IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT

Impact Factor: 6.252

Volume 2, Issue 2, March 2022

A Study on Cryptography

Rishab V[1], Sachin[2], Sagar S Yadrami[3], Shamjetshabam Noren Singh[4], Partha Sarathi Pati[5]

Students, Department of Computer Science and Engineering[1,2,3,4]

Sr. Assistant Professor, Department of Computer Science and Engineering[5]

Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security will ensure that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. High-assurance cryptography leverages methods from program verification and cryptography engineering to deliver efficient cryptographic software with machine-checked proofs of memory safety, functional correctness, provable security, and absence of timing leaks. Traditionally, these guarantees are established under a sequential execution semantics. However, this semantics is not aligned with the behavior of modern processors that make use of speculative execution to improve performance. This mismatch, combined with the high-profile Spectre-style attacks that exploit speculative execution, naturally casts doubts on the robustness of high-assurance cryptography guarantees. I Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender.*

Keywords: Cryptography.

I. Introduction

1.1 History

Cryptography was used only for military and diplomatic communication until the development of public key cryptography. Secrecy is one of most important requirements for any communication and it becomes more important when the content of communication is for military and diplomatic purpose.

Hieroglyphs used by Egyptians are earliest known example of cryptography in 1900 BC. These hieroglyphics were used to write the stories of the life of kings and describe the great acts of his life. Around 500 BC Hebrew scholars used mono alphabetic substitution cipher such as “Atbash cipher”. Around 400 BC the Spartans also developed a “Scytale cipher” that used ribbons of parchment for writing any secret message after wrapping it around a cylindrical rod named as Scytale. In second century, BC Greek historian Polybius invented “Polybius Square” a type of substitution ciphers. Around 1st century BC the Roman emperor Julius Ceaser used the substitution cipher named after him as “Ceaser Cipher”. The Caesar Cipher is a Monoalphabetic type Cipher.

Historically, cryptography has been used by armies at war to make secret communications seemingly unreadable, to prevent their enemies from intercepting vital information such as plans of attack. This usually consisted of simply encrypting the messages using a pre-determined key, such as the use of the Caesar Cipher. Another early example of cryptography was the Pigpen Cipher, which represented letters graphically using a key that was (in theory) known only to those sending the messages and their intended recipients. This key consisted only of grids which were fragmented to represent each letter. It is also known as the Freemason's Cipher, due to the movement using it so frequently to encrypt their communications.

Cryptography is hard to get right: Implementations must achieve the Big Four guarantees: Be (i) memory safe to prevent leaking secrets held in memory, (ii) functionally correct with respect to a standard specification, (iii) provably secure to rule out important classes of attacks, and (iv) protected against timing side-channel attacks that can be carried out remotely without physical access to the device under attack.

To achieve these goals, cryptographic libraries increasingly use high-assurance cryptography techniques to deliver practical implementations with formal, machine-checkable guarantees. Unfortunately, the guarantees provided by the Big Four are undermined by micro architectural side-channel attacks, such as Spectre, which exploit speculative execution in modern CPUs.

DOI: 10.48175/IJARSCT-2852

As will be explored later in more detail, these forms of cryptography were not particularly secure, as they were easy to guess based on knowledge of the languages being used and the potential contents of messages.[1]

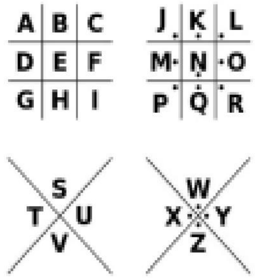

Figure 1: An example of the Pigpen Cipher.

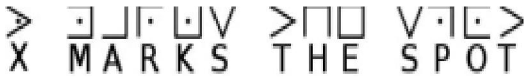

Figure 2: A message encoded using this Pigpen Cipher.

Later forms of cryptography made use of rotor cipher machines, such as the Engima Code, which made their decryption a lot more difficult. Modern cryptography makes use of discoveries in number theory and computer science, thus making modern cryptosystems more secure than any cryptosystems used prior to these discoveries. This will be studied more in depth later in this essay.

II. Caesar Cipher

It is known that Julius Caesar (13/06/100 BC - 15/03/44 BC) [2] , the famous Roman politician and general, created a cryptosystem to encode his military messages; this way his opponents would, in theory, be incapable of deciphering his plans should they intercept any messages. His cryptosystem was based on modular arithmetic, more precisely, it encrypted the alphabet by +3 mod 26, after assigning each letter of the alphabet to a number from 0 to 25. In other words, the plaintext letter A was assigned to the letter D in the ciphertext, B to E, and so on. This is an example of a polyalphabetic substitution cipher. [3]

2.1 How was this Decrypted?

The decryption of this, providing the eavesdropper knew the key, would simply work in the opposite way, by subtracting 3 instead of adding; this is based on the logic of subtracting 3 from 0 giving 23, as per arithmetic mod 26. This may, at first glance, seem to give very little help in the way of decoding a message that uses this cipher.[4] This will be explained later in more depth, but is directly linked to the probability of each letter appearing in sentences in the language of the plaintext; for example, e is widely cited as the most frequently used letter in the English language [6].

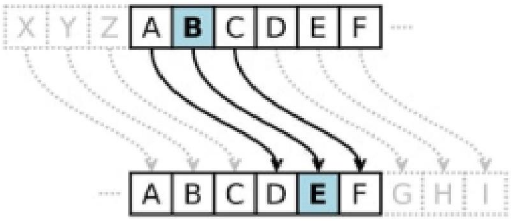

Figure 3: The Caesar Cipher.[5]

Once the eavesdropper has determined the frequency of each of the ciphertext letters, they can make a series of educated guesses about certain associations of plaintext to ciphertext letters this will then reduce the possibilities of various keys drastically, and help them to decode at least the vast majority of a message.

