Project1: Breaking a Simple Cipher
Ramesh Adhikari

Problem: Suppose you know the following pair of plaintext and ciphertext, find out the key used in the encryption.

As per the given algorithm, to find the ciphertext if we have plaintext and key. Let's take some random plaintext and key to calculate the ciphertext to understand how it works so that we can apply the reverse way to find the key of the given question:

Suppose we have Plaintext and Key as below:

Plaintext (P): F5EF5D981B5DB510 and **Key (k):** abcdefabcdefabcd

Lets use algorithm step by step to find the ciphertext

B_Plaintext (P)=
1111010111101111010111011001100000011011010111011011010100010000

B_key (K)=
1010101111001101111011111010101111001101111011111010101111001101

1. Compute D = Plaintext (P) XOR Key (K)

   P_XOR_K (D) = 0101111000100101
   01100100011001111010110101100100001111011011101

2. Compute E = D « 17, where « is rotate left operation.

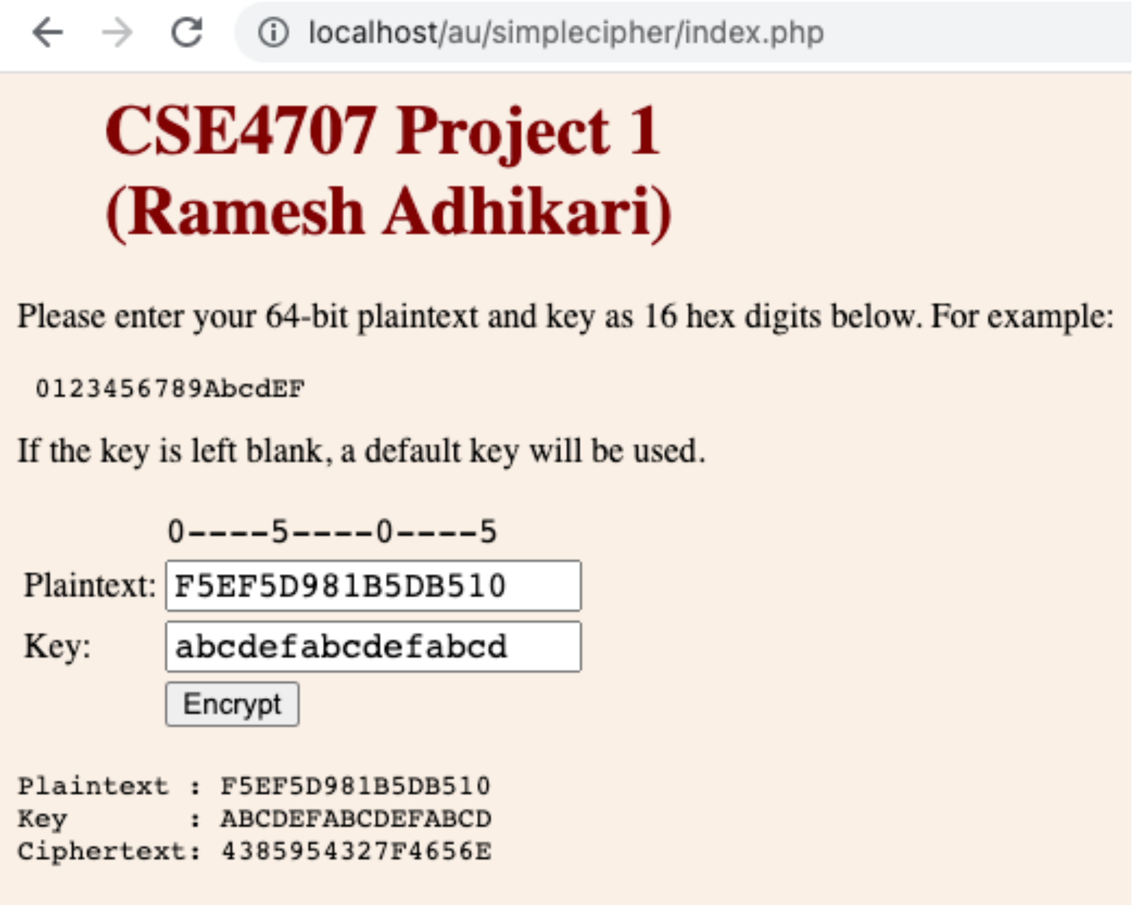
   Rotate_and_Merge(E)=011001000110011110101101011001000011110110
   1110101011110001000101

   Hex_of_E= 6467AD643DBABC45

3. Perform S-Box on each byte of E to produce the ciphertext C.

So ciphertext: 4385954327F4656E

Now, verify this calculated Ciphertext by executing given PHP program and we can found same Cipher which is attached below.



CSE4707 Project 1 (Ramesh Adhikari)

Please enter your 64-bit plaintext and key as 16 hex digits below. For example:

```
0123456789AbcdEF
```

If the key is left blank, a default key will be used.

```
           0----5----0----5
Plaintext: F5EF5D981B5DB510
Key:       abcdefabcdefabcd
```

```
Plaintext : F5EF5D981B5DB510
Key       : ABCDEFABCDEFABCD
Ciphertext: 4385954327F4656E
```

As of now we understand how the algorithm works, now follow the reverse step to find the key if we have plaintext and ciphertext.

