MONASH University
Information Technology

FIT2093 INTRODUCTION TO CYBER SECURITY

MONASH University
Information Technology

FIT2093 INTRODUCTION TO CYBER SECURITY

Lecture 5:
Introduction to Number Theory

Unit Structure

- Introduction to security of
- Authentication
- Access Control Fundamental
- Fundamental concepts of cryptography
- Symmetric encryption techniques
- Introduction to number theory
- Public key cryptography
- Integrity management
- Practical aspects of cyber security
- Hacking and countermeasures
- Database security
- IT risk management & Ethics and privacy

Previous Lecture

- **Cryptography.**
  - Classical
    - > transposition, substitution
  - Modern Private key
    - > DES, triple DES
    - > AES
- **Properties of Cryptographic ciphers**
- **Attacking Symmetric Encryption**
  - Cryptanalysis & brute force
- **Block & Stream cipher**
- **Modes of Operation**
  - ECB, CBC, CFB, OFB, CTR

Objectives

- **Understand the definition of**
  - Prime number
  - Composite number
  - Relative primes
- **Understand the idea of factorisation.**
- **Understand modulo arithmetic and their properties for use in cryptography.**

Integer

- **A whole number, eg 1, 5, -2, 100, etc.**

Property	addition	multiplication
Closure	a+b is an integer	a * b is an integer
Associative	(a+b)+c = a+(b+c)	(a*b)*c=a*(b*c)
Commutative	a+b=b+a	a*b=b*a
Existence of an identity element	a+0=a	a*1=a
Existence of inverse element	a+(-a)=0	a*1/a=1
Distributive	a*(b+c) = (a*b)+(a*c)	
No zero divisor	If a * b=0, then either a=0, or b=0 or both=0	

Prime and Composite Numbers

- **Prime number**
  - is a number that has exactly two (distinct) divisors, which are 1 and the (prime) number itself.
  - Example: 2, 3, 7, 11
- **Composite number**
  - A number that has at least one positive divisor other than 1 and itself.
  - Example: 4 has 1, 2 and 4 as possible divisors.
- **Number 0 and 1 are special numbers. They are not considered as prime or composite numbers.**

Prime Numbers

- **List of prime numbers less than 200**

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53
  59 61 67 71 73 79 83 89 97 101 103 107 109
  113 127 131 137 139 149 151 157 163 167 173
  179 181 191 193 197 199

- **Note the way the primes numbers are distributed in the first 1-200 integers**

Factor or Divisor

- **An integer *x* is called a factor of an integer *n*, if *n* can be divided by *x* without leaving a remainder.**
  - x can divide n exactly without any remainder
- **Examples:**
  - 2 is a factor of 4 because 4 / 2=2(quotient), remainder 0.
  - 2 is not a factor of 9 because 9 / 2 = 4 (quotient) and remainder = 1.
- **Trivial factor or divisor**
  - A trivial divisor of an integer *n* is number 1 and the number *n* itself.

Factor or Divisor

- **Non-trivial divisor**
  - A non-trivial divisor of an integer *n* is the number(s) other than the trivial divisors.
  - Example: For number 6, 1 and 6 are the trivial divisors, 2 and 3 are non-trivial divisors.
  - Smallest non-trivial divisors are those that are also prime numbers – called prime factors.
  - Example: For number 6, 2 and 3 are non-trivial divisors and also prime factors.

Prime number
is a number that has exactly two (distinct) divisors, which are 1 and the (prime) number itself

A trivial divisor of an integer *n* is number 1 and the number *n* itself.

Integer Factorisation

- **Factorisation is the process of breaking down a composite number into smaller non-trivial divisors, which when multiplied together equal the original integer.**
- **Example:**
  - 6=2x3
  - 12=2x2x3
  - 18=2x3x3

Prime Factorisation

- to **factor** a number `n` is to write it as a product of other numbers: `n=a x b x c`
- note that factoring a number is relatively hard compared to multiplying the factors together to generate the number
- the **prime factorisation** of a number `n` is when it is a product of primes
  - eg. `91 = 7x13 ;`
  - $3600 = 4 \times 9 \times 4 \times 25 = 2^2 \times 3^2 \times 2^2 \times 5^2 = 2^4 \times 3^2 \times 5^2$
- There are a number of algorithms to find all the prime factors of an integer.

