Recap Lecture

COSC362 Data and Network Security

Spring Semester, 2021

Reminder

From Lecture 3 and Lab 2:

- Finding the Greatest Common Divisor (GCD) of 2 numbers
- Finding the inverse (if it does exist!)
- Checking that a set (with 2 operations) is a field

From Lecture 10 and Lab 5:

- Chinese Remainder Theorem (CRT) with a modulus as a product of 2 primes
- Euler function
- Primality tests (Fermat and Miller-Rabin)
- Finding the discrete logarithm

Outline

- Finding the GCD of 2 numbers
- Finding the inverse
- Checking that a set is a field
- CRT with a modulus as a product of 2 primes
- Euler function
- Primality tests
- Finding the discrete logarithm
- RSA cryptosystem
- Elgamal cryptosystem
- Diffie-Hellman key exchange
- Square and Multiply

Outline

Example 1

Using the Euclidean algorithm, determine $\gcd(953, 51)$

$$
\begin{aligned}
953 &= 18 \times 51 + 35 \\
51 &= 1 \times 35 + 16 \\
35 &= 2 \times 16 + 3 \\
16 &= 5 \times 3 + 1 \\
3 &= 3 \times 1
\end{aligned}
$$

Therefore $\gcd(953, 51) = 1$

Example 2

Using the Euclidean algorithm, determine $\gcd(951, 51)$

$$
\begin{aligned}
951 &= 18 \times 51 + 33 \\
51 &= 1 \times 33 + 18 \\
33 &= 1 \times 18 + 15 \\
18 &= 1 \times 15 + 3 \\
15 &= 5 \times 3
\end{aligned}
$$

Therefore $\gcd(951, 51) = 3$

Outline

Example 3 – 1

Using first the Euclidean algorithm to check whether the inverse $37^{-1} \bmod 189$ exists. If so, then using back substitution to find it.

$$\begin{aligned} 189 &= 5 \times 37 + 4 \\ 37 &= 9 \times 4 + 1 \\ 4 &= 4 \times 1 \end{aligned}$$

Therefore $\gcd(189, 37) = 1$ so $37^{-1} \bmod 189$ exists.

Example 3 – 2

Now let's use back substitution:

$$\begin{aligned} 1 &= 37 - 9 \times 4 \\ &= 37 - 9 \times (189 - 5 \times 37) \\ &= (1 + (-9) \times (-5)) \times 37 - 9 \times 189 \\ &= 46 \times 37 - 9 \times 189 \end{aligned}$$

Therefore we can write:

- $46 \times 37 = 9 \times 189 + 1$
- $46 \times 37 \equiv 1 \mod 189$

Hence $37^{-1} \mod 189 \equiv 46 \mod 189$.

Example 4

Using first the Euclidean algorithm to check whether the inverse $39^{-1} \mod 189$ exists. If so, then using back substitution to find it.

$$\begin{aligned} 189 &= 4 \times 39 + 33 \\ 39 &= 1 \times 33 + 6 \\ 33 &= 5 \times 6 + 3 \\ 6 &= 2 \times 3 \end{aligned}$$

Therefore $\gcd(189, 39) = 3$ so $39^{-1} \mod 189$ does not exist.

Outline

Example 5 – 1

Demonstrating that $\mathbb{Z}_7$ is a field.

We first write the addition and multiplication tables.
The addition table applies to $\mathbb{Z}_7$:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Example 5 – 2

The multiplication table only applies to $\mathbb{Z}_7 \setminus \{0\}$ (also denoted as $\mathbb{Z}_7^*$):

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Example 5 – 3

Then, we check that both tables form abelian groups, i.e. we check that the following properties hold:

- Closure: checking that $a + b \in \mathbb{Z}_7$ for all $a, b \in \mathbb{Z}_7$ and $a \times b \in \mathbb{Z}_7 \setminus \{0\}$ for all $a, b \in \mathbb{Z}_7 \setminus \{0\}$.
- Identity: 0 for $(\mathbb{Z}_7,+)$ and 1 for $(\mathbb{Z}_7 \setminus \{0\},\times)$ such that $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}_7$ and $1 \times a = a \times 1 = a$ for all $a \in \mathbb{Z}_7 \setminus \{0\}$.
- Inverse: $-x$ is the inverse of x for $(\mathbb{Z}_7,+)$ and x^{-1} is the inverse of x for $(\mathbb{Z}_7 \setminus \{0\},\times)$ (x^{-1} exists since 7 is prime).

