



UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

---

# Cryptography

What it is and why it matters

---

*Author:*

Lars Fredrik KARLSTRÖM

February 17, 2012

## Abstract

The art of keeping secrets and messages safe stem back several thousands of years. By its very nature, cryptography is a topic shrouded in mystery, with a fascinating history and numerous legends to be told. But it is also a science in hefty debate, its essential applications both feared and treasured. If you would ask just how important cryptography has been to us, you need only acknowledge the fact that it is due to the secret battle of code breakers during World War II that we may enjoy computers today.

In this essay, we shall explore the dawn of cryptography, its impact throughout the centuries, and shed light on some encoded mysteries that continue to baffle scientists to date. We will also learn the fundamental aspects of encryption and decryption, study various ciphers, and analyze the profound impact that modern cryptographic algorithms have on our lives.

Albeit a few sections might be geared towards readers with a background in computation, the major part of this essay should be accessible - and hopefully captivating - to all audiences alike.

The most current version of this document can be retrieved from the URL <http://cbsmth.se/misc/essay-cryptography/>.

**Keywords:** Cryptology; Cryptography; Cryptanalysis; Secret writing; Codes; Ciphers

# Contents

<b>1</b>	<b>The history of cryptography</b>	<b>2</b>
1.1	The early days . . . . .	3
1.2	World War I . . . . .	6
1.3	The origin of computers . . . . .	7
<b>2</b>	<b>Legendary ciphers</b>	<b>8</b>
2.1	Kryptos, the encrypted sculpture . . . . .	8
2.2	The Voynich manuscript . . . . .	9
<b>3</b>	<b>Theoretical basis</b>	<b>11</b>
3.1	Transposition ciphers . . . . .	11
3.1.1	The rail fence cipher . . . . .	11
3.2	Substitution ciphers . . . . .	12
3.2.1	The Caesar cipher . . . . .	12
3.2.2	Nomenclator codes . . . . .	13
3.3	Breaking codes . . . . .	13
<b>4</b>	<b>Modern cryptography</b>	<b>15</b>
4.1	Implementation and impact . . . . .	15
4.2	Controversy . . . . .	16
4.3	Public Key Cryptography . . . . .	18

# Chapter 1

## The history of cryptography

The word *cryptography* stems from the ancient Greek words *kruptos*, meaning “hidden,” or “secret,” and *graphein*, which as a suffix denotes something written. Today, it is practically always associated with computers and highly complex mathematical formulae. But the art of writing messages with concealed content has a profound history dating back as much as four thousand years, when a scribe in ancient Egypt substituted well-known hieroglyphs for more obscure ones in his master’s tomb.

From safeguarding military commands during the eras of Greece and Rome, cryptography became a crucial ingredient to the success of trading empires throughout Europe, before serving as the the weight that turned the scales in the World Wars. Today, it is essential to our society, with electronic currency transactions as well as communiqués depending on cryptographic algorithms for safekeeping.

## 1.1 The early days

Although the cradle of cryptography has been traced back to to this early point in time, the concept vanished, still an infant, without ever leaving Egypt. As a matter of fact, cryptography as well as its sibling *steganography*, the concealment of written messages, has been both invented and abandoned in numerous ancient civilizations.

In eastern cultures such as India, Mesopotamia, and China, concealed messages are known to have been used for a variety of purposes, the most obvious ones being military in nature. These systems spanned from the rudimentary, perhaps substituting words such as “arrows” or “troops” with names of flowers or animals, to more developed cryptosystems. Although these ciphers might have played more or less significant roles in their time, they never seem to have attained any major, long-lasting importance. One of the primary reasons to this is probably that the vast majority of people were illiterate; there simply were no great number of prying eyes to defend against.

As with so many other scientific fields, the ancient Greek civilization later propelled cryptography forward, elaborating various ways to communicate in discession. The Spartan *scytale*, for instance, was the first device ever used to create transposition ciphers, in which the positions of the letters are systematically displaced. Wrapping a piece of parchment around a baton with a specific width and length, the message was written on the parchment along the length of the stick. The paper was then brought to the recipient who held a scytale of corresponding dimensions, which allowed him to read the message.

Attempting to solve the problem of long-distance message transmission, the writer Polybius devised a grid with numbered rows and columns into

which the alphabet was placed. Using these coordinates, a number corresponded to a letter: a fundamental conversion, often used in cryptography. Although it is unknown if the system was ever used as intended by its author, the *Polybius square* has been used as the foundation for many other cryptographic systems.

