CS 641 : ASSIGNMENT : PART 5 : SCHUTZSAS

A PREPRINT

Srinjay Kumar
170722

Abhyuday Pandey
170039

Kumar Shivam
170354

March 5, 2020

1 Path to the Cipher Text

The keyword used to get to the cipher text are :

- go
- wave
- dive
- go
- read

2 Available Text

The text we get on the final screen is :

"This is another magical screen. And this one I remember perfectly... Consider a block of size 8 bytes as 8 x 1 vector over F_{128} – constructed using the degree 7 irreducible polynomial $x^7 + x + 1$ over F_2. Define two transformations: first a linear transformation given by invertible 8 x 8 key matrix A with elements from F_{128} and second an exponentiation given by 8 x 1 vector E whose elements are numbers between 1 and 126. E is applied on a block by taking the i^{th} element of the block and raising it to the power given by i^{th} element in E. Apply these transformations in the sequence EAEAE on the input block to obtain the output block. Both E and A are part of the key. You can see the coded password by simply whispering 'password' near the screen..."

The information that we can derive from the above text is :

- The encryption algorithm used is a form of **Block Cipher**.
- The size of the block in case of this cipher is 8 bytes.
- The irreducible polynomial for the linear transformation is $x^7 + x + 1$.
- The entries in the exponentiation matrix have numbers lie between 1 and 126.

3 Ciphertext

- The text we got does not give us any hint about the ciphertext.
- In the last assignment, we got the ciphertext by entering password on the last screen.
- We entered the string "password" on the last screen.
- After entering the string "password", we got the string "ktirlqhtlqijmmhqmgkplijngrluiqlq".
- Therefore, the ciphertext for this problem is "ktirlqhtlqijmmhqmgkplijngrluiqlq".

4 Operations

There are two operations in this cipher algorithm :

- **Linear Transformation** : It is an 8 x 8 invertible matrix A. We will denote this matrix as :

$$A = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} & a_{04} & a_{05} & a_{06} & a_{07} \\ a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\ a_{20} & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} \\ a_{30} & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} & a_{37} \\ a_{40} & a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} & a_{47} \\ a_{50} & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & a_{56} & a_{57} \\ a_{60} & a_{61} & a_{62} & a_{63} & a_{64} & a_{65} & a_{66} & a_{67} \\ a_{70} & a_{71} & a_{72} & a_{73} & a_{74} & a_{75} & a_{76} & a_{77} \end{bmatrix}$$

  - According to the question, the plaintext will be given in the form of 8 x 1 column vector.
  - We will denote the plaintext vector as P and the matrix will be denoted as :

$$P = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix}$$

  - The resultant after this operation can be given by the multiplication of two matrices AP which will give a 8 x 1 column vector.

- **Exponentiation** :
  - Exponentiation matrix will be 8 x 1 matrix and will be denoted by E.
  - The elements of the matrix will be :

$$E = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \end{bmatrix}$$

  - After operating E on P, we get :

$$E(P) = \begin{bmatrix} v_0^{e_0} \\ v_1^{e_1} \\ v_2^{e_2} \\ v_3^{e_3} \\ v_4^{e_4} \\ v_5^{e_5} \\ v_6^{e_6} \\ v_7^{e_7} \end{bmatrix}$$

5 Decryption

- There are two key elements in the cipher algorithm, the linear transformation matrix A and the exponentiation matrix E.

5.1 Characteristics of E and A

- The exponentiation matrix will be a byte to byte operation. This leaves us to look just the operation happening with A.
- The linear transformation matrix does some sort of diffusion between the different bytes.

- We then did a Known Plaintext attack on the cipher.
- We sent a lot of plaintexts to the server to be converted to ciphertexts and did not find any clear correlation.
- We then sent plaintexts of the form P_{ij} where only the j^{th} index of the matrix P is a non-zero entry j where j lies between 1 and 126.

$$P_{ij} = \begin{bmatrix} 0 \\ 0 \\ j \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

- After getting the ciphertexts corresponding to all the plaintexts of the form P_{ij}, we found out some interesting properties.
  - $C_{ij} = AP_{ij}$, where C_{ij} is the ciphertext corresponding to the plaintext P_{ij}.
  - We found that the bytes in C_{ij} from the position 0 to $i-1$ are all zeroes.
  - All the bytes onwards from the i^{th} byte are all non-zero.
  - Therefore, we find out that i^{th} byte in P_{ij} affects only the bytes from the i^{th} to the last byte in C_{ij}.
  - So, in the matrix A, for any column i we have the initial i terms of that column 0.
- Therefore, the matrix A is a lower triangular matrix i.e., all the elements above the diagonal in the matrix are zero.

