Q1 Team Name
0 Points

Group Name

Cryptosenpai

Q2 Commands
5 Points

List all the commands in sequence used from the start screen of this level to the end of the level

->go
->wave
->dive
->go
->read
->password
->c
->back
->read
->turtaannhm

Q3 Cryptosystem
5 Points

What cryptosystem was used at this level?

In this a block cipher known as EAEAE (Encrypted Alphabet with Alphabet Encryption) is utilized. This cryptosystem is vulnerable to the SASAS (Substitution and Symmetric Algorithm Substitution) attack, which is considered a weaker form of attack. Under finite field F{128} over F_2 i.e. GF(2^128) with irreducible polynomial of x^7 + x+1,

Uses 128 bit key, block size of 8 bytes, The transformation process involves the use of two key-dependent operations: a linear transformation utilizing a key matrix A (8x8) and an exponentiation transformation utilizing a key vector E(8x1). The input block undergoes the sequence EAEAE, with E being applied first, followed by A, and then E again. Both E and A are components of the key for this system. To obtain the encoded password, these transformations are performed on the input block, and the resulting output block is decoded.

Q4 Analysis
80 Points

Knowing which cryptosystem has been used at this level, give a detailed description of the cryptanalysis used to figure out the password.

The SASAS attack has a weaker form known as EAEAE. Upon inputting multiple plaintexts, we have observed that the resulting ciphertext only consists of 16 letters, ranging from 'f' to 'u.' To represent each letter, we have assigned 4 bits, namely 0000 to 1111 for 'f' to 'u.' Each byte is composed of two letters, and since they are elements of the F128 field within the 0 to 127 range, the MSB of each byte is 0. Therefore, the possible letter pairs that can be formed are from 'ff' to 'mu.'

Cryptanalysis

Observations
By inputting multiple plaintexts we observed that -

i) When the input plain text is 'ffffffffffffffff,' the output will also be 'fffffffff.'

ii) If the first 'i' bytes of the plain text are 'f's, then the first 'i' bytes of the ciphertext will also be 'f's.

iii) Changing the 'ith' byte of the plaintext will result in the corresponding byte of the ciphertext changing. If the plaintext 'P' is 'po, P1,..., P7,' where each 'P,' is one byte, then altering the input from 'Po, P1, Pk, Pk+1,..., P7' to 'Po, P1,.. Pk, P'k+1,..., P7' will cause the resulting ciphertexts to differ after the 'kth' byte.

Based on the above observations, it can be inferred that matrix 'A' is a lower triangular matrix.

To derive the transformation matrices 'A' and 'E,' matrix 'A' is of dimensions 8x8, while matrix 'E' is of dimensions 8x1. We use 'aj' to denote an element in 'A,' where 'i' represents the row index and 'j' represents the column index, and 'e' for an element in 'E.'

To generate the plaintext set for the attack, we utilize 'plaingen.py' and generate plaintext using the formula $C^{i-1}PC^{(8-i)}$, where 'C' is equal to 'ff' and 'P' belongs to the range [ff, mu], while 'i' belongs to [1, 8]. This method allows us to obtain eight sets of plaintext, each containing 128 plaintexts, where each plaintext in set 'i' only differs at the 'ith' byte value. These plaintexts are stored in 'plaintexts.txt.'

To obtain the ciphertext corresponding to each plaintext in 'plaintexts.txt,' we execute 'robot.py,' a Python script that establishes a connection to the game server using the 'pexpect' library, inputs commands in order, and passes plaintext to obtain the corresponding ciphertext. The resulting ciphertext is stored in 'ciphertexts.txt.'

It is known that matrix 'A' is a lower triangular matrix, and we can derive it using the formula

$$C = (A * (A * (P)^E)^E)^E .....1$$

, where 'P' represents the plaintext, and 'C' represents the ciphertext. Our goal is to identify the possible diagonal elements of matrix 'A' and the elements of 'E.'

