ASSIGNMENT 5

CS-641

TEAM- Bullshot

Members –

Aman Tayal (180074)

Rohit Ranjan (180629)

Rishabh Kothary (180608)

For this assignment we were given to crack a crypto-system using plaintext attack. We reached the place where we could do plaintext attack using the following commands:

go->wave->dive->go->read.

Here we were told that there exists a Matrix A(8x8) with elements belonging to GF(2^7) and an exponentiation function(E) which could be viewed as 8x1 vector. It was given to us that the structure of the crypto-system is EAEAE where an input is an 8x1 vector belonging to GF(2^7) constructed over x^7+x+1.

Our first aim was to understand the mapping of input to bits. After looking through a few data we noticed that in every pair ‘ab’, ‘a’ varied from ‘f’ to ‘u’ (16 elements = 4 bits) and ‘b’ varies from ‘f’ to ‘m’(8 elements = 3 bits) Thus every pair of characters ‘ab’ constituted as an element of GF(2^7).

After understanding this mapping, we tried to understand something about the matrix. If there was something special going on or not. Indeed, it turned out to be special. It turned out to be lower triangular. To prove our claim, we took any random input and found the ciphertext corresponding to it say:

Plaintext: “ghghghjkfdshdjfk”

Ciphertext: “ksghkplqhrkqltlr”

And then changed just the last character (effectively changing the last element of the vector) and the results were as follows:

Plaintext: “ghghghjkfdshdjfg”

Ciphertext: “ksghkplqhrkqltfp”

We see that effectively just the last 2 characters (last element of the ciphertext vector) changed.

Now we changed the second last element of the plaintext vector and the results are as follows:

Plaintext: “ghghghjkfdshdhfg”

Ciphertext: “ksghkplqhrkqfrik”

We see that just the last elements of the ciphertext vector change.

Similarly, we kept changing the only (8 - i)th element of the plaintext vector and compared it with the output ciphertext and every time we found that only last i elements of ciphertext vector change, proving our claim that the matrix is lower triangular.

Our aim was to decrypt the password which was:

“ktirlqhtlqijmmhqmgkplijngrluiqlq”

We noticed that to decrypt it we did not need to know A and E specifically. Only by using the property that A is lower triangular we could find the corresponding plaintext. It out while encrypting the ith element of plaintext vector its encryption only depends on the first i-1 elements (Property of lower triangular matrix). So, we used kind of brute force approach to find the plaintext. We first ran a brute force run on the first element and ran it through the system and found the first plaintext element that gave rise to the first ciphertext element. Then, we fixed that element and ran brute force on second element and so on went sequentially and found that the correct plaintext. This Ciphertext consisted of 2 blocks so we had to run the process on each block. We found that the correct plaintext was (as in the input mapping):

“lhlgmjmkmglqlompmoltmglilqlmlgmh”

And in ASCII version it was:

“batuqkizynqckgar”

After entering the ASCII version of the plaintext, we cracked this level. Our method took about ($2x8x2^7$) = 2^{11} which is 2048 operations which is fairly efficient.

The code used to crack this round is attached in the folder.