TOBB ETÜ

Ekonomi ve Teknoloji Üniversitesi

Bilgi Güvenliği Yüksek Lisans Programı

Bil-581: Cryptography

Programming Assignment

Prepared by:

Zeynep Delal Mutlu

Discussed with:

Esra Nur Ayaz

Instructor:

Dr. Yeşem Kurt Peker

10.10.2019

Effect of change in plaintext:
Flipping a bit in the plaintext will result in flip of about 50% of the ciphertext bits.
Step 1: To make sure that your "flip bit" and "finding number of different bits" methods/operations work correctly follow these steps:

1. Use the following keytext plaintext ciphertext triple:
   `000102030405060708090a0b0c0d0e0f 00112233445566778899aabbccddeeff 69c4e0d86a7b0430d8cdb78070b4c55a`
2. Ask the user which bit (index 0-127) of the plaintext to flip.
3. Flip the bit of the plaintext at the desired index.
4. Encrypt the new plaintext in the triple with the keytext.
5. Compare the resulting ciphertext with the original ciphertext above and find how many bits were flipped.
6. Write this information on the screen in the following format:

   Plaintext: `00112233445566778899aabbccddeeff`
   Flip bit: `0`
   New Plaintext: `80112233445566778899aabbccddeeff`
   Ciphertext: `69c4e0d86a7b0430d8cdb78070b4c55a`
   New Ciphertext: `c4b6cc20a1961062ee8104adb441b569`
   Number of flipped bits: 65

Another example:

   Plaintext: `0011223344556677889aabbccddeeff`
   Flip bit: `78`
   New Plaintext: `0011223344556677889baabbccddeeff`
   Ciphertext: `69c4e0d86a7b0430d8cdb78070b4c55a`
   New Ciphertext: `219f41d14db0442822f6d9483b4c48ce`
   Number of flipped bits: 59

NOTE:

- ***Step-1 is completed succesfully. You can see this part in the computer programme.***
- ***In the programme, you will see general option menu which is asking for the operation. Option-2 is asking for input text number and bit number. The output is same with the format of above example.***

Step 2. To see the impact of flipping a bit of the plaintext on the ciphertext on more triples follow these:
For each triple in the AES_Triples.txt file,

1. Flip the bit of the plaintext at the desired index from Step 1.
2. Encrypt the new plaintext in the triple with the corresponding key
3. Compare the resulting ciphertext with the original ciphertext and find how many bits were flipped.

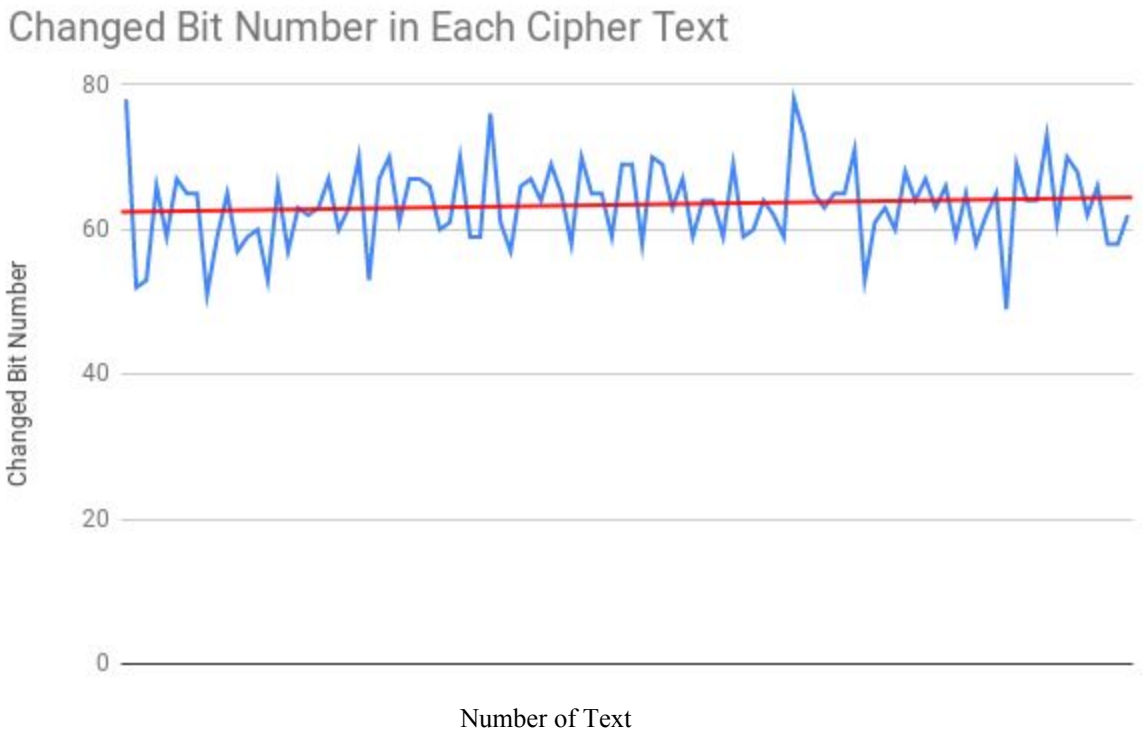
4. Write this information in a file called data.txt in the following format (separated by spaces):

