

Homework on key exchange

Suppose that the public modulus is $p = 17$, and that the public base is $s = 7$. Alice and Bob would like to exchange keys. Alice chooses $a = 8$ and Bob chooses $b = 9$. (See Barr p. 299 for the notation.)

- (1). What number does Alice send Bob?
- (2). What number does Bob send Alice?
- (3). What key do they agree on? Do both Bob's and Alice's computations, and check that they agree.