

# Groups in Cryptography



# Groups in Cryptography

- A set  $S$  and a binary operation  $\oplus$
- A group  $G = (S, \oplus)$  if  $S$  and  $\oplus$  satisfy:
  - Closure: If  $a, b \in S$  then  $a \oplus b \in S$
  - Associativity: For  $a, b, c \in S$ ,  $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
  - A neutral element:  $e \in S$  such that  $a \oplus e = e \oplus a = a$
  - Every element  $a \in S$  has an inverse  $\text{inv}(a) \in S$ :

$$a \oplus \text{inv}(a) = \text{inv}(a) \oplus a = e$$

- Commutativity: If  $a \oplus b = b \oplus a$ , then the group  $G$  is called an a commutative group or an Abelian group
- In cryptography we deal with Abelian groups

# Multiplicative Groups

- The operation  $\oplus$  is a multiplication
- The neutral element is generally called the unit element  $e = 1$
- Multiplication of an element  $k$  times by itself is denoted as

$$a^k = \overbrace{a \cdot a \cdots a}^{k \text{ copies}}$$

- The inverse of an element  $a$  is denoted as  $a^{-1}$
- Example:  $(\mathcal{Z}_n^*, * \text{ mod } n)$
- The operation  $*$  is multiplication mod  $n$
- If  $n$  is prime,  $\mathcal{Z}_n^* = \{1, 2, \dots, n-1\}$
- If  $n$  is not a prime,  $\mathcal{Z}_n^*$  consists of elements  $a$  with  $\gcd(a, n) = 1$
- In other words,  $\mathcal{Z}_n^*$  is the set of invertible elements mod  $n$

# Multiplicative Group Examples

- Consider the multiplication tables for mod 5 and mod 6

* mod 5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

* mod 6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

- mod 5 multiplication on the set  $\mathcal{Z}_5 = \{1, 2, 3, 4\}$  forms the group  $\mathcal{Z}_5^*$
- mod 6 multiplication on the set  $\mathcal{Z}_6 = \{1, 2, 3, 4, 5\}$  does not form a group since 2, 3 and 4 are not invertible
- However, mod 6 multiplication on the set of invertible elements forms a group:  $(\mathcal{Z}_6^*, * \text{ mod } 6) = (\{1, 5\}, * \text{ mod } 6)$

# Additive Groups

- The operation  $\oplus$  is an addition
- The neutral element is generally called the zero element  $e = 0$
- Addition of an element  $a$   $k$  times by itself, denoted as

$$[k] a = \overbrace{a + \cdots + a}^{k \text{ copies}}$$

- The inverse of an element  $a$  is denoted as  $-a$
- Example:  $(\mathcal{Z}_n, + \text{ mod } n)$  is a group; the set is  $\mathcal{Z}_n = \{0, 1, 2, \dots, n-1\}$  and the operation is addition mod  $n$

# Additive Group Examples

- Consider the addition tables mod 4 and mod 5

+ mod 4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+ mod 5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- mod 4 addition on  $\mathcal{Z}_4 = \{0, 1, 2, 3\}$  forms the group  $(\mathcal{Z}_4, + \text{ mod } 4)$
- mod 5 addition on  $\mathcal{Z}_5 = \{0, 1, 2, 3, 4\}$  forms the group  $(\mathcal{Z}_5, + \text{ mod } 5)$

# Order of a Group

- **The order of a group** is the number of elements in the set
- The order of  $(\mathcal{Z}_{11}^*, * \bmod 11)$  is 10, since the set  $\mathcal{Z}_{11}^*$  has 10 elements:  $\{1, 2, \dots, 10\}$
- The order of group  $(\mathcal{Z}_p^*, * \bmod p)$  is equal to  $p - 1$
- Note that, since  $p$  is prime, the group order  $p - 1$  is not prime
- The order of  $(\mathcal{Z}_{11}, + \bmod 11)$  is 11, since the set  $\mathcal{Z}_{11}$  has 11 elements:  $\{0, 1, 2, \dots, 10\}$
- The order of  $(\mathcal{Z}_n, + \bmod n)$  is  $n$ , since the set  $\mathcal{Z}_n$  has  $n$  elements:  $\{0, 1, 2, \dots, n - 1\}$ ; here  $n$  could be prime or composite