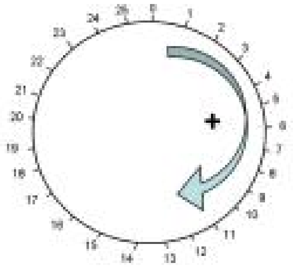

Figure 4: A modular addition circle modulo 26.

2.2 Enigma Code

Invented during World War I and implemented by the Germans during World War II, the Enigma machine is a highly complex example of a polyal phabetic substitution cipher. The machines were a series of rotors which, when operated by a user, would encrypt messages using a constantly changing key. The different parts of the machine were programmed separately according to a set of specifications that differed for every machine; to de crypt a message the eavesdropper or recipient would have to be in possession of a machine set to the same specifications.[7]

The options for adjusting the machines were: [8]

- Wheel order - the choice and order of rotors when building the machine.
- Ring settings - where each alphabet ring was positioned.
- Wiring - plugboards were a part of the machines that connected pairs of letters together, so the wiring of these was changed on every ma chine.
- Starting position of the rotors - these were different for every message, and chosen by the operator of the machine.

The machines were then operated with easily-destroyable books of keys, which were again specific to each configuration of settings. These keys were changed regularly, to make the number of possible encryptions even higher.

Without knowing the set-up of the machine used to encrypt the plain text, it was extremely difficult to decrypt any message. This system of machines was the closest that any cryptosystem had ever come to perfect secrecy.[9]

A. How was this Decrypted?

Due to the complex nature of the encryption system, this cryptosystem was incredibly difficult to decrypt. Though the system in itself actually contained a few cryptographic weaknesses, it was actually a range of other factors that contributed to the Allies breaking the code in World War II. These consisted of German procedural and organizational errors, and the capture of Enigma information and hardware by the Allies. [10]

Much of the work on the Enigma code that enabled its decryption was completed by Alan Turing, a Cambridge University mathematician and logician. His efforts are recorded in many books such as ’Alan Turing: The Enigma’ by Andrew Hodges, as well as the 2014 American historical drama film ’The Imitation Game’, starring Benedict Cumberbatch. [11]

2.3 Why not these Ciphers?

As previously described these ciphers, and similar developments, are un fortunately insecure. With modern applications for cryptography such as banking, online money transfers, emails, social media, and many more, the demand for perfectly secure encryption is ever increasing. Digital data trans fers are increasingly vital to today’s society, therefore no chances can be taken on our data being secure from prying eyes.

III. Computational Number Theory

Computational number theory is the combination of elements from number theory, and computation theory. This works in two directions; computing methods from computation theory are applied to solve number-theoretic problems, and vice-versa. [12]

This essay focuses more on using computing techniques to solve number theoretic problems, in order to create applications in modern public-key cryptography.

This section is primarily comprised of research from ’Computational Number Theory and Modern Cryptography’, Song Y. Yan, including (but not limited to) the theorems and examples presented in the Primality Testing and Integer Factorization subsections.[13]

IV. Modern Cryptography

4.1 Perfect Secrecy

Definition 4.1. Evaluate a cryptosystem with a random key, K such that K ∈ 0, 1, ..., s with the set of possible plaintexts P = 0, 1, ..., t, and the encryption function f(clear, key).
For every possible cleartext i, let Xi denote the corresponding ciphertext. That is, Xi = f(i, K).
Perfect secrecy requires the probability distributions of the random variables X0, X1, X2, ..., Xt to be the same.[14]

A. Probability Theory

An issue that arises when determining the security of a cryptosystem is whether the eavesdropper will be able to guess the message based on a series of logical connections. For example, if the eavesdropper knew what kind of message was being encrypted (i.e. war plans, a phone number, a password of a certain length), they could try a series of guesses at the key used (e.g. modulo addition) and apply these to the ciphertext. [15]

They would be left with a selection of potential plaintexts, one of which may be the actual plaintext. Due to the probability of certain letters occur ring in different languages not being a uniform distribution, these guesses are made a lot easier with only a small amount of knowledge about the plaintext. [16]

The aim with perfect secrecy is to make the chance of any letter, number or symbol appearing in the message completely equal.[17] This would ensure that, should an eavesdropper try to use every possible key and combination to guess the plaintext from the ciphertext, their selection of possible plain texts following this process would be unintelligible, leaving them no closer to decrypting the message than before. [18] Thus the aim is to create a uniform distribution with the probability of any symbol from the sample space showing up.

References

[1] FIPS 197, Advanced Encryption Standard, National Institute of Standards and Technology, US Department of Commerce, WashingtonD. C.,2001

[2] Research on Various Cryptography Techniques Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi

[3] Review and Analysis of Cryptography Techniques Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay

[4] Chandra M. Kota et al., “Implementation of the RSA algorithm and its cryptanalysis,” In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002

[5] R. GENNARO, "IEEE Security & Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64 - 67, 2006

[6] Cryptographic Hash Functions: A Review Rajeev Sobti 1, G.Geetha2 1 School of Computer Science, Lovely Professional University Phagwara, Punjab 144806, India 2 School of Computer Applications, Lovely Professional University Phagwara, Punjab 144806, India.

DOI: 10.48175/IJARSCT-2852