Cryptology 2008
(Home work 2)

February 27, 2008

- Due on Tuesday, March 14, 4 p.m.
- Late submissions will not be accepted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.
- Problem 3 bear 10 points and all other problems 5 points each.

1. Construct the finite field $GF(2^3)$. Find all the generators of the cyclic subgroup formed by the non-zero elements of this field.

2. Assume that a sender encrypts a message of m blocks using the CBC mode. During transmission, block number $m/2$ gets corrupted. After the receiver decrypts the cipher, how many blocks of the decrypted message would be corrupted?

3. Implement encryption and decryption functionality of AES. Use a low level programming language (preferably C). You should not use any publicly available library.