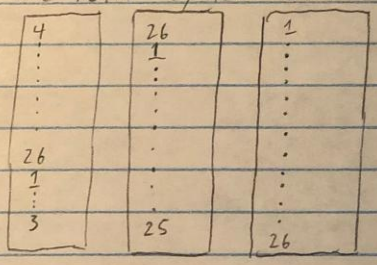
CSI 4108 A2
Aaron Ng (300176901)
Oct 17, 2022

Q1)

Assignment #2

Q1) After 20 characters have been encrypted, the rotor system will be as follows:



My plaintext will be "AARON IS FUN"

Plaintext	Output (fast)	Output (med)	Output (slow)
A	H	T	E
A	W	M	I
R	A	Y	Q
O	Z	Q	D
N	X	N	Z
I	K	Y	Q
S	K	Y	Q
F	W	X	N
U	M	P	R
N	M	P	R

CSI 4108 A2
Aaron Ng (300176901)
Oct 17, 2022

Q2)

The following was my 4-bit s-box

```
# My 4-bit s-box
inputX = [0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]
outputY = [10,9,8,3,2,5,13,6,1,4,11,15,14,12,0,7]
```

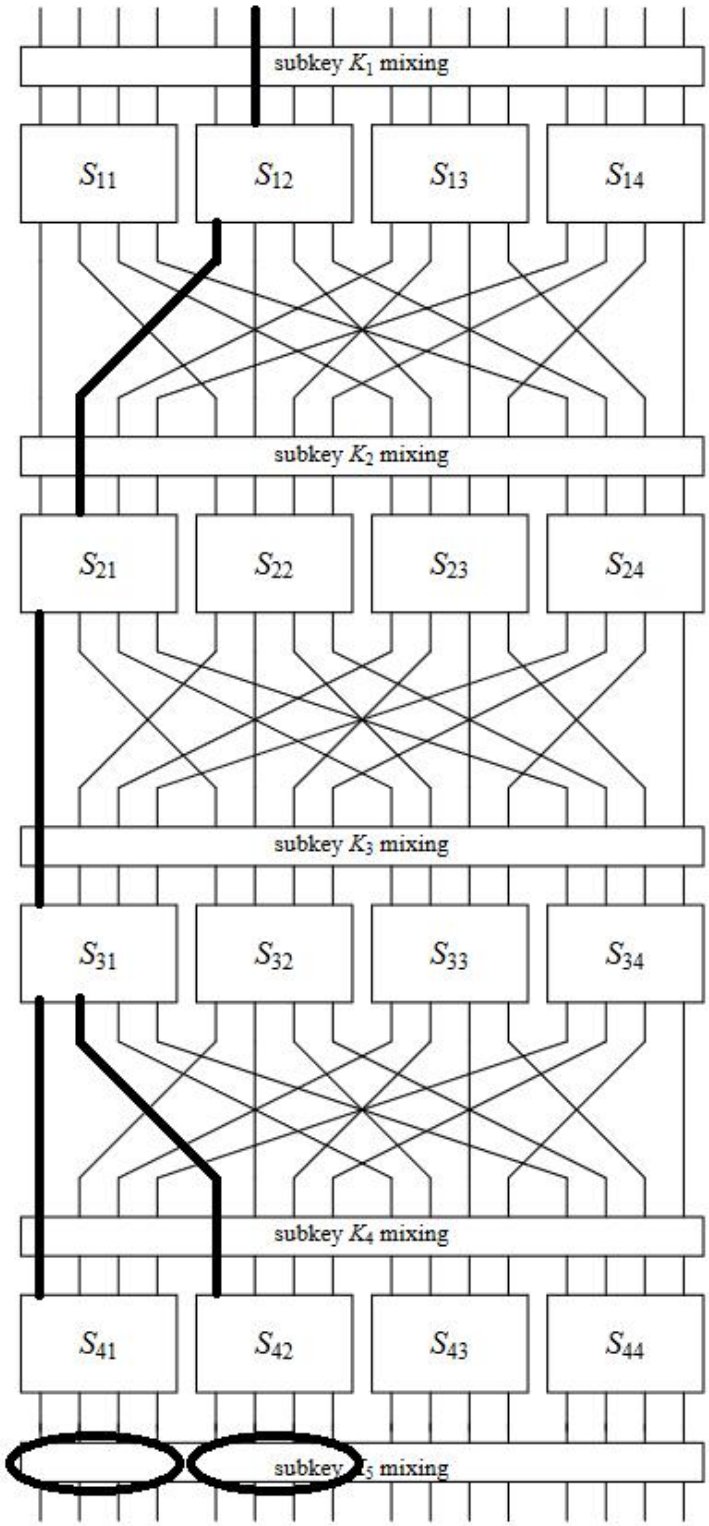
A difference distribution table was created from the s-box.
Refer to difference_distribution_table.py for code.

