**//UPDATE: We do not have to do every single subtopic in detail. Only four or five. We can mention the rest of them but we do not have to spend too much time on them. Just on the relevant ones.** *– Chris 23/10/2017*

**//Write whatever you have paraphrased or any quotes into the assigned section. Any quotes and references need to go to the Bibliography page. To do this, select the text/quote, click on “References” and then “Insert Citation”.** - *Chris 25/10/2017*

**// On this page, write a short introduction that can go on the main page. Then go to the designated section and type your research there.***– Chris 27/10/2017*

<https://www.columnit.com/how-to-prevent-cyber-security-mistakes.html> ****

[**SONIA: (Computer Security)**](#_CYBER_SECURITY)

[**CHRIS: (Cryptanalysis)**](#_RELIABILITY_&_MANAGEMENT)

This field is the rival of Cryptography. It focuses on analysing and ultimately breaking a type of code known as ciphers to have access to secret information. This requires a lot of logic and super-difficult mathematical formulae.

[**YIFAN: (Cryptography)**](#_CRYPTOLOGY)

I found this video, it is pretty cool: <https://www.youtube.com/watch?v=-yFZGF8FHSg> – Chris.

[**PAUL: (Malware)**](#_HUMANS_&_CYBERCRIME)

# **COMPUTER SECURITY**

**Sonia**

# **CRYPTANALYSIS**

**Chris**

Introduction:



Cryptanalysis

<http://www.bbc.co.uk/news/business-39341663> (Getty Images)

This field is the rival of Cryptography. It focuses on analysing and ultimately breaking a type of code known as ciphers to have access to secret information. This requires a lot of logic and super-difficult mathematical formulae. This is why this topic is one of the most challenging ones, but also on of the most historic ones in Information Security.

History:

The field of Cryptanalysis has always advanced at the same time as Cryptography. They always go together, despite being absolute opponents, this is why they are viewed as two sides of the same coin. Every time a new cipher is developed, a new cryptanalytic technique evolves to crack it. Sometimes, this takes a long time, and we can see this throughout history.

So that you get an idea of how back this goes, let’s talk about Mary, Queen of Scots in 1587. She was tried and executed for treason due to her involvement in three plots to murder Elizabeth I of England. Mary would write letters which discussed plans to assassinate Elizabeth, but these were all coded so that nobody except her and her team would understand. These plans were revealed after her coded correspondence with other conspirators was deciphered.

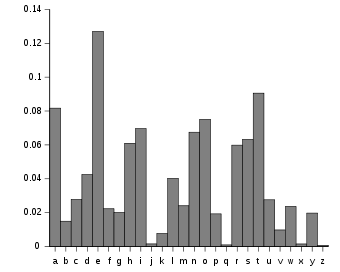
Now that you get an idea of how old the art of cryptanalysis is. Let’s look at a more recent event: World War II. In this war, the Allies benefitted tremendously from their cryptanalysis success. The most famous examples include the German Enigma Machine and the Lorenz cipher. It is estimated that thanks to this success, the war was shortened by up to two years, saving millions of lives.

<https://www.youtube.com/watch?v=ZVlMJ1tmT_c>

Ever since then, governments throughout the globe have started recognising how important cryptanalysis is, hence they invest in this field. For instance, GCHQ (the British intelligence team in charge of the country digital protection) and the NSA (same as GCHQ but in the US), which are still pretty active today, play a very important role make sure that citizens are safe, and that information is not accessed without permission.

Examples:

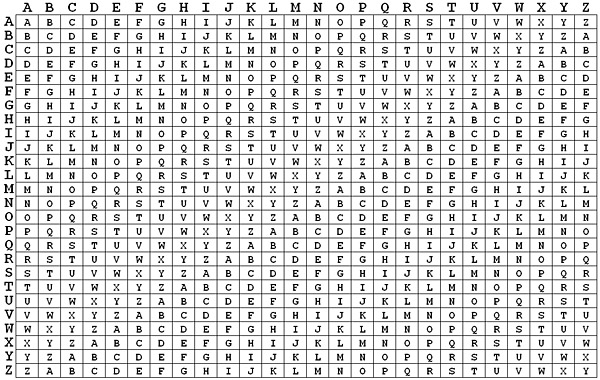
* Frequency Analysis: This is one of the most classical tools used to break simple ciphers. In most languages, some letters and combination of letters appear more often than others. In English, the letter “E” is the most common letter. Similarly, the digraph “TH” is the most likely pair of letters. These little facts of course vary with language. And in some cases, they are not applicable.



Frequency Analysis of English

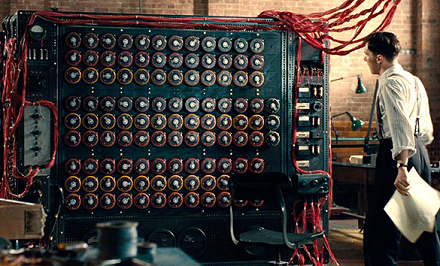
<https://en.wikipedia.org/wiki/Frequency_analysis>

* Polyalphabetic Cypher: For centuries, this cypher was considered to be completely secure: “le chiffre indéchiffrable - the indecipherable cipher” they called it. The French diplomat that came up with it, Blaise de Vigenère, thought it would be impossible to break. But he was wrong. Charles Babbage and Friedrich Kasiski succeded in breaking it, however it took them centuries!



The Vigenère Square (used to produce this polyalphabetic cypher)

<http://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html>

* The Bombe: This one was the machine that Alan Turing, the father of Computer Science, and his team developed in order to break the Enigma, mentioned before. It was an electro-mechanical device used to decipher secret messages coming from Germany during World War II.

The Bombe at The Imitation Game (TV Adaptation of Alan Turing’s Story)

<https://logosconcarne.com/2016/02/11/the-imitation-game/>

Researchers:

# **CRYPTOGRAPHY**

**Yifan**

# **MALWARE**

**Paul**

# Bibliography

**There are no sources in the current document.**