem.
- An important requirement in a number of cryptography algorithms is the ability to choose a large prime number.
- Discrete logarithms are fundamental to a number of asymmetric-key algorithms, but it operates over modular arithmetic.

Stalling, W. Cryptography and Network Security: Principles and Practices (Fourth Edition). United States of America: Pearson, Prentice Hall, 2006. (page 235)

Contents

Introduction

- The primes is one of the mathematical concept uses in asymmetric-key or public-key cryptography extensively.
- The topic is a large part of any book on number theory.

https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcQ6GWq_MOpWSU4w84vyLQxUKmEIAMirZmnGS9mvA07qNheOSMk3nA

Definition

- Primes is the positive integers can be divided into three groups.

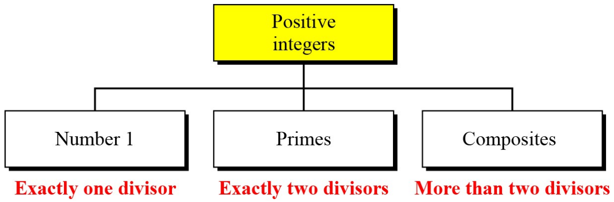
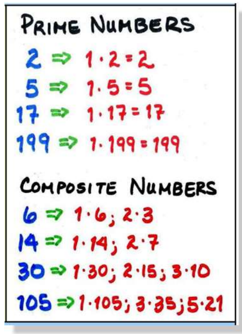


Figure: Three groups of positive integers.

A prime is divisible only by itself and 1.

- A positive integer is a prime *if and only if* it is exactly divisible by two integers: 1 and itself.
- A composite is a positive integer with more than two divisors or it can be factored into two or more values other than one (1) and itself.



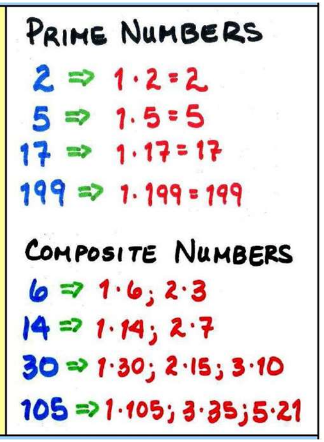
http://shanahan1.pbworks.com/f/1253699479/prime_composite.jpg

Example 9.1 What is the smallest prime?

Solution 9.1: Integer 2, which is divisible by 2 (itself) and 1.

Note - Integer 1 is not a prime because it cannot be divisible by two different integers but only by itself.

1. Prime Numbers are values that can only be factored into one (1) and itself.
2. Composite Numbers are values that can be factored into two or more values other than one (1) and itself.



http://shanahan1.pbworks.com/f/1253699479/prime_composite.jpg

Example 9.1: List the primes smallest than 10.

Solution 9.1: There are four primes less than 10: 2, 3, 5, and 7.

- It is interesting to note that the percentage of primes in the range 1 to 10 is 40%.
- The percentage decreases as the range increases.

Example 9.1: List the primes between 1 to 30.

Solution 9.1: There are ten primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29.

- the percentage of primes is 33.3%.

Cardinality of primes

- Now, two questions naturally arise:
  - *Is there a finite number of primes?*
  - *Is the list infinite?*

- Given a number n, how many primes are smaller than or equal to n?

Infinite Number of Primes

Here is an informal proof.

•Suppose the set of primes is finite (limited), with p as the largest prime.
•Multiply the set of primes become $P = 2 \times 3 \times \cdots \times p$
•The integer $(P+1)$ cannot have a factor $q \leq p$.
•If q also divides $(P+1)$, then q divides $(P+1) - P = 1$
•The only number that divides 1 is 1, which is not a prime.
•Therefore, q is larger than p.

There is an infinite number of primes.

Example 9.2 Assume that the only primes are in the set $\{\ 2, 3, 5, 7, 11, 13, 17\ \}$. If $P = 510510$, how many more primes are not in the set?

Solution 9.2: $P + 1 = 510511$

However, $510511 = 19 \times 97 \times 277$; none of these primes were in the original list.

