

Mathematics of Coding and Cryptography
Worksheet 7

1. The following algorithm allows for the computation of a multiplicative inverse in $\text{GF}(2^8)$.

(a) Convert the 8-bit number to the polynomial $b(x)$.

(b) Set

$$r_1 = x^8 + x^4 + x^3 + x + 1$$

$$r_2 = b(x)$$

$$a_1 = 0$$

$$a_2 = 1$$

$$i = 2$$

(c) while $r_i > 1$, set

$$i = i + 1$$

$$r_i = \text{remainder}(r_{i-2}/r_{i-1})$$

$$q_i = \text{quotient}(r_{i-2}/r_{i-1})$$

$$a_i = -q_i a_{i-1} + a_{i-2}$$

(d) $b(x)^{-1} := a_i$

(e) Convert $b(x)^{-1}$ back to an 8-bit number

Use this algorithm to compute the inverses of 11100110 and 00110110. Show that the inverses are actually inverses (compute $(11100110)^{-1} \cdot (11100110)$ and likewise for 00110110).

2. (a) Use the simplified DES algorithm for two rounds, and cipher block chaining to encode the message SKULLDUGGERY (using the 5-bit encoding of the alphabet we used before) with the key 001011010 and $C_0 = 111001000111$.

(b) How would Bob decode this message? Show that he gets the right message when doing so.