Cryptographic Primitives and Algorithms in LaTeX

AR

February 23, 2025

Abstract

This document is a collection of simple sample of cryptographic primitives and algorithms.

1 Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange [1] preceeeds several cryptography mechanisms we use today.

1. Choose Public Parameters

   Two parties, *Alice* and *Bob*, agree on:

   A prime number $p = 17$

   A primitive root modulo of $p = 17$, called the generator $g = 3$

2. Generate Private Keys *Alice* and *Bob* picks a private key each (a secret number):

   Alice picks private key $a = 6$ and only *Alice* knows about it

   Bob picks private key $b = 11$ and only *Bob* knows about it

   These private keys are kept secret.

3. Compute Public Keys

   Each party computes a public key using the formula:

$$A = g^a \quad mod \quad p \tag{1}$$

$$B = g^b \quad mod \quad p \tag{2}$$

   Alice computes her public key A

$$A = 3^6 \quad mod \quad 17$$
$$A = 15$$

   Bob computes his public key B

$$B = 3^{11} \quad mod \quad 17$$
$$B = 7$$

   These public keys are exchanged over the insecure channel

4. Compute the Shared Secret

   Now each party computes the shared secret $s = s_A = s_B$

   At Alice

$$s_A = B^a \quad mod \quad p \tag{3}$$

   At Bob

$$s_B = A^b \quad mod \quad p \tag{4}$$

   Alice computes s_A

$$s_A = 7^6 \quad mod \quad 17$$
$$s_A = 2$$

Bob comptes s_B

$$s_B = 15^{11} \quad mod \quad 17$$
$$s_B = 2$$

Thus,

$$s\_A = s_B$$

Verify

Since

$$(g^a)^b = g^{ab}$$

And multiplication is commutative $ab = ba$

References

[1] Whitfield Diffie and Martin E Hellman. New directions in cryptography. In Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, pages 365–390. 2022.