(Bonus) Quiz #1

MATH 481/581 — Cryptography
Friday, March 15

Please print your name:

Problem 1. (2+4 points) Consider the finite field GF(2^6) constructed using x^6+x+1.

(a) The product of x^5+x^4 and x^5 in GF(2^6) is □.

(b) The inverse of x^3 in GF(2^6) is □.

Use the extra sheet for your computations. Make sure to check your answer! You have plenty of time.

Problem 2. (2 points) The primitive roots modulo 14 are □.

Again, use the extra sheet for your computations.

Problem 3. (6 points) Fill in the blanks.

(a) DES has a block size of □ bits, a key size of □ bits and consists of □ rounds.

(b) Suppose we are using 3DES with key $k=(k_1,k_2,k_3)$, where each k_i is an independent DES key.

Then m is encrypted to $c=$ □. The effective key size is □ bits.

(c) AES-128 has a block size of □ bits, a key size of □ bits and consists of □ rounds.

(d) AES-256 has a block size of □ bits, a key size of □ bits and consists of □ rounds.

(e) The four layers of AES are □.

(f) If $x \pmod N$ has (multiplicative) order k, then x^{10} has order □.