Finding all Prime Factors - Factorisation Algorithms

- **Trial Division**
  - Given a composite number *n*, divide *n* by every prime number less than $\sqrt{n}$
  - Can be difficult for large numbers.
    - > Large division
    - > Need to know all the prime numbers ≤ $\sqrt{n}$.
- **Other famous algorithms**
  - Fermat's factorization methods
  - Pollard's rho p-1 algorithm.

- **Prime factorisation is computationally expensive (or time consuming) and can form a good basis if you want to hide your information if it requires factorisation for decoding!!**

Greatest Common Divisor

- **A Greatest Common Divisor (GCD) or greatest common factor is the largest positive integer that can divide two or more integer numbers without leaving a remainder.**
- **Example:**
  - GCD of numbers 6 and 9
    - > 6 = 2 x 3
    - > 9 = 3 x 3
    - > The largest common factor = 3 = GCD(6, 9)
  - GCD of integers 48 and 64
    - > 48 = 2 x 2 x 2 x 2 x 3 = 16 x 3 = 8 x 6 = 4 x 12 = 2 x 24
    - > 64 = 2 x 2 x 2 x 2 x 2 x 2 = 8 x 8 = 16 x 4 = 32 x 2
    - > GCD (48, 64) = 16

Relative Prime or Coprime

- **Two numbers are considered as relative prime if their greatest common divisor is 1.**
- **However each of the numbers need not necessarily to be a prime number.**
- **For example:**
  - 5 and 6 are relative primes
  - 6 and 9 are not relative primes because the GCD (6,9) = 3 as they can be divided by 3 without leaving any remainder.

Modular Arithmetic

- **It is also known as clock arithmetic**
  - Clock has 12 numbers, 13.00 hours = 1 PM.
- **Notations:**
  - a mod n = b ➔ b is the remainder of a / n.
  - 13 mod 12 = 1
    - > **13 with the operation of "modulus 12" has a remainder of 1.**
  - a ≡ b (mod n) ➔ we can omit n if it is understood implicitly.
  - 13 ≡ 1 (mod 12)
    - > **13 is a congruent class of 1 in modulo 12.**
    - > **13 and 1 occupy the same position in the 12-hrs clock.**
- **Examples**
  - 25 mod 12 = 1, 25 ≡ 1 (mod 12)
  - 9 mod 3 = 0, 9 ≡ 0 (mod 3)
  - 10 mod 3 = 1, 10 ≡ 1 (mod3)
- **Two integers a and b are said to be congruent modulo n, if**
  - (a mod n) =(b mod n).

Modular Addition

- **Let c and d be two integer numbers, then what is the value of (c+d) in modulo n?**

  (c+d) mod n =(c mod n + d mod n) mod n.

- **Example:**
  - (2 + 14) mod 12 = ?
  - It can be calculated as:
    - > 16 mod 12 = 4
      - OR
    - > (2 mod 12 + 14 mod 12) mod 12 =(2 + 2) mod 12 = 4.

Modular Subtraction

- **Let c and d be two integer numbers, what is the value of c-d in modulo n?**
  - (c-d) mod n = (c mod n + (-d) mod n) mod n
- **In a clock, positive refers to clockwise turn, and the negative refers to the anti-clockwise turn.**
- **Example:**

  (2 – 18) mod 12 = ?

  Can be calculated as

  -16 mod 12 = - 4

  OR

  (2 mod 12 + (-18) mod 12) mod 12 = (2 + (-6)) mod 12 = -4.

Modular Multiplication

- **Let c and d be two integer numbers, what is the value of c*d modulo n?**
- **Multiplication can be thought of as a repeated additions.**
- **Example:**

  (5 * 14) mod 12 =?

