Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 11
Version 09.07.2020

Exercise 1.

(a) A shift cypher key K is exchanged using the Diffie-Hellman method with $g = 5$ and $p = 47$. The actual numbers exchanged were $\alpha = 38$ and $\beta = 3$. Find the key K.

(b) Using the key in (a) decipher the message:

EQPITCVWNCVKQPU.

Exercise 2.

Let Bob's public ElGamal key be $(p, g, \alpha) = (101, 2, 11)$.

(a) Find Bob's private ElGamal key b.

(b) Find the plaintext m of the ciphertext $(\beta, y) = (64, 79)$ sent to Bob from Alice.

Exercise 3.

Assume that Alice uses Bob's ElGamal public key $(p = 11, g = 8, \alpha = 2)$ to encrypt two messages x_1 and x_2 using the same random integer a, and get the cipher texts $(\beta, y_1 = 3)$ and $(\beta, y_2 = 2)$ respectively. Eve intercepts the ciphertext and somehow she finds the value of $x_1 = 6$. Show how Eve can use a known-plaintext attack to find the plain text x_2 and calculate it.