Exercise 11

1 Domain Extension for Oblivious Transfer

Suppose Alice and Bob have a primitive that performs a 1-out-of-2 Oblivious Transfer (OT) for *one bit* from Alice (as sender) to Bob (as receiver). They would like to implement oblivious transfer of k-bit strings from Alice to Bob.

Describe a protocol that uses the *bitwise* OT primitive any number of times and implements 1-out-of-2 OT of *bit strings* from Alice to Bob. You may use additional error-free communication in either direction, secret-key cryptosystems like block ciphers, and possibly other methods.