Example 5 – 4

- Associativity: checking that $(a+b)+c = a+(b+c)$ for all $a, b, c \in \mathbb{Z}_7$ and $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in \mathbb{Z}_7 \setminus \{0\}$.
- Commutativity: checking that $a+b = b+a$ for all $a, b \in \mathbb{Z}_7$ and $a \times b = b \times a$ for all $a, b \in \mathbb{Z}_7 \setminus \{0\}$.

We also check the distributivity property for $(\mathbb{Z}_7,+,\times)$: checking that $a \times (b+c) = a \times b + a \times c$ for all $a, b, c \in \mathbb{Z}_7$.

Outline

Example 6 – 1

If possible (we need to check!), using the CRT, find x such that $x \equiv 5 \bmod 9$ and $x \equiv 7 \bmod 11$.

Firstly, we find the GCD of the 2 moduli:

- If the GCD is not equal to 1, then there is no solution and the CRT cannot be applied.
- If the GCD is equal to 1, then a solution must exist and we use the CRT to find x.

Example 6 – 2

Let $p = 9$, $q = 11$, $n = 9 \times 11 = 99$, $c_1 = 5$ and $c_2 = 7$.

Since $\gcd(9, 11) = 1$ (9 and 11 are relatively prime), a solution x must exist. Using the CRT, we have:

$$\begin{aligned} y_1 &= q^{-1} \mod p = 11^{-1} \bmod 9 = 2^{-1} \bmod 9 \\ &\quad (\text{we notice that } 11 \mod 9 = 2, \text{ so } 11^{-1} \mod 9 = 2^{-1}) \\ y_2 &= p^{-1} \mod q = 9^{-1} \bmod 11 \end{aligned}$$

Example 6 – 3

Finding y_1:

1. First, using the Euclidean algorithm:

$$\begin{aligned} 9 &= 4 \times 2 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

2. Then, using back substitution:

$$1 = 9 - 4 \times 2 = 1 \times 9 - 4 \times 2$$

3. Finally, concluding that:

$$y_1 = 2^{-1} \bmod 9 = -4 \bmod 9 = 5 \bmod 9$$

(from $-4 = (-1) \times 9 + 5$)

Example 6 – 4

Finding y_2:

1. First, using the Euclidean algorithm:

$$\begin{aligned} 11 &= 1 \times 9 + 2 \\ 9 &= 4 \times 2 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

2. Then, using back substitution:

$$1 = 9 - 4 \times 2 = 9 - 4 \times (11 - 1 \times 9) = 5 \times 9 - 4 \times 11$$

3. Finally, concluding that:

$$y_2 = 9^{-1} \bmod 11 = 5 \bmod 11$$

Example 6 – 5

$$
\begin{aligned}
x &= qy_1c_1 + py_2c_2 \bmod n \\
&= (11 \times (11^{-1} \bmod 9) \times 5) + (9 \times (9^{-1} \bmod 11) \times 7) \bmod 99 \\
&= (11 \times (2^{-1} \bmod 9) \times 5) + (9 \times (9^{-1} \bmod 11) \times 7) \bmod 99 \\
&= (11 \times 5 \times 5) + (9 \times 5 \times 7) \bmod 99 \\
&= 275 + 315 \bmod 99 \\
&= 590 \bmod 99 \\
&= 95
\end{aligned}
$$

(from $590 = 5 \times 99 + 95$)

Example 6 – 6

We verify that $x = 95 \mod 99$ actually satisfies $x \equiv 5 \mod 9$ and $x \equiv 7 \mod 11$:

