CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 13.2

NUMBER THEORY & RSA

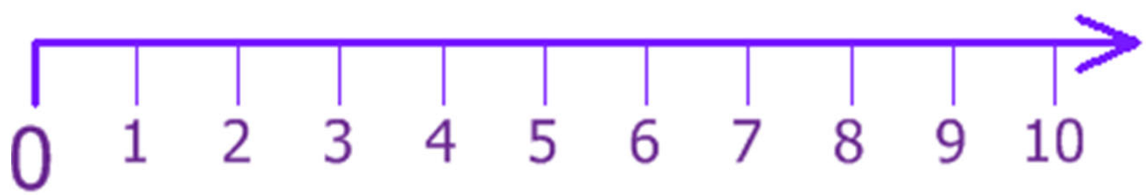
Last Updated: 22/11/2020

2

Number Theory for Asymmetric Key Cryptosystem

Whole Numbers

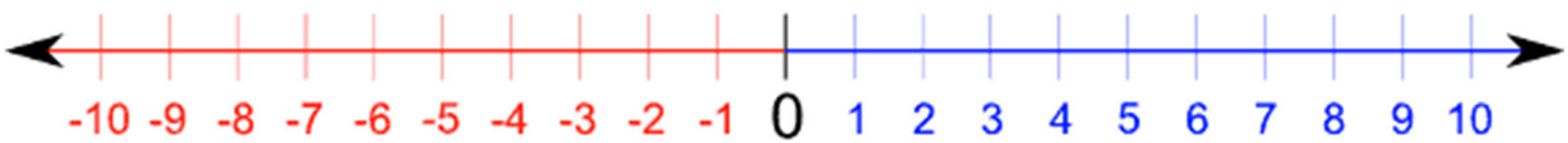
- Whole Numbers are simply the numbers 0, 1, 2, 3, 4, 5, ... (and so on).
- No Fractions.
  - Numbers like ½, 1.1 and 3.5 are not whole numbers.



Source: Whole Numbers and Integers- Math is Fun
http://www.mathsisfun.com/whole-numbers.html

Integers

- Integers are like whole numbers, but they also include negative numbers.
- No Fractions.
  - Numbers like ½, 1.1 and 3.5 are not integers.



Prime Numbers

- A Prime Number is a whole number greater than 1, which can be divided evenly only by 1, or by itself.
- Example:
  - The first few prime numbers
    - 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29…
    - For more prime numbers: Prime Numbers Chart
  - 5 can only be divided evenly by 1 or 5, so it is a prime number.
  - 6 can be divided evenly by 1, 2, 3 and 6 so it is NOT a prime number

Source: Definition of Prime Number - Math is Fun
www.mathsisfun.com/definitions/prime-number.html

Composite number

- A composite number is a whole number greater than 1, which is not a prime number.

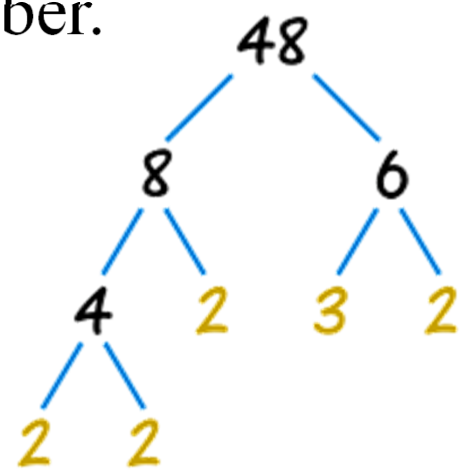
Or

- A composite number is a whole number greater than 1, which can be divided evenly by numbers other than 1 or itself.
- Example:
  - First few composite numbers
  - 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, and 24…

Source: Definition of Composite Number - Math is Fun
http://www.mathsisfun.com/definitions/composite-number.html

Prime Factorization

- "Prime Factorization" is finding which prime numbers multiply together to make the original composite number.
- There is only one (unique!) set of prime factors for any composite number.
  - Example:



