

# DLP-base cryptosystems

## Lesson 3



# Discrete Logarithm Problem – DLP

- $F_p, p \in \wp$  is a field with a prime number of elements, finite field.

**Proposition.** Let  $p \in \wp, \exists g \in F_p, n \in \mathbb{N}: \forall x \in F_p, x \equiv g^n \pmod{p}$ .  $g$  is called a primitive element or a generator.

**Definition (DLP).** Let  $g$  be a primitive root for  $F_p$  and let  $h$  be a nonzero element of  $F_p$ . The DLP is the problem of finding an exponent  $x$  such that  $g^x \equiv h \pmod{p}$ .

- **Remark.** The number  $x$  is called the discrete logarithm of  $h$  to the base  $g$ , denoted  $x = \log_g(h)$ , or index,  $\text{ind}_g(h)$ .

# Diffie-Hellman key exchange

## Public Parameter Creation

A trusted party chooses and publishes a (large) prime  $p$  and an integer  $g$  having large prime order in  $F_p^*$

## Private Computations

Alice

Bob

Choose a secret integer  $a$ .  
Compute  $A \equiv g^a \pmod{p}$ .

Choose a secret integer  $b$ .  
Compute  $B \equiv g^b \pmod{p}$ .

## Public Exchange of Values

Alice sends  $A$  to Bob  $\longrightarrow$

$B$

$A$   
 $\longleftarrow$  Bob sends to Alice

## Further Private Computations

Compute the number  $K \equiv B^a \pmod{p}$

Compute the number  $K \equiv A^b \pmod{p}$

# The Diffie-Hellman Problem – DHP

**Definition (DHP).** Let  $p$  be a prime and  $g$  an integer. The DHP is the problem of computing the value  $g^{ab} \pmod{p}$  from the known values  $g^a$  and  $g^b \pmod{p}$

**Remark.** DHP is no harder DLP.

- If Eve can solve DLP, she can get  $a$  or  $b$  from  $A \equiv g^a \pmod{p}$  and  $B \equiv g^b \pmod{p}$ . So, she can compute  $K \equiv g^{ab} \pmod{p}$ .
- Suppose that Eve has an algorithm that efficiently solves the DHP. Can she use it to also efficiently solve the DLP? The answer is not known.

# ElGamal public key cryptosystem

- It is just a variation of Diffie-Hellman key-exchange protocol for encryption data

# ElGamal public key cryptanalysis

**Proposition.** Fix a prime  $p$  and base  $g$  to use for ElGamal encryption. Suppose that Eve has access to an oracle that decrypts arbitrary ElGamal ciphertexts encrypted using arbitrary ElGamal public keys. Then she can use the oracle to solve the DHP.