Therefore, there are three primes greater than 17.

Number of Primes

- To answer the second question, a function called $\pi(n)$ is defined that finds the number of primes smaller than or equal to n.
- The following shows the values of this function for different n's.

$$\pi(1)=0 \quad \pi(2)=1 \quad \pi(3)=2 \quad \pi(10)=4$$
$$\pi(20)=8 \quad \pi(50)=15 \quad \pi(100)=25$$

- But if n is very large, we can use an approximation as:

$$[n/(\ln n)] < \pi(n) < [n/(\ln n - 1.08366)]$$

(Lagrange) (Gauss)

Example 9.3 Find the number of primes less than 1,000,000.

Solution 9.3: The approximation gives the range 72,383 to 78,543. The actual number of primes is 78,498.

Example 9.3 Find the number of primes less than 1,000,000.

Solution 9.3: The approximation gives the range 72,383 to 78,543. The actual number of primes is 78,498.

$$[n/(\ln n)] < \pi(n) < [n/(\ln n - 1.08366)]$$
$$[n/(\tfrac{1}{n})] < \pi(n) < [n/(\tfrac{1}{n} - 1.08366)]$$
$$[1000000/(\tfrac{1}{1000000})] < \pi(n) < [1000000/(\tfrac{1}{1000000} - 1.08366)]$$
$$[10^6/(10^{-6})] < \pi(n) < [10^6/(10^{-6} - 1.08366)]$$
$$[10^6 \times 10^6] < \pi(n) < [10^6/(-1.08359)]$$

Checking for Primeness

- The next question that : given a number n, how we can determine if n is a prime?
- The answer is that we need to see if the number is divisible by all primes less than $\sqrt{n}$

Theorem

If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof.

- Let $n = ab$, $1 < a < n$, $1 < b < n$.
- We can't have both $a > \sqrt{n}$ and $b > \sqrt{n}$ since this would lead to $ab > n$.
- Therefore, n must have a prime divisor less than or equal to $\sqrt{n}$.

$\square$

Example 9.4 Is 97 a prime integer?

Solution 9.4: The floor of $\sqrt{97} = 9$

- The primes less than 9 are 2, 3, 5, and 7.
- We need to see if 97 is divisible by any of these numbers.
- It is not, so 97 is a prime.

Example 9.5 Is 301 a prime integer?

Solution 9.5: The floor of $\sqrt{301} = 17$

- We need to check 2, 3, 5, 7, 11, 13, and 17.
- The numbers 2, 3, and 5 do not divide 301, but 7 does (7 x 43 = 301).
- Therefore 301 is not a prime.

Sieve of Eratosthenes

- A method method to find all primes less than n by a Greek mathematician, Eratosthenes.

Example 9.6 Suppose we want to find all primes less than 100.

- We write down all the numbers between 2 and 100.
- Because $\sqrt{100} = 10$, we need to see if any number less than 100 is divisible by 2, 3, 5 and 7.

Solution 9.6:

Table 9.1 *Sieve of Eratosthenes*

	2	3	4	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Solution 9.6: The following shows the process:

1. Cross out all numbers divisible by 2 (except 2 itself)
2. Cross out all numbers divisible by 3 (except 3 itself)
3. Cross out all numbers divisible by 5 (except 5 itself)
4. Cross out all numbers divisible by 7 (except 7 itself)
5. The numbers left over are primes.

Contents

- Notation: $\phi(n)$
- Sometimes known as Euler's totient function play a very important role in cryptography.
- The function finds the <u>number of integers</u> that are both smaller than n and relatively prime to n.
- The function $\phi(n)$ calculates the number of elements in this set.

- The following rules help to find the value of $\phi(n)$

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

- These four rules can be combined to find the value of $\phi(n)$
- **<u>Example</u>**: if n can be factored as $n = p_1^{e1} \times p_2^{e2} \times \ldots \times p_k^{ek}$ then we combine the third and fourth rules to find

$$\phi(n) = (p_1^{e1} - p_1^{e1-1}) \times (p_2^{e2} - p_2^{e2-1}) \times \ldots \times (p_k^{ek} - p_k^{ek-1})$$

The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of n.