$48 = 2 \times 2 \times 2 \times 2 \times 3$ Or $48 = 2^4 \times 3$

Source: Prime Factorization - Math is Fun
http://www.mathsisfun.com/prime-factorization.html

Greatest Common Divisor (GCD)

- Also known as Greatest Common Factor (GCF)
- GCD of two or more integers, when at least one of them is not zero, is the largest positive integer that divides the numbers without a remainder.
- Example:
  - gcd(24, 108) = 12
    - Prime factorization of 24 = $2 \times 2 \times 2 \times 3$
    - Prime factorization of 108 = $2 \times 2 \times 3 \times 3 \times 3$
    - The prime factors $2 \times 2 \times 3$ are common for both 24, 108
    - Therefore gcd(24, 108) = $2 \times 2 \times 3 = 12$
  - Easier way to calculate gcd: Euclidean Method – next slide

Euclidean Method to calculate GCD of two numbers

- Example: gcd(24, 108)
- 108 = 4 x 24 + 12 [Note: Greater number (108) on the left]
- 24 = 2 x 12 + 0 [Note: When you hit 0 stop calculation]
- The reminder above 0 is the answer = 12
- Therefore gcd(24, 108) = 12

Relatively prime, or coprime numbers

- Two numbers are called relatively prime, or coprime, if their greatest common divisor equals 1.
- Example:
  - gcd(9, 28)
    - Euclidean method
      - 28 = 3 x 9 + 1
      - 9 = 9 x 1 + 0
    - gcd(9, 28) = 1
  - Therefore 9 and 28 are relatively prime numbers or coprime numbers
- NOTE: If any one of the two numbers is a prime number then the two numbers automatically become relatively prime or coprime numbers.

Extended Euclidean Method to calculate Inverse Modulo

- In modular arithmetic, the modular multiplicative inverse of an integer "a mod m" is an integer "y" such that
  - $a * y = 1 \bmod m.$

    $y = 1/a \bmod m$

    $y = a^{-1} \bmod m$
- The multiplicative inverse of "a mod m" exists if and only if "a" and "m" are coprime (i.e., if gcd(a, m) = 1)
- What is the inverse module of 19 mod 127?
  - $y = 19^{-1} \bmod 127$
  - How? Extended Euclidean Method

Knowledge Component

Extended Euclidean Method to calculate Inverse Modulo

Euclidean Method

- gcd(19, 127)
- 127 = 6 x 19 + 13
- 19 = 1 x 13 + 6
- 13 = 2 x 6 + 1
- 6 = 6 x 1 + 0

Extended Euclidean Method

- Write the reminders in terms of 19 and 127
- 13 = 127 + (-6) 19
- 6 = 19 + (-1) 13
- Substitute value of 13 in the above
- 6 = 19 + (-1)$\boxed{(127 + (-6) 19)}$
- 6 = 19 + (-1) 127 + (6) 19
- 6 = (-1) 127 + (7) 19
- 1 = 13 + (-2) 6
- Substitute value of 13 and 6 in the above
- 1 = 127 + (-6) 19 + (-2) ((-1) 127 + (7) 19)
- 1 = 127 + (-6) 19 + (2) 127 + (-14) 19
- 1 = (3) 127 + (-20) 19

Answer: y = -20 mod 127 = 107

19^{-1} mod 127 = 107

Check: 19 x 107 = 2033 mod 127 = 1 mod 127

Extended Euclidean Method to calculate Inverse Modulo

Video

Watch the following video on Extended Euclidean Method

- https://www.youtube.com/watch?v=fz1vxq5ts5I

Exercises

Extended Euclidean Method : Exercises

Using the extended Euclidean Method to find the inverse module of the followings:

- GCD (40,65)
- GCD (735,1239)