$$A = \begin{bmatrix} a_{00} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{20} & a_{21} & a_{22} & 0 & 0 & 0 & 0 & 0 \\ a_{30} & a_{31} & a_{32} & a_{33} & 0 & 0 & 0 & 0 \\ a_{40} & a_{41} & a_{42} & a_{43} & a_{44} & 0 & 0 & 0 \\ a_{50} & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & 0 & 0 \\ a_{60} & a_{61} & a_{62} & a_{63} & a_{64} & a_{65} & a_{66} & 0 \\ a_{70} & a_{71} & a_{72} & a_{73} & a_{74} & a_{75} & a_{76} & a_{77} \end{bmatrix}$$

5.2 Exponentiation Matrix

- We will construct a matrix EXP with 126 rows and 126 columns.
- From the matrix, the element $EXP[i][j]$, the element in the i^{th} row and the j^{th} column gives the entry i^j.
- We will calculate this entire matrix before beginning our attack. The dimension of the matrix will be 126 x 126.
- The exponentiation will be done in the finite field with the irreducible polynomial $x^7 + x + 1$.

5.3 Bytes Relation

- We then choose such a plaintext which does not affect other bytes in the ciphertext.
- For our procedure we choose the plaintexts of the form

$$P = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ v_7 \end{bmatrix}$$

- After operating $EAEAE$, we get the element in the ciphertext to be

$$(a_{77}(a_{77}(v_7)^{e_7})^{e_7})^{e_7}$$

- We repeat the above process with all the possible values of v_7 ranging from 1 to 126.

Table 1: Actual Key

Pair	Possibility 1	Possibility 2	Possibility 3
(a_{00}, e_0)	$(100, 85)$	$(87, 78)$	$(25, 91)$
(a_{11}, e_1)	$(2, 103)$	$(51, 99)$	$(56, 52)$
(a_{22}, e_2)	$(40, 38)$	$(6, 2)$	$(89, 87)$
(a_{33}, e_3)	$(60, 98)$	$(22, 84)$	$(50, 72)$
(a_{44}, e_4)	$(16, 116)$	$(39, 45)$	$(59, 93)$
(a_{55}, e_5)	$(87, 38)$	$(93, 2)$	$(121, 87)$
(a_{66}, e_6)	$(14, 66)$	$(37, 77)$	$(96, 111)$
(a_{77}, e_7)	$(91, 16)$	$(54, 61)$	$(103, 50)$

5.4 Diagonal Attack

- We will take the entry a_{77} of the matrix A and the entry e_7 of the matrix E.
- Therefore, we can get $(a_{77}(a_{77}(v_7)^{e_7})^{e_7})^{e_7}$ by doing the attack.
- We will now try to guess the possibilities for a_{77} and e_7.
- There are 128 possibilities each for a_{77} and e_7.
- We can calculate the expression $(a_{77}(a_{77}(v_7)^{e_7})^{e_7})^{e_7}$ for each of the possibilities of a_{77} and e_7.
- We found out that three pairs of a_{77} and e_7 give the same result as the one obtained from the plaintext attack.

$$AP = A \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ v_6 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ v_6 a_{66} \\ v_6 a_{67} \end{bmatrix} = C$$

- In the above analysis, we can see that the 7^{th} term of C depends only on a_{66}.
- Therefore, we can see that $EAEAE$ on P gives $(a_{66}(a_{66}(v_6)^{e_6})^{e_6})^{e_6}$ for c_6.
- Again, we tried for all the possibilities of a_{66} and e_6 and we got three possible pairs of a_{66} and e_6.
- Similar analysis can also be done about the element v_0 ... v_5.
- Therefore, we know have a maximum of three possible tuples for each of the pairs a_{00}, e_0, ... a_{77}, e_7.
- Some possible values for the tuple are being depicted in the table.

