MIT World Peace University

Information and Cybersecurity
Second Year B. Tech, Semester 1

Theory Assignment 1

CCA Component

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

April 22, 2023

Contents

1 Question 1

Explain Two general Approaches to attack a Cipher. Also explain briefly the types of cryptanalytic attacks.

Two general approaches to attack a cipher

1. Cryptanalysis
2. Brute Force Attack

1.1 Cryptanalysis

Cryptanalysis is the study of ciphers with the goal of breaking them and recovering the original message without knowledge of the secret key. The ultimate goal of cryptanalysis is to understand how a cipher works and identify any weaknesses that can be exploited to recover the plaintext. Cryptanalysis is a vital component of the study of cryptography, and it has been used throughout history to break codes and ciphers used by various parties in military, political, and diplomatic communications.

1.1.1 How is Cipher Text studied?

The process of cryptanalysis involves various methods and techniques, including statistical analysis, frequency analysis, pattern recognition, and other mathematical algorithms. Cryptanalysts use these methods to study the ciphertext, which is the encrypted form of the original message, and try to find any patterns, repetitions, or other anomalies that could reveal information about the encryption key or the plaintext.

1.1.2 Frequency Analysis

Frequency analysis is a method of analyzing the frequency of letters or symbols in the ciphertext. In most languages, certain letters or symbols appear more frequently than others. For example, in English, the letter "e" appears more frequently than any other letter. In a ciphertext that is encrypted using a simple substitution cipher, where each letter of the plaintext is replaced by a different letter of the alphabet, the frequency of the substituted letters may reveal patterns that can be used to break the cipher. By counting the frequency of each letter or symbol in the ciphertext, a cryptanalyst can make educated guesses about the corresponding letter or symbol in the plaintext.

1.1.3 Statistical Analysis

Statistical analysis is a more advanced form of frequency analysis that takes into account not only the frequency of individual letters or symbols, but also the frequency of pairs, triples, or longer sequences of letters or symbols. For example, in English, certain letter pairs, such as "th" and "he", appear much more frequently than others. By analyzing the frequency of these letter pairs in the ciphertext, a cryptanalyst can make more accurate guesses about the corresponding letter pairs in the plaintext.

1.1.4 Other Methods

In addition to letter frequency and statistical analysis, cryptanalysts may also use other techniques such as pattern recognition, modular arithmetic, and information theory to analyze the ciphertext

and break the cipher. These techniques require a deep understanding of mathematics, computer science, and cryptanalysis, and are used by cryptanalysts to break even the most complex ciphers.

1.1.5 Types of Cryptanalytic Attacks

The following table summarizes the various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Type of Attack	**Known to Cryptanalyst**
Ciphertext Only	Encryption algorithm Ciphertext
Known Plaintext	Encryption algorithm Ciphertext One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	Encryption algorithm Ciphertext Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	Encryption algorithm Ciphertext Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	Combination of "Chosen Plaintext" and "Chosen Ciphertext"

In general, we can assume that the opponent does know the algorithm used for encryption. If the key space is very large, the brute-force approach of trying all possible keys, which is one possible attack, becomes impractical. Thus, the opponent must anaylyze the ciphertext itself, applying various statistical tests to it. To use this approach, the opponent must have some general idea of the type of plaintext that is concealed.

1.1.6 Ciphertext Only Attack

The ciphertext-only attack is the easiest to defend against because the opponent has the least amount of information to work with.

1.1.7 Known Plaintext Attack

In many cases, the analyst has more information than ciphertext only

- The analyst may be able to capture one or more plaintext messages and their encryptions.
- The analyst may know that certain plaintext patterns will appear in a message.

For example, a file that is encoded in the Postscript format always begins with the same pattern, or there may be a standardized header or banner to an electronic funds transfer message. All these are examples of known plaintext. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed. This is known as the known-plaintext attack.

1.1.8 Probably Word Attack

The probable-word attack is closely related to the known-plaintext attack. If the opponent is working with the encryption of some general prose message, he or she may have little knowledge of what is in the message. However, if the opponent is after some very specific information, then parts of the message may be known.

For example:

- If an entire accounting file is being transmitted, the opponent may know the placement of certain key words in the header of the file.
- The source code for a program developed by a company might include a copyright statement in some standardized position.

1.1.9 Chosen-plaintext attack

If the analyst is able to get the source system to insert into the system a message chosen by the analyst, then a chosen-plaintext attack is possible. An example of this strategy is differential cryptanalysis, explored in Chapter 3. In general, if the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

1.1.10 Chosen Ciphertext Attack

The other two types of attack: chosen ciphertext and chosen text, are less commonly employed as cryptanalytic techniques but are nevertheless possible avenues of attack.