During the grand conquests of Rome, emperor Julius Caesar made use of a substitution cipher of his own device, known rather straightforwardly as the *Caesar cipher*. The message was quite simply written by transforming each letter of the alphabet in correspondence with a given encryption key, Caesar's choice being "three to the right." Thus the letter A was transformed to D, B into E, and so forth.

With the decline of the Roman empire, Europe plunged into the intellectually stagnant Dark Ages. Cryptography, however, was taken to new, unparalleled levels in Arabia, where numerous improved encryption schemes were constructed, and even more importantly *cryptanalysis* — the study of breaking codes and ciphers without access to the secret key — for the first time was explored. With this counterpart to cryptography, the stage had at long last been set for the perpetual battle between those who write codes and those who try to break them. As the Arab world diminished, the scientific knowledge amassed was assimilated into the western world — mathematics and medicine as well as cryptology.

It is in the early days of the renaissance that the importance of cryptography begin to escalate dramatically, first in a battle over papacy between Pope Urban VI and Pope Clement VII, then in the swiftly developing political landscape of a Europe transforming from medieval states to international, capitalist nations. With embassies established in every country, diplomatic communication soon became a primary target for espionage endeavours —

and just as today, the ones who could break the codes were the ones who would reap the benefits. Back then, the winner's name was Venice; the small city-state managed to create a vast trading empire leveraging its well-developed intelligence network, and they were so capable at codebreaking that they could rent their services out to allied states, warranting both a hefty price and giving them the advantage of reading the intercepted communications first.

In the same period of time, Queen Elizabeth's spymaster Sir Francis Walsingham wove what might have been the greatest network of spies to date, intercepting and deciphering communications all over the continent. Among many other things, this network thwarted an assassination and following rebellion instigated by Mary, Queen of Scots — Queen Elizabeth's cousin — and catholic factions still lingering in the recently reformed England.

With these advances, cryptography had become far more widespread than ever before, but in complexity however, it still only equaled its eastern predecessors. The great leap forward that changed that status was the invention of the *polyalphabetic cipher*, which greatly increases the security of a ciphertext by utilizing several different substitution alphabets.

From there, new progress was gradually made throughout the years, intelligence playing pivotal roles in the various conflicts that ensued. With the course of time the board changed, as new technologies such as the telegraph and radio communication became available. Soon enough, Europe was on the brink of what would become the First World War.

## 1.2 World War I

On the very first day of the war, the English cleverly severed Germany's Atlantic communications cable, forcing them to transmit all orders over radio or via cables not in the country's control. This meant that all German orders could be intercepted, and with the aid of the individuals that came to make up the now legendary *Room 40*, much could also be decrypted.

The struggles and achievements of the cryptanalysts in Room 40 is like taken from a movie plot. Starting off as a small group of university teachers fluent in German, at first the task of deciphering the German codes seemed hopeless. But after a stroke of luck in obtaining a code book, the unit soon grew into a large, devoted and extremely efficient intelligence unit that came to have a great impact on the outcome of the war. The decrypts provided by Room 40 helped chasing German submarines, and diplomatic correspondence told tales of the adversaries' more long-term plans.

The most important decrypt performed was that of a diplomatic telegram transferred across the Atlantic. Its plain-text was an invitation to Mexico to join Germany in submarine warfare against the United States, for which Mexico in return would receive territories previously lost. The solution and subsequent delivery of this message, although a terrible ordeal given the need to keep Room 40 an absolute secret, finally succeeded in making the United States join the Allied forces and spelled the beginning of the end of the war. As any true hero, the British intelligence silently covered the truth about their own success, receiving and even instigating harsh criticism from their countrymen for their "inefficiency."

### 1.3 The origin of computers

Located within convenient walking distance from a train station between Oxford and Cambridge, two towns filled to the brim with intellectual talent, lies one of the most historically important buildings from the World War II-era: *Bletchley Park*. It was here that British and United States intelligence cooperated in breaking German communications encrypted with *Enigma*; a mechanical tool used to create extremely strong polyalphabetic ciphertext.