Plaintext	toggle bit	# bits flipped in ciphertext
9c8427fbf8484791764e30e02187ffa1	78	67

NOTE:

- ➢ ***First 4 questions of Step-2 are completed successfully.***
- ➢ ***Option-1 of the general menu gives us all the text computed by changing one random bit number.***
- ➢ ***Option-2 of the general menu asks for text number and bit number. Also find the changed bits number.***
- ➢ ***Option-11 of the general menu changes a random bit of each key text and save the consequences in the changedKey.txt file.***

5. Use an external tool visualize your results (for example Excel).



6. Calculate and display the average number of bits flipped in your visualization. (Sum of the flipped bits in the ciphertext for the 100 entries divided by 100). Take a screenshot including the graph and the average to include in your submission.
   I calculated this part while I calculated changed bit number of each plain text. As you can see on the graph, the average (mean value) of the change bits number is around 63. And the consequences are almost equally distant to the mean line. This situation can be thought as distribution is almost homogeneous.

```
KEY TEXT BITS CHANGE

Plaintext                                Toggle Bit      Flip Bits       Percentage of Changed Bits

Average percentage of 100 changed cipher text: 49.78125

87bbb323c5fdb258112ac77880491aa5         1               57                      44.53125
3728766921894762de9dd1f477064fc9         44              58                      45.3125
0e63d33238cf5aa8fb0e6273f7026ef9         81              62                      48.4375
45112f1478a2d18b776d27c7d4e5b5ef         63              68                      53.125
672b697f15c8cd17d71e90c546906074         68              65                      50.78125
d3934de2860c68f694b86f8e6a86c2b2         10              60                      46.875
3efdef210668e8059b8ab12bbfe7be4e         3               64                      50.0
```

7. Analyze different aspects of this process. For example, you can try flipping another index and compare the averages. Or you can flip bits one by one on the same plaintext and check how many bits are flipped in the ciphertext for each flip.
   I have already done this part by changing a random bit of each text. It was experimental and each time I gave the similar average of changed bit number percentage. The average consequences mostly changes between 49% and %51. On the other hand, when I used same text number and same bit number I took exactly the same changing bits as expected.

8. Write a paragraph explaining your observations and conclusions.
   It is written below under the question 4-c.

What to Submit:

1. Include partner's name in your submission files.
   Esra Nur Ayaz

2. Your java source code properly styled and documented. Make sure to include both authors' names. Do NOT include AES.java and Util.java.
   Since I wrote the code with respect to package name, I should commit whole project in order to make homework more understandable.

3. Your data.txt file.
   I upload both text file
   - **data.txt(changed one bit from each plaintext) and**
   - **changedKey.txt(changed one bit from each keytext).**

   However, you can create your both txt files as well by using the general menu of the programme.

4. A Word file with names of group members included at the top including
   a. a screenshot of a successful run of Step 1,

First example;

```
Please write the number which text you choose(between 1 - 100)
Text No: 100
Please write the bit index which you want to change(between 0 - 127)
Bit No: 124
Plain text(not changed one): e950951fc249f235d6c8e7fcb6c84c44
Changed text(one selected bit is changed): e950951fc249f235d6c8e7fcb6c84c4c
Plain Text Encryted:
94 99 b0 40 54 55 53 15 a5 71 85 f0 6a 62 1c d7
Changed Text Encryted:
3b 33 98 93 98 e3 94 b0 0f ce 99 4c f0 e3 a5 9b
Number of flipped bits: 60
Percentage of difference: 46.875
```

