2.3. Diffie-Hellman Key Exchange. Let’s suppose Alice and Bob have never met before. Diffie-Hellman key exchange allows them to jointly establish a shared secret key over an insecure channel. The algorithm can be implemented in the multiplicatively written group of any finite field. In this example, we will consider

the most common implementation in a group of a prime field, (Z/pZ)∗. It is important that g ∈ (Z/pZ)∗ is a generator since we want to make sure the generated shared key at the end received from a power of g is any element of (Z/pZ)∗. Let’s outline the process step by step:

(1) Alice and Bob agree on a prime modulus p and a generator g, which are publicly known;

(2) Alice selects a private random number a such that 1 < a < p − 1 and calculates l = ga mod p sending the result publicly to Bob;

(3) Then Bob selects his private random number b such that 1 < b < p − 1 and calculates m = gb mod p sending the result publicly to Alice;

(4) Alice takes Bob’s public result m and raises it to the power of her private number obtaining ma mod p;

(5) Bob takes Alice’s public result l and raises it to the power of his private number obtaining lb mod p;

(6) We notice that ma mod p = (gb)a mod p = (ga)b mod p = lb mod p = s is a shared key.