**Examination questions (second exam)** 7.10.2015

**Mathematical Cryptology** MAT-63256

**Examination prepared by: S. Foldes**

**Examination date:**

**Instructions:**

**Use of books, notes, dictionaries, ebooks, calculators and computers allowed.**

Questions:

1. Assume that the letters a,b,c,d,e,f,g are encoded as the integers 0,1,2,3,4,5,6 mod 7, in that order. Encrypt the following plaintext into ciphertext words using the affine encryption 4i+4:

deaf babe gab, feed a cab

2. Find all irreducible (prime) polynomials) of degree 3 over a 2-element field.

3. What are the decrypting functions for the AFFINE encryption 4i+3 mod 7 and mod 11 ?

4. Which elements of the multiplicative group of the 7-element field F(7) of residues mod 7 have order 3 ?

5. How many affine encrypting keys exist mod 13 ?