Cryptography Throughout History

Allen Jue

Department of Mathematics

UT Austin

April 30, 2025

Contents

Chapter 1

Introduction

The year is 650 BC, and you are a Spartan soldier. The Sun is a relentless thing, blazing overhead, as it has been for millenia. Its heat ravages allies and foes alike, and you can feel its rays penetrating through your bronze plate and armor even as you find a momentary respite beneath an aged tree. You have been trained since a young age as a Spartan soldier to endure such punishment, so this is nothing more than a nuisance in your austere life. In your hand is a strip of cloth that contains a crucial message that you need to deliver to your leader, Aristomenes. It contains battle plans to defeat the Messenians, a long-time enemy. The strange thing is, you do not know what the message contains–it just appears to be a strip of random Phoenician characters. Regardless, you were not trained to ask questions, and feeling rested, you set back on your solitary mission to convey this hidden letter.

❖❖❖

Cryptography has experienced dramatic changes in both its uses and implementations throughout its long history. The Spartan use of encrpyted messages on cloth to transmit cryptographic messages is just one example in cryptography's rich history. To clearly understand how cryptography has changed scientifically and practically, it is imperative to understand its three central tenets: confidentiality, integrity, and availability. To help understand these concepts, we will analyze scenarios involving the titular Alice and Bob (and sometimes the malicious Mallory). They are big fans of cryptography and try to send each other cryptographic messages.

Confidentiality can be understood as privacy around the messages sent between Alice and Bob. A third party should never be able to read their private messages, so Alice and Bob use a *cipher*, a secret code that only they can decipher! Alice starts writing her message in *plaintext*, which is written in a readable way. She then uses the cipher to encrypt or alter the message to create a *ciphertext*. To others, the ciphertext looks like jumbled garbage, but Bob can use the cipher to decrypt the message and see what Alice has sent him.

Integrity is defined as the guarantee that the received message is complete and has not been tampered with. Suppose Mallory is a malicious adversary, and she wants to see what Alice and Bob have been talking about in their letters. However, Alice and Bob have a highly-confidential cryptographic system, so Mallory just decides to change the contents of the message by ripping up some of the letters, erasing the contents of others, and replacing the rest with a collage of letters carefully cut out from a newspaper. Devilish!

Finally, availability is defined as the ability to view the message whenever you need it. We expect our messages to be sent quickly, correctly, and should be available at the tips of our fingers at a moment's notice. When malicious agents are in the picture, this guarantee is at risk. In our story, Alice and Bob have caught onto some of Mallory's ploys, but this time, she is one step ahead of them. She has flooded their mailboxes with junk letters so that genuine letters can not be received. Drats!

Cryptography is a constant battle between honest agents like Alice and Bob and malicious agents like Mallory. Alice and Bob seek a system that is easy for them to decipher and use, while being resistant to tampering and eavesdropping by Mallory. Striking a balance between these three pillars is a painstakingly difficult task that remains at the forefront of cutting-edge research. To understand contemporary cryptographic systems, this paper will trace through the history of cryptographic systems, analyze notable examples of cryptography in use, and identify their weaknesses.

Chapter 2

Ancient Cryptography

2.1 Ancient Civilizations (1500-500 BCE)

The desire to conceal information is as old as civilization itself. In ancient Sumer, the Sumerians had a pantheon of gods, of which, twelve were considered part of the "Great Circle." They sometimes referred to these special gods by an abbreviated coded names, rather than their complete epithets (Bauer 2021, p. 3). Another instance of cryptography was utilized in 1500 BCE in Ancient Mesopotamia on clay tablets. These clay tablets, preserved through their durability, appear to contain secret recipes for ceramic glazes. In Today, deciphering such messages remains a challenge, since the recipients are long gone and are inevitably subject to anachronistic interpretations.

Nearly a millennium later, in 500 BCE, the Ancient Spartans introduced the use of a *skytale* (pronounced like "Italy" but with an sk- prefix), a hexagonal staff of wood. A user would write a message on a piece of cloth wrapped around the skytale to create rows of plaintext message. Upon unwrapping the cloth, the letters appear scrambled, creating a ciphertext. In order to recover the original message, the recipient would use a skytale with the same diameter as the one used to write the message. This introduces

