VE475 Homework 8

Liu Yihao 515370910207

Ex. 1 — Lamport one-time signature scheme

1. Lamport signature is a method of constructing a digital signature. It needs a cryptographic hash function.

   Suppose there is an x-bit cryptographic hash function, first Alice generates x pairs of random numbers of x bits (each pair contains two numbers) as the private key. Then she hashes the $2x$ numbers generated into $2x$ hashed values of x bit as the public key.

   When Alice wants to sign a message, first she hashes the message into a x-bit hash sum. Then, for each bit of the hash sum, she picks the corresponding pair in the private key and select one number in the pair. When the bit is 0, she selects the first number; otherwise, she selects the second number. After that, she will get a sequence of x numbers in x bits, which is the signature of the message and will be published along with the message. Note that the private key can only be used once.

   When Bob wants to verify the message sent by Alice, he also hashes the message into a x-bit hash sum. Similar to the signing procedure, he can select x numbers from the public key according to each bit of the hash sum (0 for the first number and 1 for the second number). Then he can hash the x numbers provided by Alice and see whether they exactly match the numbers he selected from the public key. If they all match, the signature is ok; otherwise, the signature is wrong.

2.