Q1 Teamname

0 Points

Stuxnet

Q2 Commands

5 Points

List the commands used in the game to reach the ciphertext.

go, wave, dive, go, read

Q3 Analysis

50 Points

Give a detailed description of the cryptanalysis used to figure out the password. (Explain in less than 100 lines and use Latex wherever required. If your solution is not readable, you will lose marks. If necessary, the file upload option in this question must be used TO SHARE IMAGES ONLY.)

Since the EAEAE method works on matrices i.e. on numbers so first we need to find the encoding used here to convert input text to numbers. We used the most used encoding which is ASCII values. Since the total input block size is 128 bits and the output has size of 32 bits, so only 16 characters can be represented in this encoding. After analyzing the output we observed that all the outputs were ranged from f to u. Also since the input was of 8 bytes and the field was 128 so we could only have inputs ranging from 'ff' to 'mu'. All the input strings consisting of 128 different characters have their respective unique strings.

We tried an idea of fixing 7 bytes as constant and varying 1 byte and observing output like C^7P , we also tried the same approach by varying 1 byte at different positions like C^6PC. After analysis, we found out that after changing the i^{th} byte of input, it changes all bytes of output after i^th bit. After observing this our intuition said that this could be a lower triangular matrix. We also observed that whenever the input plain text has $I_0...I_j =' ff'$ we get ciphertext $C_0...C_j =' ff'$ and when we change the inputs from say $I_0..I_kI_{k+1}...I_7$ to $I_0..I_kI'_{k+1}...I_7$, the output gets changed only after k. This means that ff present in each row must be at the end row. Thus it is a lower triangular matrix.

So we have generated inputs from $C^{8-i}PC^{i-1}$. The E box has elements between 1 to 126 and Linear Transformation Matrix A had elements from GF(128) which we find out to be a lower triangular matrix. Since the matrix is lower triangular if X is the value of a non-zero input block (say i) then the corresponding block of output has the value $O = (a_{i,j}(a_{i,i} * x^{ei})^{ei})^{ei}$. We then performed operations over a finite field of 128 with generators $x^7 + x + 1$. For each pair of plaintext-ciphertext, we calculated possible values of e_i and $a_{i,j}$ and compared the output.

Block number-->	0	1	2	3	4	5	6	7
possible values of $a_{i,i}$ [0,:2] -->	[73, 84, 20]	[72, 101, 70]	[43, 17, 15]	[37, 126, 12]	[73, 112, 57]	[31, 11, 12]	[27, 14]	[38, 11, 58]
possible values of e_i [0,:2]-->	[18, 21, 88],	[53, 83, 118],	[39, 106, 109]	[22, 37, 68]	[45, 93, 116]	[9, 44, 74]	[20, 108]	[29, 43, 55]

After that we have found out every element next to each diagonal entry, as we need to eliminate pairs and find the non-diagonal elements as well.

Block number-->	0	1	2	3	4	5	6	7
final value of $a_{i,i}$	84	70	43	12	112	11	27	38
final value of e_i	21	118	39	68	93			

44 20 29

Having found every element of the matrix by checking the possible values between (0,127) and using final values of exponent matrix and above found values of linear transformation matrix. Thus the validity of O is also checked.

Similarly, we found the linear transformation matrix as follows,

$$A^T = \begin{bmatrix} 84 & 113 & 14 & 105 & 111 & 24 & 13 & 64 \\ 0 & 70 & 31 & 17 & 57 & 53 & 122 & 3 \\ 0 & 0 & 43 & 0 & 1 & 29 & 20 & 77 \\ 0 & 0 & 0 & 12 & 113 & 46 & 102 & 27 \\ 0 & 0 & 0 & 0 & 112 & 99 & 22 & 19 \\ 0 & 0 & 0 & 0 & 0 & 11 & 89 & 67 \\ 0 & 0 & 0 & 0 & 0 & 0 & 27 & 25 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 38 \end{bmatrix}$$

And the EXPONENT MATRIX is =

$$\begin{bmatrix} 21 & 118 & 39 & 68 & 93 & 44 & 20 & 29 \end{bmatrix}$$

After doing this we decrypted the password by checking all possible values for a block and checked whether out EAEAE function's output is same as the current password block or not. We did it in 2 halves as the password consisted of 32 letters. The password after decryption is --> uwpjeqmzff

No files uploaded

Q4 Password

5 Points

What was the final command used to clear this level?

```
uwpjeqmzff
```

Q5 Codes

0 Points

No files uploaded

Assignment 5

● **GRADED**

GROUP

YASH SARASWAT
MAYANK BANSAL
HIRAK MONDAL

View or edit group

TOTAL POINTS

60 / 60 pts

QUESTION 1 Teamname		**0** / 0 pts
QUESTION 2 Commands		**5** / 5 pts
QUESTION 3 Analysis	R	**50** / 50 pts
QUESTION 4 Password		**5** / 5 pts

QUESTION 5

Codes

0 / 0 pts