During the encryption process, various mathematical operations are performed including exponentiation, linear transformation, and addition using XOR of integers. The process involves using Field F128 and modulo $x^7 + x + 1$, which is an irreducible polynomial over F2. To determine the diagonal elements of A and elements of E, the plaintext and ciphertext pairs are iterated over values ranging from 0 to 127 for A and 1 to 126 for E. The purpose of this iteration is to check whether the plaintexts can be successfully encrypted to ciphertexts. The resulting values where the plaintexts successfully map to ciphertexts are then stored for future use.

ith Byte	Possible Values of a[i,i](Diagonal)	Possible Values of E
0	[84, 67]	[20, 108]
1	[46, 63, 70]	[45, 93, 116]
2	[105, 43, 107]	[17, 41, 69]
3	[12, 8, 104]	[78, 85, 91]
4	[118, 112, 20]	[40, 89, 125]
5	[106, 11, 70]	[10, 54, 63]
6	[123, 27, 63]	[18, 21, 88]
7	[38, 61, 125]	[17, 41, 69]

The next step is to identify the non-diagonal elements of A and eliminate some pairs of (a,e). To achieve this, we iterate through the plaintext-ciphertext pairs with (a,i, ei), searching for values that satisfy equation 1 as mentioned earlier.

ith Byte	Possible Values of A	Possible Values of E

0	84		20
1	70		116
2	43		41
3	12		78
4	112		89
5	11		54
6	27		21
7	38	.	17

To find ai,j we have to know all values of set

$$Z_{i,j} = (a_{n,m} | n > m, j <= n, m <= i) \cap (a_{n,n} \mid j \ <= \ n)$$

Linear Transformation Matrix:

$$A = \begin{pmatrix} 84 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 70 & 0 & 0 & 0 & 0 & 0 & 0 \\ 12 & 29 & 43 & 0 & 0 & 0 & 0 & 0 \\ 127 & 21 & 30 & 12 & 0 & 0 & 0 & 0 \\ 96 & 37 & 7 & 110 & 112 & 0 & 0 & 0 \\ 30 & 49 & 24 & 43 & 111 & 11 & 0 & 0 \\ 23 & 121 & 22 & 100 & 0 & 93 & 27 & 8 \\ 94 & 12 & 81 & 29 & 12 & 69 & 29 & 38 \end{pmatrix}$$

Final Exponent Vector is :
E = [20, 116, 41, 78, 89, 54, 21, 17]

To decrypt the Password

To decrypt the password, the A transformation matrix and E exponent vector discussed earlier are used. The decryption process involves reversing the applied transformation. Specifically, for each 8 byte block of encrypted password (p), the following operation is performed to obtain the 8 byte decrypted password:

E_inv (A_inv (E_inv (A_inv (E_inv(p))))

Our encrypted password is
'lhisiniokohpkrmsiifqgfglhrikgqfq'
Encrypted Block 1 = 'lhisiniokohpkrms'
Encrypted Block 2 = 'iifqgfglhrikgqfq'

Decrypted Block 1 ASCII = [116, 117, 114, 116, 97, 97, 110, 110]
Decrypted Password1 = 'turtaann'
Decrypted Block 2 ASCII = [104, 109, 48, 48, 48, 48, 48, 48]
Decrypted Password2 = 'hm000000'
Decrypted Password:

'turtaannhm000000'

We assumed '000000' at end to be padding and tried

'turtaannhm'

as password for level and successfully cleared it.

Q5 Password
10 Points

What was the password used to clear this level?

turtaannhm

Q6 Code
0 Points

Please add your code here. It is MANDATORY.

Cryptosenpai Assignment 5.zip Download

```
1  Binary file hidden. You can download it using the
```

```
button above.
```

Assignment 5

Graded

Group

Rumit Pingleshwar Gore
Kuruma Abhinav
VAMSEE KRISHNA KAKUMANU
View or edit group

Total Points

100 / 100 pts

Question 1

Team Name — **0** / 0 pts

Question 2

Commands — **5** / 5 pts

Question 3

Cryptosystem — **5** / 5 pts

Question 4

Analysis — **80** / 80 pts

Question 5

Password — **10** / 10 pts

Question 6

Code — **0** / 0 pts