Difference Distribution Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	2	2	2	0	4	0	0	0	4	0	0	0	0
2	0	0	2	2	0	0	0	0	0	0	4	4	0	0	2	2
3	0	2	0	0	2	0	0	0	2	4	0	0	2	0	2	2
4	0	0	0	0	0	4	0	0	6	0	0	0	2	2	0	0	2
5	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	4	4
6	0	2	0	4	0	2	2	2	0	0	2	0	0	0	0	2
7	0	4	0	0	4	0	2	2	0	0	0	0	2	2	0	0
8	0	2	0	2	0	0	0	0	0	0	2	0	2	4	4	0	0
9	0	0	0	0	0	0	0	2	2	4	0	2	2	0	0	4	0
10	0	2	4	2	0	0	2	2	0	2	2	0	0	0	0	0
11	0	2	4	0	0	6	0	0	2	0	0	0	2	0	0	0
12	0	2	0	2	4	2	2	0	2	2	0	0	0	0	0	0
13	0	0	2	2	2	0	4	2	0	0	0	0	0	2	0	2
14	0	0	2	0	0	0	2	0	0	2	4	0	2	0	2	2
15	0	0	0	0	2	0	0	2	0	4	0	0	0	6	2	0

CSI 4108 A2
Aaron Ng (300176901)
Oct 17, 2022

The best differential characteristic was made using data from the difference distribution table.



K5,1 ... K5,4 K5,5 ... K 5,8

Probability of (1000 1000 0000 0000)

$$\frac{6}{16} \cdot \frac{6}{16} \cdot \frac{4}{16} = \frac{9}{256} = 0.0352$$

CSI 4108 A2
Aaron Ng (300176901)
Oct 17, 2022

Then, I generated 10,000 16-bit plaintext and encrypted them. Details of the code can be found in Encryption.py. The plaintext-ciphertext pairs can be found in pc-pairs.txt
I proceeded to attempt a differential cryptoanalysis attack. Details of code can be found in Differential_Attack.py. The results of the attack are shown in the frequency table below.

Round Keys	['51480', '5632', '5177', '16886', '21226\n']
Frequency Table of Differential Attack	0.0027 0.0035 0.0043 0.0041 0.0037 0.0026 0.0051 0.0039 0.0035 0.0037 0.0036 0.004 0.0037 0.004 0.0045 0.0043 0.0036 0.0037 0.0039 0.004 0.0038 0.004 0.0036 0.0038 0.0041 0.004 0.0041 0.0034 0.0044 0.0035 0.0045 0.003 0.0026 0.0041 0.0037 0.0043 0.0036 0.0046 0.0034 0.0038 0.006 0.0037 0.0036 0.0043 0.0045 0.0039 0.0042 0.0035 0.0042 0.0049 0.0037 0.0048 0.0028 0.0047 0.0036 0.0048 0.0041 0.0032 0.0029 0.0053 0.0041 0.0036 0.0033 0.0038 0.0036 0.0039 0.0034 0.0039 0.0037 0.0035 0.0044 0.0032 0.0039 0.0028 0.0049 0.0045 0.0037 0.0038 0.0042 0.004 0.0044 0.004 0.0038 0.0033 0.0051 0.0045 0.0044 0.0022 0.0051 0.0039 0.0049 0.0032 0.0038 0.0036 0.0035 0.0041 0.0047 0.0037 0.0034 0.0032 0.0037 0.0056 0.0029 0.0038 0.0042 0.0049 0.0036 0.0036 0.0035 0.0035 0.0049 0.0036 0.0052 0.0042 0.0043 0.0045 0.0043 0.0045 0.0036 0.0032 0.0047 0.0041 0.0044 0.0036 0.0042 0.0051 0.0036 0.0043 0.0029 0.003 0.0039 0.0047 0.0034 0.0038 0.003 0.0045 0.0041 0.0041 0.0029 0.0045 0.0045 0.0042 0.0042 0.0043 0.0027 0.0031 0.0034 0.0039 0.0039 0.0036 0.0044 0.0049 0.0044 0.0036 0.0034 0.0031 0.0044 0.0038 0.0032 0.0034 0.004 0.004 0.0031 0.0042 0.0038 0.0039 0.0036 0.0038 0.0036 0.0023 0.0044 0.0036 0.0042 0.0031 0.0041 0.0043 0.0038 0.004 0.0035 0.0035 0.0041 0.005 0.004 0.0049 0.0033 0.0051 0.0056 0.0048 0.0043 0.0026 0.0048 0.0039 0.004 0.004 0.0034 0.004 0.0038 0.0039 0.0043 0.0043 0.0042 0.0036 0.0031 0.0031 0.0049 0.0048 0.004 0.0031 0.0035 0.0036 0.005 0.0038 0.0028 0.0031 0.0037 0.0034 0.004 0.0039 0.0042 0.0038 0.0044 0.0031 0.004 0.0045 0.004 0.0054 0.0036 0.0025 0.0039 0.0036 0.0035 0.0036 0.0035 0.0038 0.0035 0.0037 0.0037 0.0041 0.0054 0.0035 0.0026 0.0042 0.0039 0.0041 0.0026 0.0043 0.005 0.0031 0.0039 0.0036 0.0042 0.0035 0.0034 0.0036 0.0045 0.0043
Highest Probability	0.006
Partial Subkey (dec)	40
Partial Subkey (hex)	28_ _
Actual Final Round Key	52EA

I was unable to find any partial subkey with noticeably high probability. I suspect I may have incorrectly implemented counting the frequency for the differential attack.