  Can be calculated as:

  70 mod 12 = 10

  OR

  (5 mod 12 * 14 mod 12) mod 12 = (5 * 2) mod 12 = 10

Modular Division

- **Let c and d be two integer numbers, what is the value of c/d modulo n?**
- **The problem is usually solved using the expression:**
  – dx = c mod n
  – We need to find x.
- **It is possible that:**
  – There is no value that satisfy x.
  – x is not a unique value.
  – x is a unique value.
- **There exists mathematical methods to find x. (outside the scope in this unit).**

Modular Arithmetic Properties

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z = 0 \bmod n$

Integer Exponentiation

- **Exponentiation is a mathematical operation, written a^n, involving two numbers, the base a and the exponent n. When n is a positive integer, exponentiation corresponds to n times multiplication of a.**

exponent

$$\underset{\text{base}}{a^n} = a \times a \underbrace{\times a \times a \times a \times \ldots \times a}_{\text{n times}}$$

Modular Exponentiation

- **Type of exponentiation performed over modulus.**
- **Notation:**

  $a^e \bmod n = b$

  $b \equiv a^e \pmod{n}$
- **Examples:**
  - $3^3 \bmod 12 = 27 \bmod 12 = 3$
  - $4^2 \bmod 10 = 16 \bmod 10 = 6$
- **Finding the value of b is relatively easy even when *a* and/or *e* are/is large.**
- **However, finding the value of *e* given *a, b* and *n* is time consuming.**
- **This can form a good basis if you want to hide your information. May be treat the information an integer (how?) and perform a modular exponential and store it, then decoding will be difficult according to the above property.**

Multiplicative Inverse

- **The multiplicative inverse of a number *x*, denoted 1/*x* or x^{-1}, is the number which, when multiplied by *x*, yields 1.**
- **Examples:**
  - 0.2 is multiplicative inverse of 5 => 0.2 * 5 = 1.
  - What is the multiplicative inverse of
    - > 4?
    - > 0.8?
- **The idea of multiplicative inverse can be used for encrypting and decrypting message.**

Euler Totient function **ø(n)**

- **The Euler Totient *ø(n)* of a positive integer *n* is defined to be the number of positive integers less than or equal to *n* that are relative prime or coprime to *n* (*see slide no: 15*)**
  - *Numbers below n that are coprime with n (= no of factors that has a GCD of 1).*

Euler's Totient Function ø(n)

- **Example for ø (10)**
- **complete set of residues for n is : `0..n-1`**
  - all numbers less than n
- **reduced set of residues consists of those numbers (residues) which are relatively prime to n = ø(n)**
  - n=10,
  - complete set of residues is {0,1,2,3,4,5,6,7,8,9}
  - reduced set of residues is {1,3,7,9}
- **number of elements in reduced set of residues is called the Euler Totient Function ø(n)**
  - ø(10) = 4

Prime Numbers and Modular Arithmetic (1)

- **Let ø(*n*) denote the total numbers that are *less than n* and relatively prime to *n.***
  - **If *n* is a prime number, then ø(*n*) = *n* – 1**
  - Example:
    - > Let Xn be the set of relative primes of n that is less than n,
    - > n=3, ø(3) = 3-1 = 2, Xn = {1,2}
    - > n=5, ø(5) = 5-1 = 4, Xn = {1,2,3,4}

Prime Number and Modulo Arithmetic (2)

- **If *p*, *q* are prime numbers and *n*=*p**q*, then**
  - **Ø(*n*) = Ø(*p**q*) = (*p*-1)*(*q*-1) = *p**q* – (*p* + *q* -1)**
    - > *p* & *q* are prime numbers => only multiples of *p* and *q* are **not** relatively prime to p*q ;
    - > Number of integers < pq = [pq – 1];
    - > Residues **not** relatively prime to pq= [p, 2p, 3p..(q-1)p]+[q,2q, 3q…(p-1)q]
    - > Number of residues **not** relatively prime to pq = (q-1+p-1)
    - > That is: there are (*p* + *q* – 2) multiples of *p* and *q*
    - > *ø*(*p**q*)=pq-1-(p+q-2)=(p-1)(q-1)
- **Example:**
  - *p* = 3; *q*=7; => {0, 0, 3, 6, 7, 9, 12, 14, 15, 18} are not relatively prime to *p**q*
  - Ø(*n*) = *ø*(*p**q*) = (3-1)*(7-1)=12 ; Xn= {1,2,4,5,8,10,11,13,16,17,19,20}