- $x = 95 = 10 \times 9 + 5$
- $x = 95 = 8 \times 11 + 7$

Outline

Example 7

- $\phi(p) = p - 1$ where p is prime
- $\phi(pq) = (p-1)(q-1)$ where p, q are distinct primes
- $\phi(n) = \prod_{i=1}^{t} p_i^{e_i - 1}(p_i - 1)$ where $n = p_1^{e_1} \cdots p_t^{e_t}$ and p_i are distinct primes

- $\phi(30) = \phi(2 \times 3 \times 5)$
  $= (2^{1-1} \times (2-1)) \times (3^{1-1} \times (3-1)) \times (5^{1-1} \times (5-1))$
  $= (2^0 \times 1) \times (3^0 \times 2) \times (5^0 \times 4) = 8$
- $\phi(31) = 31 - 1 = 30$
- $\phi(32) = \phi(2^5) = 2^{5-1} \times (2-1) = 2^4 \times 1 = 16$
- $\phi(33) = \phi(11 \times 3) = (11-1) \times (3-1) = 10 \times 2 = 20$
- $\phi(34) = \phi(17 \times 2) = (17-1) \times (2-1) = 16 \times 1 = 16$
- $\phi(35) = \phi(7 \times 5) = (7-1) \times (5-1) = 6 \times 4 = 24$

Outline

Example 8

Using Fermat test to check whether 517 is prime or not.
The test is run at most 4 times with base values $a = 2, 3, 11, 17$.
The test roughly asks whether $a^{517-1} \mod 517$ is equal to 1.

- *Reminder:* $(a^m)^k \mod n = (a^m \mod n)^k \mod n$
- $517 - 1 = 516 = 43 \times 3 \times 4$
- Let us start with $a = 2$:
  - $2^{43} \equiv 382 \bmod 517$
  - $382^3 \equiv 28 \bmod 517$
  - $28^4 \equiv 460 \bmod 517 (\equiv 2^{516} \mod 517)$
- Thus, $2^{516} \mod 517 \neq 1$
- The test outputs `composite`

If the test outputs `composite` then 517 is definitely composite.

Example 9

Using Fermat test to check whether 211 is prime or not.
The test is run at most 4 times with base values $a = 2, 3, 11, 17$.

- $211 - 1 = 210 = 2 \times 7 \times 3 \times 5$
- Let us start with $a = 2$:
  - $2^{2\times 7} \equiv 137 \mod 211$
  - $137^3 \equiv 107 \mod 211$
  - $107^5 \equiv 1 \mod 211 (\equiv 2^{210} \mod 211)$
- Thus, $2^{210} \mod 211 = 1$
- We repeat with $a = 3, 11, 17$ and get $a^{210} \equiv 1 \mod 211$
- The test outputs `probable prime` for each base value *a*.

If the test outputs `probable prime` then we can be *confident* that 211 is prime.

Example 10

Using Miller-Rabin test to check whether $n = 109$ is prime or not:

- $109 - 1 = 108 = 2^2 \times 27$
- Hence $v = 2$ and $u = 27$

1. Choose $a = 2$
2. $b = a^u \mod n = 2^{27} \mod 109 = 33$
3. Since $b \neq 1$, continue (loop from 0 to $v - 1 = 1$):
   - $b = 33^2 \mod 109 = 108 = -1$
4. Since $b = -1$, return `probable prime`

Run the test again for other base values $a = 3, 5, 7, 11, 13, 17$.

Outline

Example 11

What is the discrete logarithm of the number 4 with regard to base 2 for the modulus $p = 7$?
In other words, find x such that $2^x = 4 \bmod 7$:

- $2^1 = 2 \mod 7$
- $2^2 = 4 \mod 7$
- $2^3 = 8 = 1 \mod 7$
- $2^4 = 16 = 2 \mod 7$
- $2^5 = 32 = 4 \mod 7$
- etc.

We observe a cycle. Therefore, powers of 2 modulo 7 are thus 2, 4, 1. Hence $x = 2$.

