Homework 1 in Cryptography I

Prof. Dr. Rudolf Mathar, Georg Böcherer, Paul de Kerret

29.04.2010

Exercise 1. Are 377 and 161 invertible in $\mathbb{Z}_{2011}$? 54 in $\mathbb{Z}_{2010}$? 3^{2009} in $\mathbb{Z}_{37}$? Justify and find the inverse when it exists.

hint: Apply the extended euclidian algorithm (in the script). $3^{29} \equiv 28 \mod 37$.

Exercise 2. Decrypt the following ciphertexts and explain your approach. The plaintext messages are in english.

a) Caesar cipher:
sdscsxceppsmsoxddyzbydomdyebcovfocgsdrv
kgcgoxoondyzbydomdyebcovfocgsdrwkdrowkdsmc

hint: Use the most frequent letter in english for the frequency analysis.

b) Affine cipher:
onhldqrttydxtlgtojkhqtjxctdc

hint: Use "t" and "o" on the code side for the frequency analysis.

Exercise 3. Consider an affine cipher over an alphabet with m letters.

(a) Determine the number of keys for this cipher. How many keys are there if m is prime? Why is it "better" to use an affine cipher with an alphabet of 23 instead of 26 letters?

(b) Show that the repeated encryption of a plaintext with two affine ciphers is not different from the encryption with one affine cipher using a different key.