*UBI 523 Cryptosystems and Cryptographic Protocols*

*Homework Problems*

**4.4.** Addition in GF(24): Compute A(x)+B(x) mod P(x) in GF(24) using the irreducible polynomial P(x) = x4 +x+1. What is the influence of the choice of the reduction polynomial on the computation?

1. A(x) = x2+1, B(x) = x3+x2+1

2. A(x) = x2+1, B(x) = x+1

**4.6.** Compute in GF(28):

(x4+x+1)/(x7+x6+x3+x2),

where the irreducible polynomial is the one used by AES, P(x)=x8+x4+x3+x+1.

Note that Table 4.2 contains a list of all multiplicative inverses for this field.

**4.13.** We consider the first part of the ByteSub operation, i.e, the Galois field inversion.

1. Using Table 4.2, what is the inverse of the bytes 29, F3 and 01, where each byte is given in hexadecimal notation?

2. Verify your answer by performing a GF(28) multiplication with your answer and the input byte. Note that you have to represent each byte first as polynomials in GF(28). The MSB of each byte represents the x7 coefficient.

**4.16.** The minimum key length for the AES algorithm is 128 bit. Assume that a special-purpose hardware key-search machine can test one key in 10 ns on one processor. The processors can be parallelized. Assume further that one such processor costs $10, including overhead. (Note that both the processor speed and the prize are rather optimistic assumptions.) We assume also that Moore’s Law holds, according to which processor performance doubles every 18 months.

How long do we have to wait until an AES key search machine can be built which breaks the algorithm on average in one week and which doesn’t cost more than $1 million?

