Universidad de los Andes Colombia | Departamento de Ingeniería de Sistemas y Computación

Maestría en Seguridad de la Información
MSIN-4212 Deciphering Bitcoin
Periodo: 2022 - 18

Cryptography Assignments

You need to complete three cryptography assignments: a take-home exam, a theoretical exercise, and a programming exercise.

You will be working in **groups of two** for the three assignments. Partners should have been assigned to you during the Cryptography review session on June 10, 2022.

You have until **Thursday June 23, 5:00 p.m.** to turn in the three assignments via bloqueneon (assignment 1, assignment 2, assignment 3). Please turn all your assignments in as a group, not separately. Ensure that all answers are typed, not hand-written, and checked for grammar, spelling, and readability. *Also, remember to include the names of the members of the group at the first line -of all the files- you submit*.

The three assignments together are 20% of your final grade. The weighting of the assignments is as follows: take-home exam (12%), theoretical exercise (4%), programming exercise (4%).

1. Take-home exam

Below you will see eight questions, pertaining to the book on "An Introduction to Cryptography" (https://github.com/JWBurgers/An_Introduction_to_Cryptography). The number of percentage points, out of a total of 12%, are listed at the end of the question.

Please answer each of them clearly and in complete sentences. A good answer typically requires three to eight sentences. Make sure you edit your answers for proper English.

Question 1: What is the difference between an encryption scheme and an encryption algorithm? And what is the difference between encryption schemes in symmetric and asymmetric cryptography with regards to the cryptographic keys used? (1 point)

Question 2: What are the most common ways in which symmetric encryption schemes are used? (1 point)

Question 3: Please consider this statement: "Cryptography is concerned with secrecy." Is it True or False? Explain your answer. (2 points)

Question 4: What is a stream cipher? What specifically is a primitive stream cipher? Is RC4 an example of a primitive stream cipher? (1 point)

Question 5: What are the key distribution and key management problems? How are these addressed by asymmetric cryptography? (2 points)

Question 6: What two types of computationally hard problems is most of asymmetric cryptography based on? Specifically, what is the computationally hard problem on which Bitcoin's digital signature schemes are based? (1 point)

Question 7: What are the main two properties required of hash functions in cryptographic applications? Can you give an example for each property of how it is used in practice? (1 point)

Question 8: Suppose that you and your team have created new Bitcoin wallet for desktop computers. It looks really fantastic. However, your team does not have a recognized TLS certificate from a certificate authority. How could your team release this wallet using digital signatures, so that you can improve user security in downloading and installing it? Please broadly describe the steps you would take. (3 points)

2. Theoretical exercise

Please answer the following questions.

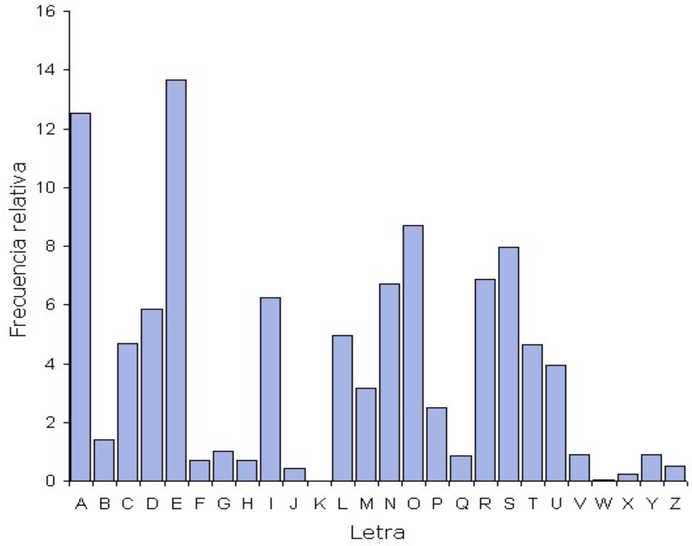
Question 1 (2 points)
The message below was encrypted using an old encryption algorithm. Use frequency analysis to recover the original message (it is in Spanish). We attached the relative frequency of letters in Spanish. Please remember that old encryption algorithms are susceptible to frequency analysis. Modern encryption algorithms are not.
In your answer include: the original message, the substitution map, and describe the procedure you followed to get to that map.

Encrypted text:

```
hjlnjzdrnuqrmjupxodnacnzdnjcjungcanvxuunpx
mnejurnwcnzdnbnjmernacnzdnujvdnacnwxcardwox
mnbdermjlxwbdvdnacncdexjcxmxnuvdwmxnwyxlx
odnnunbyjwcjsxhnulxlxmnuvdwmxnwcjulxhdwcdaj
zdnjlanmrcxbdjenwcdajvxaraldnamxhereauxlx
```

The original text only included lowercase letters and spaces were removed before encryption.

Letter Frequency for Spanish [Taken from Wikipedia[1]]:



Question 2 (1 point)

Suppose a user wants to store a file on a hard disk with the goal of keeping information confidential across time. Describe a scheme (step by step) to store the file, guaranteeing that only the owner of the file can read the information and validate that it has not been tampered with.

Question 3 (1 point)

Suppose Alice sends to Beto the following message:

C(K_B+, C (K_A-, K)) | C(K, M) | C(K_A-, H(M))

Where:

Alice has her public and private keys: K_A+, K_A-

Beto has his public and private keys: K_B+, K_B-

K is a symmetric key

| means concatenated

Describe the procedure (step by step) that Beto must follow to recover information, identify what security guarantees we have (confidentiality, integrity, authentication, non-repudiation) and justify your answer.

3. **Programming exercise** (4 points)

We know that cryptographic hash functions have the property of hiding. However, if we know possible inputs, we may try attacks knows as dictionary attacks.

[1] https://es.wikipedia.org/wiki/Frecuencia_de_aparici%C3%B3n_de_letras

To better understand these ideas, your group must write a program (you may write it in Python or Java) that

1. Computes the hash value of a given input.
2. Given a hash value seeks to identify the original input.

To reduce the time for step 2, we will restrict the allowed inputs to words that only have lowercase letters (no ñ) ~~and numbers~~ (no numbers) and have a maximum length of 7 characters. Run your program for 10 inputs of each possible length, measure the time it takes to find the input from the hash value, and make a figure that shows the times.

Submit your answer in a .zip file with:

- your program (source code)
- a document with:
    - data table (word length, time, recovered word)
    - the figure
    - the instructions to run your program. If your code requires libraries the instructions must inform what libraries and where to get them