Abel Marin

Prof Joe

Cryptology

May 17, 2020

Assignment 3

1. GF(23) for P(x) = x3+x+1:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***x*** | ***0*** | ***1*** | ***x*** | ***x+1*** | ***x2*** | ***x2+1*** | ***x2+x*** | ***x2+x+1*** |
| ***0*** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ***1*** | 0 | 1 | x | x+1 | x2 | x2+1 | x2+x | x2+x+1 |
| ***x*** | 0 | x | x2 | x2+x | x+1 | 1 | x2+x+1 | x2+1 |
| ***x+1*** | 0 | x+1 | x2+x | x2+1 | x2+x+1 | x2 | 1 | x |
| ***x2*** | 0 | x2 | x+1 | x2+x+1 | x2+x | x | x2+1 | 1 |
| ***x2+1*** | 0 | x2+1 | 1 | x2 | x | x2+x+1 | x+1 | x2+x |
| ***x2+x*** | 0 | x2+x | x2+x+1 | 1 | x2+1 | x+1 | x | x2 |
| ***x2+x+1*** | 0 | x2+x+1 | x2+1 | x | 1 | x2+x | x2 | x+1 |

1. We can derive the keystream with XOR. This means that we would know what input was given for all blocks except the first one. Thus, we can brute force a key that produces the key from the known inputs. The IV can be derived by decrypting the first block’s keystream.
2. If the IV is not different for each execution of the encryption algorithm, then the confidentiality could be compromised. If the plaintext block of a message is known the output can be obtained from the ciphertext fairly easily. Once you have this then you can compute any new plaintext block from a new message that is encrypted using the same IV.
3. Problem 4
   1. When using ECB, the only block which would be affected should be only be the one containing the error xi.
   2. When using CBC, the blocks which would be affected should be the one containing the error xi and the next block xi+1.
   3. When using CBC, the blocks which would be affected should be the one containing the error xi, the next block xi+1 andany subsequent blocks.
   4. The error propagates to xi and a few additional blocks.
   5. For ECB, errors are contained to the block in which they occurred in. For CBC, the transmission errors will affect the block in which they occurred in and the next block. For CFB, transmission errors will affect the bit from the block it occurred on and the entire next block. For OFB, errors are limited to the bit where it occurred. For CTR, errors are limited to the bit where it occurred.