5.5 Second Line Attack

- We will now try to find the elements of the line below the diagonal, i.e. the elements of the form $a_{i+1,i}$.
- The element to be found are $a_{10}, a_{21}, a_{32}, a_{43}, a_{54}, a_{65}, a_{76}$.
- **Finding** a_{76} :
  - We will take plaintext of the form

$$P = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ v_6 \\ 0 \end{bmatrix}$$

- Executing EAEAE on the plaintext P will give the output

$$C = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ (a_{66}(a_{66}(v_6)^{e_6})^{e_6})^{e_6} \\ (a_{77}(a_{76}(v_6)^{e_7})^{e_7} + a_{76}(a_{76}(v_6)^{e_7})^{e_7})^{e_7} \end{bmatrix}$$

- We observe that the term c_7 depends on $e_7, e_6, a_{66}, a_{76}, a_{77}$.
- In the above terms, we have the following number of possibilities in the Table 2.
- For each of the possibilities we use 10 random values from 1 to 126 for v_6.
- We check if the value calculated by the formula $(a_{77}(a_{76}(v_6)^{e_7})^{e_7} + a_{76}(a_{76}(v_6)^{e_7})^{e_7})^{e_7}$ equals the actual value for c_7 we get from the known plaintext attack.
- After checking through all the values, we find that only one set of values are possible for $e_6, e_7, a_{66}, a_{76}, a_{77}$.
- Therefore, we have successfully calculated the values of $e_6, e_7, a_{66}, a_{76}, a_{77}$.

- **Finding** a_{65} :
  - We will take plaintext of the form

$$P = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ v_5 \\ 0 \\ 0 \end{bmatrix}$$

  - Executing EAEAE on the plaintext P will give the output

$$C = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ (a_{55}(a_{55}(v_5)^{e_5})^{e_5})^{e_5} \\ (a_{66}(a_{65}(v_5)^{e_6})^{e_6} + a_{65}(a_{65}(v_5)^{e_6})^{e_6})^{e_6} \\ m \end{bmatrix}$$

  - We observe that the term c_6 depends on $e_5, e_6, a_{55}, a_{65}, a_{66}$.
  - In the above terms, we have the following number of possibilities in the Table 3.
  - For each of the possibilities we use 10 random values from 1 to 126 for v_5.
  - We check if the value calculated by the formula $(a_{66}(a_{65}(v_5)^{e_6})^{e_6} + a_{65}(a_{65}(v_5)^{e_6})^{e_6})^{e_6}$ equals the actual value for c_7 we get from the known plaintext attack.
  - After checking through all the values, we find that only one set of values are possible for $e_5, e_6, a_{55}, a_{65}, a_{66}$.
  - Therefore, we have successfully calculated the values of $e_5, e_6, a_{55}, a_{65}, a_{66}$.

- **Finding** $a_{54}, a_{43}, a_{32}, a_{21}, a_{10}$:
  - The procedure for calculating $a_{54}, a_{43}, a_{32}, a_{21}, a_{10}$ is similar to the process for calculating a_{76}.
  - In the process for calculating $a_{54}, a_{43}, a_{32}, a_{21}, a_{10}$, we will also calculate $e_0, e_1, e_2, e_3, e_4, e_5$ along the way.

- Now, we have successfully calculating the values a_{10} .. a_{76}, a_{00} .. a_{77} and e_0 .. e_7.

- The values of the matrix E can be given by

$$E = \begin{bmatrix} 85 \\ 52 \\ 38 \\ 72 \\ 116 \\ 38 \\ 66 \\ 50 \end{bmatrix}$$

5.6 Calculating Rest of the Matrix

- Calculating the 3^{rd} line
  - We will be finding the elements of the form $a_{i+2,i}$ i.e., we will be calculating the elements a_{20}, a_{31} .. a_{75}.
  - **Calculating** a_{75}
    * We will use the plaintext of the form

$$P = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ v_5 \\ 0 \\ 0 \end{bmatrix}$$

    * Executing $EAEAE$ on P will give the C.
    * The element c_7 will depend on $e_5, e_6, e_7, a_{66}, a_{55}, a_{77}, a_{65}.a_{76}, a_{75}$.
    * Only a_{75} is unknown of the above dependencies and there are 126 possible values ranging from 1 to 126.
    * For each of the possible values, we try with 10 random plaintext values for v_5 and find the appropriate value of a_{75} which give correct values for all the ten random plaintexts.
    * Correct values imply that the value obtained from the plaintext attack is equal to the value computed with the help of chosen a_{75}.
    * Therefore, we have successfully calculated a_{75}.
  - With analysis similar to that for calculating a_{75}, we can successfully calculate a_{20}, a_{31} .. a_{64}.
- With analysis similar to that for calculating the 3^{rd} line, we can successfully calculate the elements in the lines $4, 5, 6, 7, 8$. The elements for each line are given in Table.
- Now, we have successfully calculated all the elements of the matrix A.
- The values of the matrix A can be given by

$$A = \begin{bmatrix} 100 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 122 & 56 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 121 & 40 & 0 & 0 & 0 & 0 & 0 \\ 10 & 97 & 77 & 50 & 0 & 0 & 0 & 0 \\ 58 & 14 & 78 & 10 & 16 & 0 & 0 & 0 \\ 9 & 76 & 114 & 116 & 92 & 87 & 0 & 0 \\ 104 & 30 & 98 & 92 & 104 & 44 & 14 & 0 \\ 13 & 91 & 54 & 58 & 113 & 17 & 37 & 103 \end{bmatrix}$$

