

CS355: Cryptography

Lecture 23: Discrete logarithm.

CERIAS SYMPOSIUM

- **1:30 - 4:00 p.m. Poster Session and Refreshments**
- South Ballroom
- *Purdue Memorial Union*

Many cryptographic algorithms rely on exponentiation
Example: Diffie-Hellman key exchange, ElGamal encryption

$a^x \bmod n$, where x is supposed to be secret

QUESTIONS:

- 1) how difficult is to compute x from $a^x \bmod n$**
- 2) from $a^x \bmod n$ and $a^y \bmod n$ how easy it to compute $a^{xy} \bmod n$**

Logarithm: $\log_a b = x$, where $a^x = b$

Discrete logarithm: x with property that $a^x \bmod n = b$

Groups

Definition

A *group* $(G, *)$ is a set G on which a binary operation is defined which satisfies the following axioms:

Closure: For all $a, b \in G$, $a * b \in G$.

Associative: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

Identity: $\exists e \in G$ s.t. for all $a \in G$, $a * e = a = e * a$.

Inverse: For all $a \in G$, $\exists a^{-1} \in G$ s. t. $a * a^{-1} = a^{-1} * a = e$.

Example

$(\mathbb{Z}_n, +)$ is a group, where $+$ is addition modulo n

$(\mathbb{Z}_p, *)$ is a group, where $*$ is multiplication modulo p

Groups (cont.)

Definition:

A group $(G, *)$ is called an *abelian group* if operation $*$ is a commutative operation:

Commutative: For all $a, b \in G$, $a * b = b * a$.

Example:

$(\mathbb{R}, +)$ is an abelian group

Definition

A group G is *cyclic* if $\exists g \in G$ s.t. any $h \in G$ can be written $h = g^i$.

g is called group generator.

Example

Cyclic groups: $(\mathbb{Z}_2, *)$, $(\mathbb{Z}_3, *)$

Order of a Group

Definition

The *order* of a group G , $\text{ord}(G)$, is defined as the number of elements in the group.

Definition

A group G is *finite*, if $|G| = \text{ord}(G)$, is finite.

We can show that the order of $(\mathbb{Z}_n, *)$ is $\Phi(n)$

Example:

What is the order of $(\mathbb{Z}_7^*, *)$, $(\mathbb{Z}_{700}^*, *)$?

Order of an Element

Definition

The *order of an element* g from a finite group G , is the smallest power of n such that $g^n=e$, where e is the identity element.

Example:

What is the order of 2 in $(\mathbb{Z}_5^*, *)$?

It is 4 because $2^4 \equiv 1 \pmod{5}$

What is the order of 3 in $(\mathbb{Z}_{10}^*, *)$?

It is 4 because $3^4 \equiv 1 \pmod{10}$

OBS: order of an element modulo $n \leq \Phi(n)$

Primitive Root

Definition

An integer g whose order modulo n is $\Phi(n)$ is called a primitive root modulo n .

Example

$(\mathbb{Z}_7^*, *)$, $5^6 \equiv 1 \pmod{7}$ and $\Phi(7) = 6$

$5^6 = 15625$

$(\mathbb{Z}_8^*, *)$ does not have a primitive root

FACT

The group $G = \langle \mathbb{Z}_n^*, * \rangle$ has primitive roots only if n is 2 , 4 , p^t or $2p^t$ where p is an odd integer.

Primitive Roots and Cyclic Groups

FACT

If a group $(\mathbb{Z}_n^*, *)$ has a primitive root, it is cyclic. Each primitive root is a generator and can be used to create the whole set. $\mathbb{Z}_n^* = \{g_1, g^2, \dots, g^{\Phi(n)}\}$

FACT

If the group $(\mathbb{Z}_n^*, *)$ has any primitive root, the number of primitive roots is $\Phi(\Phi(n))$

OBSERVATION

$(\mathbb{Z}_n^*, *)$ is cyclic if it has primitive roots

$(\mathbb{Z}_p^*, *)$ is always cyclic

Discrete Logarithm

Definition

Let $G = (\mathbb{Z}_n^*, *)$ be a cyclic group with generator (primitive root) g . Then every element a of G can be written as $g^k \equiv a \pmod{n}$.

k is called the index of a base g modulo n , or the discrete logarithm of a to base g modulo n .

Discrete logarithms behave similar with traditional logarithms.

$$\log_g 1 \equiv 0 \pmod{\Phi(n)}$$

$$\log_g xy \equiv (\log_g x + \log_g y) \pmod{\Phi(n)}$$

$$\log_g x^k \equiv k \log_g x \pmod{\Phi(n)}$$

$$(\mathbb{Z}_p^*, *)$$

1, 2, ... p-1

It always has primitive roots

It is cyclic

**The primitive root is the base of the discrete
logarithm**