Cryptanalysis

Reading

40m

Status Incomplete

Introduction

This readings introduces you to the concept of Cryptanalysis, including explaning what is cipher and how to break ciphers.

Reading

Purpose of the Cryptanalysis

Cryptanalysis has contributed significantly to the development of humankind for centuries. It is the science of breaking encrypted messages to recover their meaning. Not only was it widely used in wars, it was also widely used in solving humanity's mysteries. For instance, cryptanalysis is now used to translate historical documents discovered in what was called a secret language. Over time, these secret languages lost meaning and were considered useless due to a lack of understanding and knowledge of their structure. Cryptanalysis has been responsible for resurrecting these secret languages by using cryptography to translate their meaning.

Many successful cases of cryptanalysis can be cited in history. For example, in 1587, Mary, Queen of Scots, was tried and charged with treason and involvement in three assassination attempts on Queen Elizabeth I of England, which were discovered due to the interception of her coded correspondence, deciphered by Thomas Phelippes.

Another example of successful cryptanalysis is the Enigma ciphering system. It enabled the Allies in World War II to read substantial amounts of German radio communications that had been enciphered using Enigma machines and yielded military intelligence, which, along with that from other decrypted Axis radio and teleprinter transmissions, was given the codename `Ultra.`

Governments recognize the great strength of cryptanalysis and its beneficial power for military intelligence and diplomatic force. For this reason, they created entities that broke encryption codes, such as the **Government Communications Headquarters (GCHQ)** and the **National Security Agency (NSA)**, both from the USA.

Because cryptanalysis can strengthen encryption algorithms and improve communication between networks, like banking transactions, credit card payments, and personal information on the Internet, it has been widely adopted in the field of Cyber Security.

Cipher and Code

In a code, common phrases are replaced by four or five letters or numbers, called **code groups**, taken from a codebook. The word to be replaced can have several codes, leaving it up to the user to choose the code to be used. Codes are particular types of ciphers, but not all ciphers are codes.

Ciphers are encryption methods that don't use the codebook. The difference between these two concepts becomes subtle. The Julius Caesar cipher studied earlier can be seen as a code that uses a single-page codebook. However, it is unreasonable to call it a code since we need to convert character by character, and we have seen that a code delimits an entire word.

Breaking Ciphers

Breaking a cipher is not necessarily the same as finding a way to discover secrets recovered by transforming a cipher into plain text. For academics, **cipher cracking** means finding a weakness in a cipher that can be exploited with less complexity than brute force. For example, if brute force requires us to test 2,256 and we find some weakness in the cipher that allows us to break it with “only” 2,250 tests, we can already say that the cipher has been broken. A cipher break is just a statement that the cipher is not as secure as the developer assured it to be.

Most successful cracks were first applied to a simpler version of the ciphers and in some cases, years later extended to other versions of the same cipher.

Steps to Break a Cipher

We must adopt three crucial steps to break a cipher: identification, breaking, and configuration.

1. **Identification:** the first step involves finding out which cipher system was used. It is important to note that the method used may be unknown to the cryptanalyst. The preamble can help the cryptanalyst discover which technique was used to encrypt the message.

   Then, the cryptanalyst must analyze the message. If it is too small, they will probably have to wait for more messages. Otherwise, they should have enough information to start breaking the message.

2. **Breaking:** the second step is breaking the message to determine fixed parts. It must be performed after the analyst is aware of the system used to encrypt the message. With this information, they will be able to test codebooks, transpositions, and substitutions that can break the message or determine the fixed parts of the cipher.

3. **Configuration:** the third step is configuring the variable parts which will then allow for the start of the breaking tests. It is worth mentioning that the second step, the break, is the most complex, and it may take months to complete this stage of the process.

Ciphertext

Ciphertext is the unreadable format or encrypted text that we use. When you take some plain text and encrypt it using an encryption algorithm, we are encrypting it, or changing it into a ciphertext. Don’t get ciphertext confused with a cipher. Ciphertext is the actual encrypted text, whereas a cipher is the type of encryption method used to encrypt plain text into ciphertext.

Cryptosystems

A **cryptosystem** takes a combination of a few algorithms, also referred to as a “suite of cryptographic algorithms”. A cipher is used to encrypt, but also decrypt, a message. A cryptosystem adds a third aspect to cryptography. What this means is that cryptosystems are used for three things: **key generation** (symmetric or asymmetric), **encryption**, and **decryption**. These are more advanced than ciphers, due to also being able to generate keys. An example of a contemporary cryptosystem is the RSA, since it is used to generate keys and encrypt and decrypt messages.

External Readings

First Reading: Read the following article to get a deeper understanding of the concepts covered in this course thus far: Cryptanalysis explained. The article explains the following concepts in further detail:

- Cryptography: symmetric and asymmetric key cryptography
- Hash functions
- An illustration of cryptanalysis

- Types of attacks
- Results
- Popular tools used for cryptanalysis

> Reflection Questions: After reading the article and taking notes, reflect on the questions given below.

- What are cryptanalysis techniques?
- How do they work?
- How can you protect against attacks?

Second Reading Read the following two articles published by the FBI to learn about well-known coded messages used to commit major crimes throughout history. These were written by Dorn Vernessa Samuel, who works in the Cryptanalysis and Racketeering Records Unit in the FBI Laboratory.

> While reading, take note of how cryptanalysts discovered the meaning in the coded messages of the criminals that helped to solve the crimes.

- Code Breakers: A 400-Year History of Cryptanalysis
- Code Breaking in Law Enforcement: A 400-Year History

Conclusion

With the advancement of the Internet and the high complexity of Internet transactions, new operations began to be carried out through this worldwide network: financial transactions, purchases and sales using credit cards, and transfer of confidential information. Therefore, it is necessary to develop some form of authentication that increases the security of these operations. Cryptography successfully addresses many of the problems associated with these types of operations. On the other hand, cryptography is always changing and evolving due to advancements in hardware and software applications.

With this, we can see that cryptanalysis and cryptography are developing together because a more modern way of masking information is needed when someone breaks the code. When inventing a new encryption method, faults and breaks must be found to ensure information security. Therefore, cryptanalysis is essential and should always follow cryptography, as there will always be people taking advantage of their knowledge of these techniques.

✓ Mark Completed

Previous
Encryption Tools

Next
The Use of the Historical vs. Modern Encryption

W06D5

Fri Aug 2

Outline & Notes (1)

Lectures (1)

Work (10)

7 hrs

- Cryptanalysis
- The Use of the Historical vs. Modern Encryption
- Cryptanalysis Quiz
- Cryptography Features and Objectives
- Typical Levels of Cryptography
- The Use of Cryptography
- Code a Python Playfair Cipher
- Cryptographic Encryption
- Cryptographic Methods with GPG

W06D5 Schedule »