CTIS 496::Computer and Network Security:: SPRING 2024-2025:: Third Homework

Instructor: Hamdi Murat Yıldırım

Deadline to submit this homework's related files:

On May 27, 2025, Tue 23:59

NOTICES

1. **Two of you form a group and as a group you will be able submit your homework.**

2. **Copying someone else's solution to this homework, or letting someone else copy your solution is strictly forbidden.**

3. **Write the answers of Question 1), 2), and 3) on papers. Handwritten answers should be submitted to the instructor. Scan these answers. Provide a set of screenshots for all steps in Question 4. Cover page of this homework, these scanned answers, screenshots of Question 4, and references (pdf file) etc should be in the single pdf file. This pdf file and the source code of Question 5) compressed into a zip file (yourname-surname1_yourname-surname2.zip) which will be submitted via course moodle page:**

   https://moodle.bilkent.edu.tr/2024-2025-spring/mod/assign/view.php?id=42349

4. **All references being used should be clearly and correctly indicated in the reference part. Use your own words.**

5. **This homework is out of 110 points. Bonus: 10 points.**

Question 1) Choose one of ciphertext files (each associated plaintext file is encrypted by the Affine Cipher available from

https://moodle.bilkent.edu.tr/2024-2025-spring/mod/resource/view.php?id=42351

and post the filename of the ciphertext file that you have chosen to a forum available from https://moodle.bilkent.edu.tr/2024-2025-spring/mod/forum/view.php?id=42354

To find a teammate for the THIRD Homework, you can send a message to this forum: https://moodle.bilkent.edu.tr/2024-2025-spring/mod/forum/view.php?id=42355

a) (25 points) Use the hand calculation to apply a suitable cryptanalysis techniques to find the secret key K=(a,b). *Mention about this technique which shouldn't be fully automated. That is, you are required to show all mathematical calculations to solve two equations to solve a and b.* ***Write down all steps and software that you use if you want to get a full grade for this question***.

b) (5 points) Write down first two sentences of the plaintext that you recover.

Question 2) Assume that the alphabet of the **Substitution Cipher** for the plaintext and ciphertext consists of only letters A, B, C, D, E, H, I, J, L, N, O, R, S, T, U and Y.

a) **(5 points)** Choose and write down a secret key permutation on these letters.
b) **(5 points)** How many such keys are there? Explain your reasoning.
c) **(5 points)** Choose a meaningful plaintext, and encrypt with the **Substitution Cipher** using the key that you pick in part a) to write down the associated ciphertext.

Question 3) (15 points) Assume that **Permutation Cipher** is used to encrypt the plaintext (a word which consists of 11 letters in English) to get the following ciphertext. According to your student ID’s last digit, you examine the plaintext/ciphertext pair given. Find all candidate keys by applying Known Plaintext Attack (KPA). **You are required to explain every steps that you follow to find candidate keys. Write down the number of candidate keys and list 6 (six) of them. Each group member will answer this question seperately.**

List of plaintext and ciphertext pairs given (for student ID 200031428, 8th ciphertext will be examined).

0.	redargutory	rogutdaryre
1.	teletypists	ytsttesiepl
2.	tractellate	aclelrtteat
3.	impenitible	ipiilembent
4.	totalizator	ottizlatoar
5.	tetraborate	tebrrateota
6.	titillation	lotitlintia
7.	tottergrass	erorstasttg
8.	sistomensin	etiomsnniss
9.	recordatory	rdtrrcaeoyo

Question 4) Download its picture from https://upload.wikimedia.org/wikipedia/commons/6/65/Stork.svg

i. Use GIMP to convert **Stork.svg** into ***Stork.ppm***

ii. Encrypt ***Stork.ppm*** with AES block cipher with key size 128 in ECB mode. Run the following command in the following order.

- ***head -n 4 Stork.ppm > header.txt***
- ***tail -n +5 Stork.ppm > body.bin***
- ***openssl enc -aes-128-ecb -nosalt -pass pass:"CTISBILKENT" -in body.bin -out body.ecb.bin***
- ***cat header.txt body.ecb.bin > Stork-ECB.ppm***
- ***gimp Stork-ECB.ppm***

iii. Encrypt the file ***Stork.ppm*** with AES block cipher with key size 128 in CBC mode. Run the following command in the following order.

- ***openssl enc -aes-128-cbc -nosalt -pass pass:"CTISBILKENT" -in body.bin -out body.cbc.bin***
- ***cat header.txt body.cbc.bin > Stork-CBC.ppm***
- ***gimp Stork-CBC.ppm***

(10 points) Write down your observations for all these steps, and mention about lessons you learned.

(10 points) Provide a set of screenshots for all these steps

Note: It is recommend to use Linux distribution to perform tasks given above.
Windows users can install Virtual Machine with Linux OS on Virtualbox.
Alternatively, on Windows to use commands like head, tail and cat you can download cygwin from https://www.cygwin.com/install.html and install it. You can

install Gimp on Windows or MacOS.

Question 5) **(30 points)** **(**Consider one of the standard available from https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

As a group use *five rules for this standard* to write your code (successfully compiled/executed) to perform a task you determine. ***You need to submit your code and write and explain how to apply these rules in this code as a comment.***
NOTE THAT Each of PREXX from C Security Coding Standard (similarly IDSXX from Java Security Coding Standard) is considered as a single rule.