Prime Number and Modulo Arithmetic (3)

- ***y* & *n* are relatively prime integers and *y* (mod ø(*n*)) = 1, for any M < *n*, then**

  M^y mod n = M

  – e.g:

  > y=13 ; n=7; M = 2 or 4 (2 examples are shown here);

  > ø(n) = 6; y mod ø(n) = 13 mod 6 = 1;

  > M^y = 2^{13}; M^y mod n = 2^{13} mod 7 = 2^3x2^3x2^3x2^3x2 mod 7
  = 8X8X8X8X2 mod 7 = 2 mod 7
  = 2 = M mod n;

  > M^y = 4^{13}; M^y mod n = 4^{13} mod 7 = 4^3x4^3x4^3x4^3x4 mod 7=
  64x64x64x64x4 mod 7 = 4 = M mod n;

= n-1 since n=7 is prime

MONASH University
Information Technology

Look at this → $M^y \bmod n = M$ *(from the previous slide)*

- Let y = a *b, then

$a^* b = 1 \bmod ø(n)$

$$M^y \bmod n = M$$
$$= M^{a^* b} \bmod n$$
$$= M \quad \text{if} \quad a^* b \bmod ø(n) = 1$$

- a & b are multiplicative inverse in modulo ***ø(n)*** arithmetic.

Multiplicative Inverse in Modular Arithmetic

- **If a and b are multiplicative inverse in modulo n, then we have**
  (a * b) mod n = 1
- **e.g: Let n=10, a = 3; b = 7;**
  - Are a and b multiplicative inverse under mod 10?
  - Yes, because 3 * 7 = 21 mod 10 = 1
  - But a = 4 and b = 7 is not because 4 * 7 = 28 mod 10 = 8

Putting it together – Remember the following!

- **From slide 13**
  - Prime factorisation is computationally expensive (or time consuming) and can form a good basis if you want to hide your information if it requires factorisation for decoding!!
- **From slide 23**
  - $a^e \bmod n = b$
  - However, finding the value of *e* given *a, b* and *n* is time consuming.
- **From slide 30**
  - $M^{a*b} \bmod n = M$ if $a * b = 1 \bmod ø(n)$

$a * b = 1 \bmod ø(n)$

Putting together – Remember the following!

- **From slide 30**
  - $M^{a*b} \bmod n = M$ if $a*b = 1 \bmod ø(n)$
- **If message/data M need to be protected, transform M as $M^a \bmod n$ and store it and to get it back, do $(M^a)^b = M \bmod n$**
- Not knowing b, it will be difficult to get M from M^a.
  - Due to the previous observation that if $a^e \bmod n = b$; then finding the value of *e* given *a, b* and *n* is time consuming

Lesson that you learn from the previous slide are:

- **Choose a number which is a product of at least 2 or more prime numbers so that finding those numbers from the product is time consuming.**
- **If you need to store an information securely, then transform the information with an exponentiation operation so that it is difficult to guess the exponent.**
- **To get back to the original information, do an exponentiation with the corresponding inverse!**

Summary

- **Prime number**
- **Coprime or relative prime**
- **Modular arithmetic / clock arithmetic**
- **Modular arithmetic properties.**
- **Euler' s Totient**
- **Prime number and modulo arithmetic**

Further Reading

- **Appendix B: "*Some aspects of number theory*"**
- **The textbook: *Computer Security: Principles and Practice*" *by William Stallings & Lawrie Brown,* Prentice Hall, 2015**

- **Acknowledgement: part of the materials presented in the slides was developed with the help of Instructor's Manual and other resources made available by the author of the textbook.**