Outline

Example 12 – 1

Key generation:

- Let $p = 11$ and $q = 13$:
  - $n = p \times q = 11 \times 13 = 143$
  - $\phi(n) = (p-1)(q-1) = 10 \times 12 = 120$
- Let $e = 7$:
  - We need to find $d = e^{-1} \mod \phi(n) = 7^{-1} \mod 120$.
  - Solving $ed + k'\phi(n) = 1$ using the Euclidean algorithm (unknowns are d and the integer k').
  - $120 = 7 \times 17 + 1$, hence $1 = 7 \times (-17) + 1 \times 120$.
  - Therefore, $k' = 1$ and $d = -17 \mod \phi(n) = 103 \mod \phi(n)$ (since $1 \times 120 - 17 = 103$).
- We can check that $ed = 1 \mod \phi(n)$:
  - $7 \times 103 = 721 = 1 \mod 120$.

Example 12 – 2

Encryption:

- $M = 5$, thus $C = M^e \mod n = 5^7 \mod 143 = 47$.

Decryption:

- $C^d \mod n = 47^{103} \mod 143 = 5 = M$.

Outline

Example 13 – 1

Key generation:

- Choose prime $p = 17$ and generator $g = 3$.
- Bob's private key is $x = 12$.
- Compute $y = g^x \mod p = 3^{12} \mod 17 = 4$.
- Bob's public key is $(17, 3, 4)$.

Encryption:

- Alice wants to send $M = 9$.
- Alice chooses at random $k = 3$ and compute $C_1 = g^k \mod p = 3^3 \mod 17 = 10$.
- She also computes $C_2 = M \times y^k \mod p = 9 \times 4^3 \mod 17 = 15$.
- Ciphertext is $C = (C_1, C_2) = (10, 15)$.

Example 13 – 2

Decryption:

- Bob receives $C = (C_1, C_2) = (10, 15)$.
- Bob computes $C_1^x \mod p = 10^{12} \mod 17 = 13$.
- Bob finds $(C_1^x)^{-1} \mod p = 13^{-1} \mod 17$:
  - Let A denote the inverse of C_1^x.
  - That is, Bob finds A and k' such that $C_1^x \times A + k' \times p = 1$.
  - *Euclidean algorithm:*
    1. $17 = 13 \times 1 + 4$
    2. $13 = 4 \times 3 + 1$
  - *Back substitution:*
    $1 = 13 - 4 \times 3 = 13 - (17 - 13) \times 3 = 13 \times 4 - 3 \times 17$
  - Therefore, $A = 4$ and $k' = -3$.
- Bob recovers $M = C_2 \times (C_1^x)^{-1} \mod p = 15 \times 13^{-1} \mod 17 = 15 \times 4 \mod 17 = 60 \mod 17 = 9$.

Outline

Example 14

Public elements are prime $p = 17$ and generator $g = 3$.

- Selecting private keys:
  - Alice selects $a = 7$
  - Bob selects $b = 12$
- Sharing public keys:
  - Alice sends $g^a \mod p = 3^7 \mod 17 \equiv 11$ to Bob
  - Bob sends $g^b \mod p = 3^{12} \mod 17 \equiv 4$ to Alice
- Computing the shared key:
  - Alice computes $Z = (g^b)^a \mod p \equiv 4^7 \mod 17 = 13$
  - Bob computes $Z = (g^a)^b \mod p \equiv 11^{12} \mod 17 = 13$

The common secret is $Z = 13$.

Outline

Example 15 – 1

Given x and n, what does the square-and-multiply algorithm require when used to compute $x^{68} \mod n$ (in terms of squarings and multiplications)?

- We write 68 in binary: 1000100.
- If we encounter a 0, we square x.
- If we encounter a 1, we square x, then multiply by x.

Example 15 – 2

Bit	Calculation	Why?
1	x	First 1 lists number
0	(x^2)	0 calls for Square
0	$((x^2)^2)$	0 calls for Square
0	$(((x^2)^2)^2)$	0 calls for Square
1	$((((x^2)^2)^2)^2 \times x)$	1 calls for Square + Multiply
0	$(((((x^2)^2)^2)^2 \times x)^2)$	0 calls for Square
0	$((((((x^2)^2)^2)^2 \times x)^2)^2)$	0 calls for Square

The algorithm thus requires 6 squarings and 1 multiplication modulo n.