Second example;

```
Please write the number which text you choose(between 1 - 100)
Text No: 45
Please write the bit index which you want to change(between 0 - 127)
Bit No: 2
Plain text(not changed one): 1e0941bee5f9f0f69829652ee7b83b00
Changed text(one selected bit is changed): 3e0941bee5f9f0f69829652ee7b83b00
Plain Text Encryted:
e6 83 eb 42 3a 1f 40 ef b6 d5 46 5c 8a 67 da 48
Changed Text Encryted:
14 43 21 75 9d 26 a7 b5 7e e9 49 f4 85 d6 68 99
Number of flipped bits: 63
Percentage of difference: 49.21875
```

b. screenshot from item 7 above,
I wrote a function which changes one random bit of each plain text and writes in data.txt file.

```
PLAIN TEXT BITS CHANGE

Plaintext                                Toggle Bit      Flip Bits       Percentage of Changed Bits

Average percentage of 100 changed cipher text: 49.875

9c8427fbf8484791764e30e02187ffa1         74              60                      46.875
87bbb323c5fdb258112ac77880491aa5         12              70                      54.6875
3728766921894762de9dd1f477064fc9         120             66                      51.5625
0e63d33238cf5aa8fb0e6273f7026ef9         46              68                      53.125
45112f1478a2d18b776d27c7d4e5b5ef         9               59                      46.09375
672b697f15c8cd17d71e90c546906074         88              55                      42.96875
d3934de2860c68f694b86f8e6a86c2b2         38              60                      46.875
3efdef210668e8059b8ab12bbfe7be4e         37              60                      46.875
2f212e6614332e3acbf9e18faaf7919a         115             69                      53.90625
8246d295f36a3a7a7aaa9849f235348b         53              56                      43.75
e61710b92b060e76f17a0d394407d8cf         91              59                      46.09375
5fca55b506594e05eb4d6234b0ed43bf         3               62                      48.4375
c493ab7a148a617b1aa56bce2a510ba4         27              69                      53.90625
42711bc8a716f581a20b02630ad8e74e         70              58                      45.3125
d73ddb21586720779c5026238c4fb5bc         123             57                      44.53125
```

c. paragraph for item 8 above,
I share all my observation under the other questions. To sum up, changing one bit in the plain text causes 50 percent change in cipher text. The same result applies to the keytext one bit change(question-5).

d. responses to these reflection questions (to be done individually):
   i. What was the most challenging part of this assignment?
   I had really hard time while I was trying to convert texts in hexadecimal and byte format. I tried to use some functions from Util library. However, I gave some meaningless consequences like -100. After that I realized this consequences caused because of negative numbers. However, I wanted to write my own specific functions for bit changing. It took time but I definitely understood what I am doing and what I should do for next steps.
   ii. What was the most enjoyable part of this assignment?
   After I finished all coding task, I tried my programme for many times. All the consequences were exactly what I expect. This is the most enjoyable time:)
   iii. What did you learn/practice when completing this assignment ?
   I can say that definitely I remembered decimal to hexadecimal and binary converting.
   iv. Your thoughts on working with your partner on this assignment.
   I did the coding assignment by myself. However, we discussed with Esra and we saw that our consequences are almost the same. Her flipped bit number changes between 62-66, so am I. While she working with visualization (graphs) she spend much more time than me. I just used some tool with my consequence with data.txt.

5. Examine the effect of change of a bit in the key. Provide a similar analysis for the effect of changes in key bits.
   I wrote code to see the consequences of changing bits int key text. You can observe this by using option 11 in the general menu of the programme. When I used this property, I saw that changing one bit in key text causes approximately 50% percent difference in cipher text again.

```
KEY TEXT BITS CHANGE

Plaintext                               Toggle Bit      Flip Bits       Percentage of Changed Bits

Average percentage of 100 changed cipher text: 49.78125

87bbb323c5fdb258112ac77880491aa5        1               57                      44.53125
3728766921894762de9dd1f477064fc9        44              58                      45.3125
0e63d33238cf5aa8fb0e6273f7026ef9        81              62                      48.4375
45112f1478a2d18b776d27c7d4e5b5ef        63              68                      53.125
672b697f15c8cd17d71e90c546906074        68              65                      50.78125
d3934de2860c68f694b86f8e6a86c2b2        10              60                      46.875
3efdef210668e8059b8ab12bbfe7be4e        3               64                      50.0
```