MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

ECDH-Key Exchange for Beginners

Author: Lena Meier

February 2012

Prearrangement

Alice and Bob agreed upon the elliptic curve

$$E: y^2 = x^3 + 4x + 20 \bmod 29$$

The primitive element $\alpha = (8, 10)$ and this curve E are the basis for an Elliptic Curve Diffie-Hellman (ECDH) key exchange.

Key Exchange

Alice and Bob choose the private keys $k_{pr_A} = 2$ and $k_{pr_B} = 7$. Each one calculates his or her public key Q_A or Q_B which are points on the curve E. They exchange these points and both can calculate the joint secret K_{AB}:

Alice: $K_{AB} = k_{pr_A} \cdot Q_B$
Bob: $K_{AB} = k_{pr_B} \cdot Q_A$

The session key k_{AB} is derived from the y-coordinate of K_{AB}:

$k_{AB} = y_{K_{AB}}$

Encryption Method

This session key is used in the following symmetric encryption method:

$$y = k_{AB} \cdot x + 4 \bmod 26$$
$$x = k_{AB}^{-1} \cdot (y - 4) \bmod 26$$

Now Alice receives the following encrypted message from Bob:

EHHUWALYOOJYHWRIVWAQ

The letters A,...,Z are represented by the numbers 0,...,25 for all calculations.
Try to decrypt this message, add spaces at the correct positions and hand in the decrypted message in capital letters.

Sources

This challenge is based on an assignment that was provided in connection with a lecture given by Christof Paar, tutored by Daehyun Strobel, in 2010.

For further information on elliptic curve cryptography you can refer to e.g. one of the following sources:

- Understanding Cryptography by C. Paar and J. Pelzl, published in 2010 by Springer.
  Further information: www.springerlink.com
- Elliptic curve cryptography (ECC)
- Elliptic curve Diffie-Hellman (ECDH)