The RSA Cryptosystem

Knowledge Component

The RSA Cryptosystem

- Martin Hellman and Whitfield Diffie published their landmark public- key paper in 1976
- Ronald Rivest, Adi Shamir and Leonard Adleman proposed the asymmetric RSA cryptosystem in1977
- Until now, RSA is the most widely use asymmetric cryptosystem although elliptic curve cryptography (ECC) becomes increasingly popular
- RSA is mainly used for two applications
  - Transport of (i.e., symmetric) keys
  - Digital signatures

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

The RSA - Encryption and Decryption

- RSA operations are done over the integer ring Z_n (i.e., arithmetic modulo n), where $n = p * q$, with p, q being large primes
- Encryption and decryption are simply exponentiations in the ring

Definition

Given the public key $(n,e) = k_{pub}$ and the private key $d = k_{pr}$ we write

$$y = e_{k_{pub}}(x) \equiv x^e \bmod n$$

$$x = d_{k_{pr}}(y) \equiv y^d \bmod n$$

where x, y ε Z_{n}.

We call $e_{k_{pub}}()$ the encryption and $d_{k_{pr}}()$ the decryption operation.

- In practice x, y, n and d are very long integer numbers (≥ 1024 bits)
- The security of the scheme relies on the fact that it is hard to derive the „private exponent“ d given the public-key (n, e)

Source: “Understanding Cryptography”
by Christof Paar and Jan Pelzl

The RSA – Key Generation

- Like all asymmetric schemes, RSA has set-up phase during which the private and public keys are computed

Algorithm: RSA Key Generation

Output: public key: $k_{pub} = (n, e)$ and private key $k_{pr} = d$

1. Choose two large primes p, q
2. Compute $n = p * q$
3. Compute $\Phi(n) = (p-1) * (q-1)$
4. Select the public exponent $e \in \{1, 2, \ldots, \Phi(n)-1\}$ such that gcd$(e, \Phi(n)) = 1$
5. Compute the private key d such that $d * e \equiv 1 \bmod \Phi(n)$
6. **RETURN** $k_{pub} = (n, e), k_{pr} = d$

Remarks:

- Choosing two large, distinct primes p, q (in Step 1) is non-trivial
- gcd$(e, \Phi(n)) = 1$ ensures that e has an inverse and, thus, that there is always a private key d

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Example: RSA with small numbers

ALICE

Message $x = 4$

BOB

1. Choose $p = 3$ and $q = 11$
2. Compute $n = p * q = 33$
3. $\Phi(n) = (3-1) * (11-1) = 20$
4. Choose $e = 3$
5. $d \equiv e^{-1} \equiv 7 \bmod 20$

$\xleftarrow{K_{pub} = (33,3)}$

$y = x^e \equiv 4^3 \equiv 31 \bmod 33$

$\xrightarrow{y = 31}$

$y^d = 31^7 \equiv 4 = x \bmod 33$

Integer Factorization Problem

- The most efficient means known to solve the RSA problem is to first factor the "*n*", which is believed to be impractical if "*n*" is sufficiently large
- Several researchers concluded in 2009, factoring a 232-digit number (768 bits), utilizing hundreds of machines over a span of two years.
- Refer: RSA Numbers

Exercises

RSA: Exercises

- $p = 11$, $q = 3$, $d = 7$ $C=3$
  - $n = ?$
  - $\varphi(n) = ?$
  - $d = ?$
  - Plaintext (P) = ?
- $p = 5$, $q = 11$, $e = 3$ $P=4$
  - $n = ?$
  - $\varphi(n) = ?$
  - $d = ?$
  - Ciphertext (C) = ?
- $p = 5$, $q = 7$, $e = 5$ $P=17$
  - $n = ?$
  - $\varphi(n) = ?$
  - $d = ?$
  - Ciphertext (C) = ?

Summary

Summary

- You learnt
  - Prime factorization & Greatest Common Divisor (GCD)
  - How Euclidean Method can be used to calculate GCD of two numbers
  - How Extended Euclidean Method can be used to calculate Inverse Modulo
  - The encryption and decryption operations of RSA Cryptosystem