Homework 12 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

26.01.2010

Exercise 34.

Alice and Bob use the Diffie-Hellman key exchange to agree upon a shared key. As system parameters they use the prime number $p = 101$ and the primitive element $a = 2$ modulo p. Alice chooses as her secret $x = 37$ and Bob chooses $y = 33$. Use the Square and Multiply algorithm to compute large integer powers.

(a) How does the protocol work? Which values must Alice and Bob exchange?

(b) Compute the shared key.

Exercise 35.

How can the man-in-the-middle (MITM) attack against the DH key-exchange protocol be easily avoided?

Exercise 36.

Alice and Bob are using the Shamir's no-key protocol to exchange a message. They agree to use the prime $p = 31337$ for their communication. Alice chooses her random number $r_A = 9999$ while Bob chooses $r_B = 1011$. Alice's message is $m = 3567$.

Carry out the protocol by calculating the inverses $a^{-1} \pmod{p-1}$ and $b^{-1} \pmod{p-1}$. Then, compute all messages with the given values.