Since I worked alone, I “switched” Person1 and Person2 by generating a different set of round keys

Round Keys	['8124', '9645', '35912', '31504', '48138\n']
Frequency Table of Differential Attack	0.0046 0.0044 0.0046 0.0039 0.0053 0.0039 0.0033 0.0032 0.0032 0.0037 0.0037 0.0036 0.0044 0.005 0.0051 0.0033 0.0042 0.004 0.0042 0.004 0.0039 0.005 0.0036 0.0032 0.0045 0.0048 0.0048 0.0039 0.0033 0.0041 0.0028 0.0046 0.0052 0.0032 0.0048 0.0043 0.0044 0.0026 0.0043 0.0041 0.0036 0.0042 0.0042 0.0034 0.0039 0.0048 0.0051 0.0049 0.0041 0.0039 0.0033 0.0042 0.0044 0.0037 0.0047 0.0038 0.0035 0.0045 0.0027 0.0043 0.0043 0.0034 0.0048 0.0035 0.0048 0.0038 0.003 0.0035 0.0036 0.0047 0.0036 0.0038 0.0043 0.004 0.0035 0.0037 0.0045 0.0042 0.0036 0.0045 0.0037 0.004 0.0055 0.0041 0.0045 0.0035 0.0024 0.0043 0.0034 0.0041 0.0039 0.0039 0.0041 0.0037 0.0034 0.0035 0.0038 0.0043 0.0046 0.0034 0.0035 0.002 0.0039 0.004 0.0043 0.0045 0.0048 0.0036 0.0039 0.0045 0.0028 0.0043 0.0044 0.0048 0.0033 0.003 0.0039 0.0033 0.0036 0.0028 0.0036 0.0033 0.0037 0.0036 0.0041 0.0035 0.0036 0.0027 0.0033 0.0046 0.0033 0.0047 0.0028 0.0051 0.0047 0.0043 0.0036 0.0031 0.0045 0.003 0.0042 0.0031 0.0031 0.0037 0.005 0.0032 0.0038 0.0045 0.0034 0.0025 0.0045 0.004 0.0046 0.0027 0.0044 0.0034 0.0037 0.0029 0.0031 0.0037 0.004 0.0033 0.0047 0.004 0.0045 0.004 0.0044 0.0034 0.0035 0.0048 0.0041 0.0044 0.0039 0.0036 0.0042 0.0027 0.004 0.0046 0.0052 0.0044 0.005 0.0031 0.0031 0.0044 0.0041 0.0037 0.0041 0.0056 0.0041 0.0038 0.0034 0.0037 0.0033 0.0043 0.0042 0.0039 0.0048 0.0033 0.004 0.0023 0.0037 0.0043 0.0048 0.0034 0.0042 0.004 0.0044 0.0028 0.004 0.0037 0.003 0.0037 0.0041 0.0041 0.004 0.0046 0.0043 0.0048 0.0036 0.0045 0.0035 0.0035 0.0025 0.0048 0.0031 0.0027 0.0043 0.0029 0.0045 0.003 0.0044 0.0046 0.0046 0.0044 0.0044 0.0041 0.0035 0.0032 0.0048 0.0031 0.0035 0.0035 0.0038 0.0046 0.0031 0.0036 0.0029 0.0034 0.0031 0.0033 0.0034 0.004 0.0058 0.0038 0.0036 0.0034
Highest Probability	0.0058
Partial Subkey (dec)	252
Partial Subkey (hex)	FC_ _
Actual Final Round Key	BC0A

Again I was unable to find any partial subkey with significant high probability, hence why the guess for the partial subkey was incorrect.

CSI 4108 A2
Aaron Ng (300176901)
Oct 17, 2022

Q3)

Q3) $p = 787$, $q = 367$

$n = 288,829$

Let $s = 512$

$x_0 = 512^2 \bmod 288\,829$

$= 262\,144$

i	x_i	b_i
1	125740	0
2	48140	0
3	184533	1
4	66 647	1
5	210 247	1
6	255 533	1
7	97 914	0
8	50 399	1
9	96 975	1
10	167 214	0
11	141 622	0
12	216 295	1
13	160 921	1
14	26 588	0
15	157 181	1

* We will need 56-bit primes to match security of DES and 128-bit primes to match security of AES-128