The advances in electronic engineering made in the span between the First and Second World War allowed for cryptographical devices far more advanced than ever before, such as Enigma and the *Lorentz machine*. This in turn called for the invention of machinery to break ciphers as well, which was what now world-famous British mathematician and computer scientist Alan Turing was tasked with at Bletchley Park. Refining a Polish device he created the *Bombe*, a machine that utilized logical contradictions in order to find possible keys to Enigma ciphers. Turing, who is known as the “Father of Computer Science,” has contributed considerably to the field, defining both *Turing-completeness* — a cornerstone of modern computing, and the *Turing test*, which is used to define Artificial Intelligence.

Although a computational device, the Bombe was not programmable and thus not a computer per say. The first programmable computer, *Colossus*, was also created by the codebreakers at Bletchley Park, in order to find keys for the Lorentz cipher which was even more complex than the famous Enigma. As with many war-time inventions, the Colossus was kept secret until the 1970’s, which means that some researchers never were credited for their innovations until after they died. In 2007, a functional imitation of this machine was constructed; it is now on exhibit at the National Museum of Computing — in Bletchley Park.

# Chapter 2

## Legendary ciphers

*The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others.*

— Chadwick

### 2.1 Kryptos, the encrypted sculpture

On a large, wave-shaped copper sculpture located on the grounds of the Central Intelligence Office's headquarters in Langley, Virginia, an engraved cipher teases the employees passing by. Erected in late 1990 by the sculptor Jim Sanborn, so far three parts of the cipher, which is spread around the headquarters, has been solved. The fourth and final part however, which is rumored to unlock yet another riddle, remains unsolved to date.

The solutions to the first three parts were announced nine years after the sculpture was first unveiled, by a California computer scientist named Jim Gillogy. After he publicly announced his findings, however, the CIA claimed that one of their own cryptanalysts had solved the same parts before, using only pen and paper.

The first and second messages were encrypted using *Vigenère*-style polyalphabetic ciphers. The third message used a *transposition cipher*, and the fourth one is yet unknown.

In making the sculpture, which took two years and cost \$250,000 USD, the artist collaborated with an experienced CIA cryptologist, Ed Scheidt, and — although Sanborn later denounced it — allegedly also an anonymous “prominent fiction writer.” When Dan Brown’s *The Da Vinci Code* was released in 2003 the Kryptos sculpture immediately became internationally known, as the book’s cover displayed mysterious coordinates on the back, as well as the phrase “Only WW knows” — both elements from the second Kryptos message. It has been speculated that the famous author indeed was the anonymous helper, but that has neither been proven nor denounced.

The message “Only WW knows” refers to the previous director of the CIA, William Webster, who supposedly received an envelope with the solutions to the ciphers. This well-guarded secret, Sanborn has stated, has been set up so that it will not be lost in case the current holder dies before the full riddle has been solved.

## 2.2 The Voynich manuscript

Written some 600 years ago by an unknown author in a manner nobody has ever been able to read, the Voynich manuscript — known today after the Polish antiquarian Wilfrid Voynich who bought it from Jesuits in Italy in 1912 — has been described as the world’s most mysterious manuscript.

The manuscript has been dated back to the early 15<sup>th</sup> century by carbon dating, but it first appears in historical records as a belonging of Rudolf II, Holy Roman Emperor and King of Bohemia, who bought it from an unknown

individual for 600 gold ducats — a staggering amount, roughly \$80,000 USD in today's currency. A lover of the occult and intriguing, the Emperor no doubt felt that the mysterious document warranted the price.

The manuscript passed between various men during a hundred years until it was stored, accompanied by a cover letter written in 1666, in the library of the Collegio Romano — from which Voynich finally retrieved it. The letter mentioned that one of the manuscript's previous owners believed its author to be none other than Roger Bacon, a philosopher and Franciscan friar who pioneered in many scientific areas and is credited as the first European to describe the formula for gunpowder.

Although modern evidence contradicts this belief — as Roger Bacon died in 1294 — many still believe he might have been the author; understandably, as the manuscript seems to contain close to 250 pages on topics he researched, such as botany, astronomy, biology, and pharmacy, judging from the almost equally numerous illustrations.

The collection has vexed many great minds, including numerous experienced codebreakers from the First and Second World War, and will no doubt continue to do so for a very long time. It is just as difficult to prove the entire compilation a hoax as it is to decrypt it, and the imagination of what secrets might be unveiled if and when it is solved is enough to make the captivated keep on trying.