Example 9.7 What is the value of $\phi(13)$?

Solution 9.7: (Second rule)
Because 13 is a prime, $\phi(13) = (13-1) = 12$

Example 9.8 What is the value of $\phi(10)$?

Solution 9.8: (Third rule) Because 2 and 5 are a primes.

$$\begin{aligned}\phi(10) &= \phi(2) \times \phi(5)\\ &= (2-1) \times (5-1)\\ &= 1 \times 4 = 4\end{aligned}$$

Example 9.9 What is the value of $\phi(240)$?

Solution 9.9: We can write $240 = 2^4 \times 3^1 \times 5^1$

Then,
$$\begin{aligned}\phi(240) &= (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0)\\ &= (16-8) \times (3-1) \times (5-1)\\ &= 8 \times 2 \times 4 = 64\end{aligned}$$

Example 9.1 Can we say that $\phi(49) = \phi(7) \times \phi(7)$
$= (7-1) \times (7-1)$
$= 6 \times 6 = 36$

Solution 9.10:
- No. Because third rule applies when m and n are relatively prime.
- (Fourth rule) Here $49 = 7^2$

$$\phi(49) = \phi(7^2)$$
$$= 7^2 - 7^{2-1}$$
$$= 49 - 7 = 42$$

Example 9.1 What is the number of elements in $Z_{14}*$?

Solution 9.11:
- (Third rule) $\phi(14) = \phi(7) \times \phi(2)$
$= (7-1) \times (2-1)$
$= 6 \times 1 = 6$
- The numbers are 1, 3, 5, 9, 11 and 13.

Interesting point: If $n > 2$, the value of $\phi(n)$ is even.

Exercise 9.1 Find the value of the following $\phi(n)$.

a) $\phi(29)$

b) $\phi(32)$

c) $\phi(80)$

d) $\phi(100)$

e) $\phi(101)$

Solution 9.1: a) $\phi(29) = 28$

b) $\phi(32) = 16$

c) $\phi(80) = 32$

d) $\phi(100) = 40$

e) $\phi(101) = 100$

Contents

9.4 Fermat's Little Theorem

- Plays a very important role in number theory and cryptography.
- Sometime helpful for quickly finding a solution to some exponentiations.
- Two version of the theorem:

$a^{p-1} \equiv a \bmod p$	$a^{p} \equiv a \bmod p$
• If p is a prime and a is an integer such that p does not divide a.	• Remove the condition on a. • If p is a prime and a is an integer.

9.4 Fermat's Little Theorem

Example 9.12 Find the result of 6^{10} mod 11.

Solution 9.12
- We have 6^{10} mod 11 = 1.
- This is the first version of Fermat's little theorem where p = 11.

Example 9.13 Find the result of 3^{12} mod 11.

Solution 9.13
- Here the exponent (12) and the modulus (11) are not the same.
- With substitution, this can be solved using Fermat's little theorem.

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)(3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

9.4 Fermat's Little Theorem

Multiplicative Inverses

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

→ A very interesting application of Fermat's theorem in finding some multiplicative inverses quickly if the modulus is a prime.

- p is a prime and a is an integer.

Example 9.14 The answers to multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$
b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$
c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$
d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

Exercise 9.2: Find the result of the following, using Fermat's little theorem:

a) 5^{15} mod 13

b) 5^{18} mod 17

c) 456^{17} mod 17

d) 145^{102} mod 101

Solution 9.2: Find the result of the following, using Fermat's little theorem:

a) 5^{15} mod 13

b) 5^{18} mod 17

c) 456^{17} mod 17

d) 145^{102} mod 101

Exercise 9.3: Find the result of the following, using Fermat's little theorem:

a) 5^{-1} mod 13

b) 15^{-1} mod 17

c) 27^{-1} mod 41

d) 70^{-1} mod 101

(Note that all moduli are primes)