# Order of an Element

- **The order of an element**  $a$  in a multiplicative group is the smallest integer  $k$  such that  $a^k = 1$ , where 1 is the unit element of the group
- $\text{order}(3) = 5$  in  $(\mathcal{Z}_{11}^*, * \bmod 11)$  since

$$\{3^i \bmod 11 \mid 1 \leq i \leq 10\} = \{3, 9, 5, 4, 1\}$$

- $\text{order}(2) = 10$  in  $(\mathcal{Z}_{11}^*, * \bmod 11)$  since

$$\{2^i \bmod 11 \mid 1 \leq i \leq 10\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$$

- Note that  $\text{order}(1) = 1$



# Order of an Element

- **The order of an element**  $a$  in an additive group is the smallest integer  $k$  such that  $[k]a = 0$ , where  $0$  is the zero element
- $\text{order}(3)$  in  $(\mathcal{Z}_{11}, + \text{ mod } 11)$  is computed by finding the smallest  $k$  such that  $[k]3 = 0$
- This is obtained by successively computing

$$3 = 3, \quad 3 + 3 = 6, \quad 3 + 3 + 3 = 9, \quad 3 + 3 + 3 + 3 = 1, \quad \dots$$

until we obtain the zero element

- We find  $\text{order}(3) = 11$  in  $(\mathcal{Z}_{11}, + \text{ mod } 11)$

$$\{ [i]3 \text{ mod } 11 \mid 1 \leq i \leq 11 \} = \{3, 6, 9, 1, 4, 7, 10, 2, 5, 8, 0\}$$

- Note that  $\text{order}(0) = 1$

# Lagrange's Theorem

## Theorem

*The order of an element divides the order of the group.*

- The order of the group  $(\mathcal{Z}_{11}^*, * \bmod 11)$  is equal to 10, while  $\text{order}(3) = 5$  in  $(\mathcal{Z}_{11}^*, * \bmod 11)$ , and 5 divides 10
- $\text{order}(2) = 10$  in  $(\mathcal{Z}_{11}^*, * \bmod 11)$ , and 10 divides 10
- Similarly,  $\text{order}(1) = 1$  in  $(\mathcal{Z}_{11}^*, * \bmod 11)$ , and 1 divides 10
- Since the divisors of 10 are 1, 2, 5, and 10, the element orders can only be 1, 2, 5, or 10

# Lagrange Theorem

- On the other hand,  $\text{order}(3) = 11$  in  $(\mathcal{Z}_{11}, + \text{ mod } 11)$ , and  $11|11$
- Similarly,  $\text{order}(2) = 11$  in  $(\mathcal{Z}_{11}, + \text{ mod } 11)$
- We also found  $\text{order}(0)=1$
- The order of the group  $(\mathcal{Z}_{11}, + \text{ mod } 11)$  is 11
- Since 11 is a prime number, the order of any element in this group can be either 1 or 11
- 0 is the only element in  $(\mathcal{Z}_{11}, + \text{ mod } 11)$  whose order is 1
- All other elements have the same order 11 which is the group order

# Primitive Elements

- An element whose order is equal to the group order is called **primitive**
- The order of the group  $(\mathcal{Z}_{11}^*, * \bmod 11)$  is 10 and  $\text{order}(2) = 10$ , therefore, 2 is a primitive element of the group
- $\text{order}(2) = 11$  and  $\text{order}(3) = 11$  in  $(\mathcal{Z}_{11}, + \bmod 11)$ , which is the order of the group, therefore 2 and 3 are both primitive elements — in fact all elements of  $(\mathcal{Z}_{11}, + \bmod 11)$  are primitive except 0

## Theorem

*The number of primitive elements in  $(\mathcal{Z}_p^*, * \bmod p)$  is  $\phi(p - 1)$ .*

- There are  $\phi(10) = 4$  primitive elements in  $(\mathcal{Z}_{11}^*, * \bmod 11)$ ,
- The primitive elements are: 2, 6, 7, 8
- All of these elements are of order 10

# Cyclic Groups and Generators

- We call a group **cyclic** if all elements of the group can be generated by repeated application of the group operation on a **single element**
- This element is called a **generator**
- Any primitive element is a generator
- For example, 2 is a generator of  $(\mathcal{Z}_{11}^*, * \text{ mod } 11)$  since

$$\{2^i \mid 1 \leq i \leq 10\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = \mathcal{Z}_{11}^*$$

- Also, 2 is a generator of  $(\mathcal{Z}_{11}, + \text{ mod } 11)$  since

$$\{[i]_2 \text{ mod } 11 \mid 1 \leq i \leq 11\} = \{2, 4, 6, 8, 10, 1, 3, 5, 7, 9, 0\} = \mathcal{Z}_{11}$$