6 Deriving Input

- We will now develop a methodology to derive plaintext from the ciphertext.
- Initially, we will try to see the impact of different bytes in plaintext in bytes in the ciphertext.

- We will take the plaintext P to see the effect. P will be denoted by

$$P = \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix}$$

- The ciphertext after operating $EAEAE$ on P will be

$$AP = A \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix} = \begin{bmatrix} f(v_0) \\ f(v_0, v_1) \\ f(v_0, v_1, v_2) \\ f(v_0, v_1, v_2, v_3) \\ f(v_0, v_1, v_2, v_3, v_4) \\ f(v_0, v_1, v_2, v_3, v_4, v_5) \\ f(v_0, v_1, v_2, v_3, v_4, v_5, v_6) \\ f(v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7) \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = C$$

- We know c_0 .. c_7 since they constitute the ciphertext.
- The plaintext bytes v_0 .. v_7 are unknown and need to be calculated. Each of them have 126 possible values.
- **Calculating** v_0
  - According to our analysis, c_0 depends only on v_0.
  - We can iterate for all the 126 possible values of v_0 and for exactly one value of v_0, we would get the correct value of c_0.
  - Therefore, we have successfully calculated v_0.
- **Calculating** v_1
  - According to our analysis, c_0 depends only on v_0 and v_1 and we already know v_0.
  - We can iterate for all the 126 possible values of v_1 and for exactly one value of v_1, we would get the correct value of c_1.
  - Now, we know v_1.
- We can successfully calculate the values v_2 .. v_7 by using similar method to that of the above one for calculating v_2.

7 Encryption of Ciphertext

- The ciphertext for this problem is "ktirlqhtlqijmmhqmgkplijngrluiqlq".
- We observed that the characters of the ciphertext are always in range $f - u$ which is similar to the previous assignment, so we quickly concluded that $f - u$ are hexadecimal numbers from 0 to F as they are precisely 16 in number.

$$f = 0000$$
$$g = 0001$$
$$i = 0010$$
$$............$$
$$t = 1110$$
$$u = 1111$$

- Also, two characters combine together to form 1 byte of ciphertext.
- The total number of characters in the ciphertext is 32, therefore, we have a total of 16 bytes and 2 blocks of ciphertext.

Table 2: Number of Possibilities

Element	Possibilities
(e_7, a_{77})	3
(e_6, a_{66})	3
a_{76}	126

Table 3: Number of Possibilities

Element	Possibilities
(e_6, a_{66})	1
(e_5, a_{55})	3
a_{65}	126

8 Decrypting the Ciphertext

- We now derive the plaintext from the ciphertext by using the methodology mentioned in Section 6.
- Using this method on the "ktirlqhtlqijmmhqmgkplijngrluiqlq", we get "lhlgmjmkmglqlompmoltmglilqlmlgmh".

9 Get the Password

- We now have the plaintext "lhlgmjmkmglqlompmoltmglilqlmlgmh" and we tried that as our password but we were unsuccessful.
- Next, we tried to somehow derive some sense from the ASCII values.
- ASCII values require a byte for each character. Therefore, we will require 2 characters to get an ASCII value.
- After processing, we get the password "batuqkizynqckgar".

```
Password :  batuqkizynqckgar
```

10 Conclusion

- We were able to break the 3 round DES with just 1016 plain-texts by chosen plaintext attack.
- The password for this level is mentioned in the previous section.
- Fully automated code for this process is in the folder.

Table 4: Actual Key

Pair	Binary 1	Decimal	Character
lh	01100010	98	b
lg	01100001	97	a
mj	01110100	116	t
mk	01110101	117	u
mg	01110001	113	q
lq	01101011	107	k
lo	01101001	105	i
mp	01111010	122	z
mo	01111001	121	y
lt	01101110	110	n
mg	01110001	113	q
li	01100011	99	c
lq	01101011	107	k
lm	01100111	103	g
lg	01100001	97	a
mh	01110010	114	r