Generally, an encryption algorithm is designed to withstand a known-plaintext attack; only weak algorithms fail to withstand a ciphertext-only attack.

1.2 Brute Force Attack

> A brute force attack is a method of attacking a cipher by trying all possible keys until the correct one is found. This method is often used when other attacks fail, and can be effective for breaking simple ciphers or weak encryption algorithms. However, brute force attacks can be time-consuming and computationally expensive, especially for ciphers with long keys.

The basic idea behind a brute force attack is to systematically try all possible keys until the correct one is found. For example, if a cipher uses a 3-digit key consisting of numbers from 0 to 9, there are 1000 possible keys (10 Power 3). A brute force attack would involve trying each of these keys in turn until the correct one is found.

In practice, brute force attacks are often more sophisticated than simply trying all possible keys in order. Attackers may use various techniques to speed up the process, such as using parallel processing or specialized hardware to perform the computations faster. They may also use heuristics or other methods to prioritize the search and try keys that are more likely to be correct.

1.2.1 Example

Let us say pin number consists of 4 digits. They could be numbers or alphabets. If an attacker gains access to your system, he may write the following code for example to generate all possible values, and then find their hashses to match with the hash of your password, encrypted with your algorithm. In this case Ceaser Cipher.

Let us say your password is "abcd". The cipher of this password is "efgh".

A program to crack this scenario would be:

```
ciphertext = "efgh"
alphabet = "abcdefghijklmnopqrstuvwxyz"

# Iterate over all possible keys
for key in range(len(alphabet)):
    # Create a new plaintext by shifting each letter by the key
    plaintext = ""
    for letter in ciphertext:
        if letter in alphabet:
            index = (alphabet.index(letter) - key) % len(alphabet)
            plaintext += alphabet[index]
        else:
            plaintext += letter
    # Print the key and plaintext if it matches the target plaintext
    if plaintext == "abcd":
        print("Key found: ", key)
        print("Plaintext: ", plaintext)
```

2 Question 2

Solve the following problem with chinese remainder theorem.
Use Chinese Remainder Theorem to solve

$$x = 3 (\mathrm{mod}\, 5)$$
$$x = 4 (\mathrm{mod}\, 6)$$
$$x = 5 (\mathrm{mod}\, 7)$$

Solution:

Given the following equations

$$x \equiv 3 (\mathrm{mod}\, 5) \rightarrow (1)$$
$$x \equiv 4 (\mathrm{mod}\, 6) \rightarrow (2)$$
$$x \equiv 5 (\mathrm{mod}\, 7) \rightarrow (3)$$
$$a_1 = 3, a_2 = 4, a_3 = 5$$
$$n_1 = 5, n_2 = 6, n_3 = 7$$

Check if each n_i is pairwise coprime

$$GCD(5,6) = 1$$
$$GCD(5,7) = 1$$

$$GCD(6,7) = 1$$

since all gcd is 1 , so each n_i is pairwise coprime There is a unique solution modulo N

$$N = n_1 \cdot n_2 \cdot n_3 = 5 \cdot 6 \cdot 7 = 210$$

Step-1: $z_i = \frac{N}{n_i}$

$$z_1 = \frac{N}{n_1} = \frac{210}{5} = 42$$
$$z_2 = \frac{N}{n_2} = \frac{210}{6} = 35$$
$$z_3 = \frac{N}{n_3} = \frac{210}{7} = 30$$

Step-2: find $y_i \equiv z_i^{-1} (\mod n_i)$ using Extended Euclidean Algorithm

$$y_1 \equiv z_1^{-1} (\mod n_1) \equiv 42^{-1} (\mod 5) \equiv 2^{-1} (\mod 5) \equiv -2 (\mod 5)$$
$$t = -2$$

$$y_2 \equiv z_2^{-1} (\mod n_2) \equiv 35^{-1} (\mod 6) \equiv 5^{-1} (\mod 6) \equiv -1 (\mod 6)$$
$$t = -1$$
$$y_3 \equiv z_3^{-1} (\mod n_3) \equiv 30^{-1} (\mod 7) \equiv 2^{-1} (\mod 7) \equiv -3 (\mod 7)$$
$$zt = -3$$

Step-3: The solution, which is unique modulo 210 , is

$$x \equiv a_1 \cdot y_1 \cdot z_1 + a_2 \cdot y_2 \cdot z_2 + a_3 \cdot y_3 \cdot z_3 (\mod 210)$$
$$\therefore x \equiv 3 \cdot -2 \cdot 42 + 4 \cdot -1 \cdot 35 + 5 \cdot -3 \cdot 30 (\mod 210)$$
$$\therefore x \equiv -252 - 140 - 450 (\mod 210)$$
$$\therefore x \equiv -842 (\mod 210)$$
$$\therefore x \equiv 208 (\mod 210)$$

So Value of x is 208