*But his toil was in vain, for such Sphinxes as these obey no one but their master.*

— Johannes Marcus Marci, 1666

# Chapter 3

## Theoretical basis

In the previous chapters we explored the origin of cryptology, and we scratched the tip of the iceberg of what impact it has had on our past. This could not be done without mentioning a great variety of encryption schemes, a few of which we shall now study further in order to learn how a cipher works.

### 3.1 Transposition ciphers

A transposition cipher creates a *permutation*, a distinctly ordered rearrangement of the plaintext, rather than exchanging words or letters for other characters. The Spartan scytale mentioned in chapter 1 was a tool used to create a transposition cipher.

#### 3.1.1 The rail fence cipher

In the rail fence cipher, the plain-text message is written on a grid in a zig-zag pattern, resembling a fence. When the letters have been placed out on the grid, they are read in rows, which make up the encrypted text. To reassemble the message, the recipient must know how many “rails” the grid

constitutes of. In the following example, the key is having three rails. Our plaintext message is: *THE CAT IS LAZY*.

T				A				L			
	H		C		T		S		A		Y
		E				I				Z	

The encoded message now reads: *TALH CTSA YEIZ*, with extra spacing added.

## 3.2 Substitution ciphers

In a substitution cipher, the characters in the original message are exchanged for others in accordance with a predefined system, which serve as the key to the cipher. This type of cipher range from the most simple, such as the Caesar cipher, to polyalphabetic ciphers which utilize a number of different encryption alphabets, like the Vigenère square.

### 3.2.1 The Caesar cipher

In the Caesar cipher, the alphabet is shifted a given number of positions in a certain direction. In accordance with the emperor's choice, our example shall move the alphabet three positions to the right. Once again, we will encode the message *THE CAT IS LAZY*.

Original	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Shifted	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Using this cipher, the encoded output becomes *WKHF DWLV ODCB*.

### 3.2.2 Nomenclator codes

Nomenclator codes differ from other ciphers in that they allow for whole words or sometimes even sentences to be replaced by a number or code-word. The *Gran Chiffre*, used by the French King Louis XIV, was a highly successful nomenclator code that kept archived messages unbroken for several hundred years. They were also frequently used in the First World War.

In order to counter frequency analysis, a nomenclator code can hold a great number of synonyms; codes that translate into the same plain-text.

## 3.3 Breaking codes

The field of cryptanalysis was discovered in 9<sup>th</sup> century Arabia, by the polymath Al-Kindi, also known as the father of Islamic philosophy. Building upon Greek knowledge, Al-Kindi made tremendous advances in fields as varying as mathematics, medicine, optics and philosophy, as well as cryptography.

Up until the age of mechanized cryptography, the primary tool of code-breaking was *frequency analysis*, a method of reverse-engineering the encoded message into plain-text by counting the most frequently occurring characters and matching them to the language's most common letters. In English and Spanish, for example, the most common letters are E, T, and A. Similarly, the least occurring letters are Z, Q, and X.

If a codebreaker studies an encoded message which he believes to be written in English, and notices that the letters E, T and A appear often, he could be fairly certain that he is tasked with solving a transposition cipher. With that vital piece of information, he can begin repositioning letters, making anagrams, until he finds a pattern that efficiently solves the entire message. Respectively, if other arbitrary numbers or characters seem to be appearing

frequently, the cryptanalyst has most likely found the substitution cipher's corresponding characters for the common letters.

It was first after this formal study became commonplace that encryption schemes begun evolving into more complex systems, but even with polyalphabetic substitution ciphers, autokey ciphers, and later on mechanical encryption devices being invented, the cryptanalysts kept their lead, breaking into most correspondence of importance. The tables only recently turned, as increasingly powerful computers allowed for complex mathematical encryption schemes to render trial-and-error methods obsolete.

# Chapter 4

## Modern cryptography

*The common person needs encryption to function effectively in the information age. So it's time for cryptography to step out of the shadows of spies and military stuff, and step out into the sunshine and be embraced by the rest of us.*

— Zimmermann

### 4.1 Implementation and impact

Today we live in the age of information, in which cryptography has become an essential component of our daily lives. Your bank account is purely electronic, protected by various layers of encryption and verification to ensure the integrity of your assets. You use credit cards and Personal Identification Numbers to perform authorized transactions, in physical stores as well as on the Internet — and the vast majority of the services you use online, such as Facebook, e-mail, and chatting, make ample use of cryptography.

