Cryptography I, homework sheet 7

Due: 02 December 2011, 10:45

Note that from now on Sebastiaan corrects the homeworks.

1. Compute the product of all monic, irreducible polynomials of degree 6 over $\mathbb{F}_2$.
2. How many monic, irreducible polynomials of degree 6 exist over $\mathbb{F}_5$?
3. Compute the number of irreducible polynomials of degree 30 over $\mathbb{F}_3$.
4. $3 \in \mathbb{F}_{1013}^*$ generates a group of order 1012, so it generates the whole multiplicative group of the finite field.

   Alice's public key is $h_A = 224$. Use ElGamal encryption to encrypt the messge $m = 42$ to her using the "random" value $k = 654$.