Understanding Cryptography **Homework No. 3** **Due Date:**

1. Generate the multiplication table for the extension field $GF(2^3)$ for the case that the irreducible polynomial is $P(x) = x^3 + x + 1$. The multiplication table is in this case a 8×8 table. (Remark: You can do this manually or write a program for it.)

2. Find all irreducible polynomials
   a) of degree 3 over GF(2),
   b) of degree 4 over GF(2).

3. In the following, we check the diffusion properties of AES after a single round.
   Let $W = (w_0, w_1, w_2, w_3) = (0x01000000, 0x00000000, 0x00000000\ 0x00000000)$ be the input in 32-bit chunks to a 128-bit AES. The sub-keys for the computation of the result of the first round of AES are $W_0, \ldots, W_7$ with 32 bits each are given by:
   $W_0 = (0x2B7E1516)$, $W_1 = (0x28AED2A6)$,
   $W_2 = (0xABF71588)$, $W_3 = (0x09CF4F3C)$,
   $W_4 = (0xA0FAFE17)$, $W_5 = (0x88542CB1)$,
   $W_6 = (0x23A33939)$, $W_7 = (0x2A6C7605)$.
   a) Compute the output of the first round of AES to the input W and the sub-keys $W_0, \ldots, W_7$.
   b) Compute the output of the first round of AES for the case that all input bits are zero.
   c) How many output bits have changed? Remark that we only consider a single round and after every further round, more output bits will be affected (avalanche effect).

4. Besides simple bit errors, the deletion or insertion of a bit yields even more severe effects since the synchronization of blocks is disrupted. In most cases, the decryption of subsequent blocks will be incorrect. A special case is the CFB mode with a feedback width of 1 bit. Show that the synchronization is automatically re-stored after K + 1 steps, where K is the block size of the block cipher.

5. In a company, all files which are sent on the network are automatically encrypted by using AES-128 in CBC mode. A fixed key is used, and the IV is changed once per day. The network encryption is file-based, so that the IV is used at the beginning of every file. You managed to spy out the fixed AES-128 key, but do not know the recent IV. Today, you were able to eavesdrop two different files, one with unidentified content and one which is known to be an automatically generated temporary file and only contains the value 0xFF. Briefly describe how it is possible to obtain the unknown initialization vector and how you are able to determine the content of the unknown file.

HAPPY NEW YEAR!