Solution 9.3: Find the result of the following, using Fermat's little theorem:

a) 5^{-1} mod 13

b) 15^{-1} mod 17

c) 27^{-1} mod 41

d) 70^{-1} mod 101

(Note that all moduli are primes)

Chapter 9 Contents

Chapter 9 9.5 Euler's Theorem

- Can be thought of as a generalization of Fermat's Little theorem.
- The modulus in Fermat's theorem is a *prime*, while Euler's theorem is an *integer*.
- Two version of this theorem:

$a^{\phi(n)} \equiv 1(\bmod n)$	$a^{k\times\phi(n)+1} \equiv a(\bmod n)$
• If a and n are coprime.	• Remove the condition that a and n should be coprime. • If $n = p$ x q, $a < n$, and k an integer.

Chapter 9 9.5 Euler's Theorem

This version will be used in the RSA cryptosystem

Euler's Theorem

$$a^{k\times\phi(n)+1} \equiv a(\bmod n)$$

Advantage(s):

•Euler's theorem is very useful for solving some problems.

•It sometimes is helpful for quickly finding a solution to some **exponentiations**.

Chapter 9 9.5 Euler's Theorem

Proof of the second version based on the first version.

- Since $a < n$, three cases are possible:

Example 9.1 Find the result of 6^{24} mod 35.

Solution 9.15: We have 6^{24} mod 35 = $6^{\phi(35)} \bmod 35 = 1$

Example 9.1 Find the result of 20^{62} mod 77.

$\phi(77) = \phi(7) \times \phi(11)$
$= (7-1) \times (11-1)$
$= (6) \times (10) = 60$

Solution 9.16:
- Let $k = 1$ on the second version;
- We have 20^{62} mod 77 $= 20^{1\times\phi(77)+1} \bmod 77$

$= (20 \bmod 77)(20^{60+1} \bmod 77)$

$= (20)(1)(20) \bmod 77 = 15$

$20^{\phi(77)} \bmod 77 = 1$
$20^{60} \bmod 77 = 1$

Chapter 9 9.5 Euler's Theorem

Multiplicative Inverses

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

- Euler's theorem can be used to find multiplicative inverses modulo a **prime** or a **composite**.
- n and a are coprime.

Example 9.1 The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the composite:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$
b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$
c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$
d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$

Chapter 9 9.5 Euler's Theorem

Exercise 9.4 Find the result of the following, using Euler's theorem:

a) $12^{-1} \bmod 77$

b) $16^{-1} \bmod 323$

c) $20^{-1} \bmod 403$

d) $44^{-1} \bmod 667$

(Note that 77 = 7 x 11, 323 = 17 x 19, 403 = 31 x 13, and 667 = 23 x 29)

Chapter 9 9.5 Euler's Theorem

Solution 9.4: Find the result of the following, using Euler's theorem:

a) $12^{-1} \bmod 77$

b) $16^{-1} \bmod 323$

c) $20^{-1} \bmod 403$

d) $44^{-1} \bmod 667$

(Note that 77 = 7 x 11, 323 = 17 x 19, 403 = 31 x 13, and 667 = 23 x 29)

Contents

9.6 Summary

- The integers can be divided into three groups:
  - the number 1,
  - primes, and
  - composite.
- Euler's phi-function, $\phi(n)$, which is sometimes called Euler's totient function, plays a very important role in cryptography.
- Euler's phi-function finds the number of integers that are both smaller than n and relatively prime to n.

9.6 Summary

Table: Fermat's little theorem and Euler's theorem.

Fermat	**First version:**	If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod p$
	Second version:	$a^p \equiv a \pmod p$
Euler	**First version:**	If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$
	Second version:	If $n = p \times q$ and $a < n$, then $a^{k \times \phi(n)+1} \equiv a \pmod n$

9.6 Summary

- In cryptography, a common modular operation is exponentiation.
- Cryptography also involves modular logarithms.
- If exponentiation is used to encrypt or decrypt, the adversary can use logarithms to attack.
- Therefore, we need to know how hard it is to reverse the exponentiation.