Abel Marin

Prof Joe

Cryptology

May 3, 2020

Assignment 2

1. In order to break this encryption, we will need 128 bits of ciphertext bits and plaintext bits. We then take stream bit and set it to the XOR of the ciphertext bit and the plaintext bit for each i = 1, 2, 3, ... 128, si = xi ⊕ yi. This would give you the stream bit for all 128 bits of the key stream.
2. The reason why a brute-force attack will fail is because for any ciphertext bit there is an equal 50% chance that the plaintext bit will be 0 and for 1. The same goes for the finding the key bit. Thus, if you only know the ciphertext, you cannot identify the plaintext or the key stream.
3. Problem 3
   1. S1(X1) ⊕ S1(X2) = 1110 while S1(X1⊕X2) = 0000. Thus 1110 does not equal 0000.
   2. S1(X1) ⊕ S1(X2) = 1001 while S1(X1⊕X2) = 1000. Thus 1001 does not equal 1000.
   3. S1(X1) ⊕ S1(X2) = 1010 while S1(X1⊕X2) = 1101. Thus 1010 does not equal 1101.
4. Problem 4. S1 = 14 = 1110, S2 = 15 = 1111, S3 = 10 = 1010, S4 = 7 = 0111, S5 = 2 = 0010, S6 = 12 = 1100, S7 = 4 = 0100, S8 = 13 = 1101
5. Problem 5
   1. There are 2 s-boxes that get different inputs compared to the all-zeroes case and they are S1 and S8.
   2. The minimum number of output bits of the S-boxes that will change according to the S-box design criteria is 4 since for each 1 bit changed there will be 2 output bits changed and 2 S-boxes will have an input changed.
   3. The output after the first round is S1 = 3 = 0011, S2 = 15 = 1111, S3 = 10 = 1010, S4 = 7 = 0111, S5 = 2 = 0010, S6 = 12 = 1100, S7 = 4 = 0100, S8 = 1 = 0001
   4. There were 6 bits which changed. These include 3 from S1, 2 from S8 and 1 from the left half.