Given plaintext and Ciphertext in question are as below:

Plaintext= F5EF5D981B5DB510

Ciphertext=2AAA8E541A37D5AF

Let’s first use S-Box to obtain E and then we can apply 17-bit binary right operation to obtain D and key (K) can be found by an XOR operation of the plaintext(P) and D.

1. Find the equivalent S-Box of Chphertext
   S_BOX_ Chphertext (E) = 9562e6fd43b2b51b
   Convert this hex to binary
   B_S_BOX_ Chphertext =
   10010101011000101110011011111101010000111011001
   01011010100011011
2. Rotate 17 bits right operation to find D
   Rotated_S_BOX_Chiphertext (D)=
   0101101010001101110010101011000101110011011111101010000111011
   001

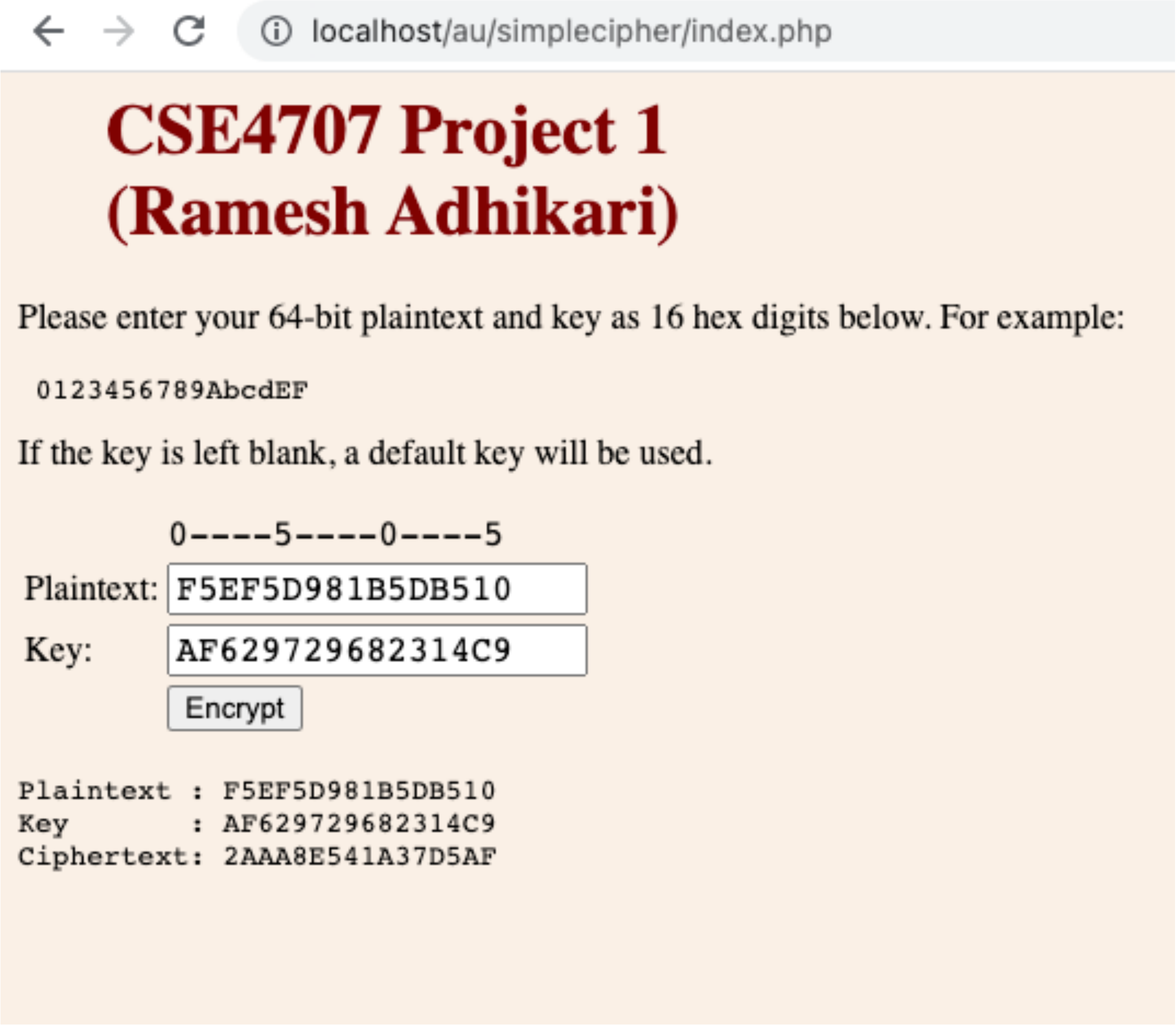
   Binary of plaintext(P)=
   1111010111101111010111011001100000011011010111011011010100010
   000

3. Now XOR P and D to obtain key (K) =
   1010111101100010100101110010100101101000001000110001010011001
   001

   Key(K)= AF629729682314C9

So the required solution key is **AF629729682314C9**

Now we can verify this key with the given PHP code and see whether this key with given plaintext generate the same mention Ciphertext or not. The executing programs gives the same Ciphertext which is also shown in below figure.



CSE4707 Project 1 (Ramesh Adhikari)

Please enter your 64-bit plaintext and key as 16 hex digits below. For example:

```
0123456789AbcdEF
```

If the key is left blank, a default key will be used.

```
           0----5----0----5
Plaintext: F5EF5D981B5DB510
Key:       AF629729682314C9
```

```
Plaintext : F5EF5D981B5DB510
Key       : AF629729682314C9
Ciphertext: 2AAA8E541A37D5AF
```