Modern cryptographical algorithms base their security on mathematical formulae that are profoundly hard to compute, meaning that without the proper key, there is close to an infinite number of combinations to try. Ad-

vances have also been made in concepts such as *asymmetric key* cryptography, in which each involved party has two different but mathematically related keys — solving the age-old problem of cipher key distribution, as well as in *hashing*, a form of one-way encryption often used for storing and verifying passwords and other sensitive information.

## 4.2 Controversy

As you might have noted, the obscure world of cryptology has since long been tilted in favor of the codebreaking cryptanalysts, enabling governments to tap into streams of everflowing data. In recent years, however, this has changed. Today, any computer is more than capable to make use of virtually impregnable encryption schemes.

This is obviously a frightening situation for any state fearful of enemy activity; but outlawing cryptographic algorithms for public use greatly imposes on our sanctioned human right to privacy. As Phil Zimmermann, the author of PGP encryption, argues in an interview:

Sometimes in a democracy bad people can be elected, and if democracy is allowed to function normally, these people can be taken out of power by the next election. But if a future government inherits a technology infrastructure that's optimized for surveillance, where they can watch the movements of their political opposition, they can see every bit of travel they could do, every financial transaction, every communication [...] if the incumbency has that political advantage over their opposition, then if a bad government ever comes to power, it may be the last government we ever elect.

In light of recent events, governments are taking increasingly drastic actions to leverage intelligence both as a shield and as a weapon against the much feared terrorist threat, but this deal comes with a high cost; personal privacy becomes a memory of the past. Renowned security expert Bruce Schneier argues that one must always assess the *trade* when it comes to security: does the benefits outweigh the cost? When it comes to this type of surveillance, the simple answer is *no*. The only way to access properly encrypted information today is by somehow obtaining the key, a situation which has led to debate and trials regarding the authorities' right to force a suspect to hand this information over.

In many dictatures, such as China for instance, utilizing cryptography without a government-issued licence is a criminal offense which can land the culprit in jail. The poorly concealed, wanton lust for control displayed by governments worldwide inches modern legislation closer and closer to this type of state; it is imperative not to allow the situation to get out of hand.<sup>1</sup>

*The more corrupt the state, the more numerous the laws.*

— Tacitus

---

<sup>1</sup>Earlier this month, the *Stop Online Piracy Act* caused a great stir internationally, as it would enable both government and private institutions to perform censorship — forcing search engines to exclude websites from search results, and banning advertisement and payment services from dealing with them.

### 4.3 Public Key Cryptography

In 1976, Whitfield Diffie and Martin Hellman published *New Directions in Cryptography*, a paper in which they introduced a revolutionary new concept known as *public key* cryptography. In accordance to this structure, each party has two different albeit mathematically related keys — one private, and one public. The public key can be shared with anybody without worry; the private key cannot be derived from it.

The system is rather straightforward: If Alice wants to send an encrypted message to Bob, she uses his public key to perform the encryption. The message can then only be decoded by Bob, who has access to the corresponding private key.

A prerequisite for this exchange is that Alice indeed has Bob's authentic public key, a problem which has been partially solved by *key signing*. If a person knows for certain that a public key is real, he or she can sign it, which adds a layer of trust to the key. Another solution is the existence of *certificate authorities*, organizations who certify ownership of key pairs.

In addition to encrypting whole messages, the public key system can be used to generate *digital signatures*, which easily can be included in e-mail correspondence. By checking a signature against the author's public key, the recipient can verify that the sender indeed possesses the private key.

The public key infrastructure is a fundamental component of *Pretty Good Privacy*, which together with its free and open source counterpart *GNU Privacy Guard* constitute the primary encryption software used by both private and corporate entities to encrypt e-mail, documents and entire filesystems.

# Bibliography

R. Belfield. *The Six Unsolved Ciphers: Inside the Mysterious Codes That Have Confounded the World's Greatest Cryptographers*. Ulysses Press, 2007.

R.S. Brumbaugh. *The most mysterious manuscript: the Voynich "Roger Bacon" cipher manuscript*. Southern Illinois University Press, 1978.

J. Chadwick. *The decipherment of linear B*. A Canto Book Series. Cambridge University Press, 1990.

D. Kahn. *The codebreakers: the story of secret writing*. Scribner, 1996.

S. Singh. *The Code Book: The Secret History of Codes and Code-breaking*. HarperCollins Publishers, 2010.