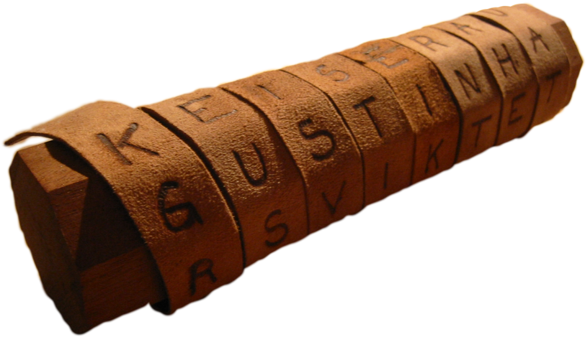


Figure 2.1: A Skytale (Wikipedia, the free encyclopedia 2007).

the idea of a *private key*. This is a shared tool that can be used to encrypt and decrypt a message. Attempting to decrypt a message with a skytale with a diameter that is different from the original skytale, the cloth will generate a message that is unaligned. Evaluating the skytale has a cryptographic instrument clearly demonstrates that the message is not actually secure, as the skytale is a hexagonal prism. By analyzing every six letters, attackers can decrypt the message. Moreover, as a physical instrument, it is subject to theft and degradation. Although there is some historical debate surrounding the actual usage of the skytale, it represents an interesting first step for the development of cryptographic ideas.

2.2 Monoalphabetic Substitution Ciphers (500-44 BCE)

Another early development in cryptography was the concept of *monoalphabetic substitution ciphers* (MASCs). Given an alphabet, which can be defined as the accepted characters that can be used to create words in a language, an MASC assigns each character in an alphabet to a *cipher letter* (Bauer 2021, p. 8). This contrasts to a *polyalphabetic substitution cipher* where each letter is replaced by more than one letter in a cipher, increasing the confidentiality of the ciphertext.

A notable MASC is the Atbash cipher, and it has its roots in the Christian World (Easttom 2022, p. 8). n-th character from the start of the alphabet to the n-th character from the end of the alphabet.

`Plain:  ABCDEFGHIJKLMNOPQRSTUVWXYZ`

`Cipher:  ZYXWVUTSRQPONMLKJIHGFEDCBA`

In this example, the plaintext message `HELLO, WORLD` would be encrypted as `SVOOL DLIOW`.

Another simple MASC could be to "shift" the a character to the character three characters after it (the amount shifted is the private key). If the character reaches the end of the alphabet while shifting, it will continue shifting from the start of the alphabet. Given this cipher of shifting by three characters:

`Plain:  ABCDEFGHIJKLMNOPQRSTUVWXYZ`

`Cipher:  DEFGHIJKLMNOPQRSTUVWXYZABC`

The plaintext message `HELLO WORLD` can be written as `KHOOR ZRUOG`. In fact, such a cipher can be generalized to any shift modulo the size of the alphabet. In other words, shifting by the entire size of the alphabet is a cycle and is the same as not shifting at all. This encryption algorithm is commonly referred to as the Caesar cipher, which was commonly used by Julius Caesar around 100 BCE (Dooley 2018, p. 14) Such a cipher is trivially breakable, as an attacker needs to only try at most 25 different shifts to recover the plaintext message. However, considering the time period and the rate of illiteracy, such an encryption algorithm may have been sufficiently confidential. Unlike the Atbash cipher, the Caesar cipher, relies on shifts to recover the plaintext message, rather a reflection. It can be used in conjunction with the Atbash cipher to create a *reversed Caesar cipher* that offers an extra layer of indirection. Regardless, simply knowing both encryption schemes, allows an attacker to easily decrypt the ciphertext by trial and error.

2.3 Frequency Analysis (900 CE)

While the Western world was heavily reliant on MASCs, these simple ciphers would eventually decline in use until their rediscovery in the Renaissance. Interest in cryptography sprung to life across the world in the Islamic Golden Age (900 CE). Even without knowing the private key to decrypt the cipher text for the aforementioned MASCs, they are still breakable in a trivial amount of time with *frequency analysis*. In the English alphabet, `E` is the most common letter and is more likely to be seen at the end of a word than at the beginning. Conversely, the least common letter used is `Z`. Using prior knowledge of how frequently letters are used, Abu Yūsuf Ya-qūb ibn Isāq as-Sabbāh al-Kindi (801–873 CE) pioneered the use of frequency analysis for cryptanalysis. Al-Kindi noticed that MASCs scrambled the letters, but they did not actually conceal the characteristics of the language. By comparing the frequency of the most common letters in a ciphertext to the frequency of the most common letters in plaintext, it is possible to make educated guesses to decrypt the message, even without knowing the specific cipher.

Chapter 3

Pre-20th Century Developments

3.1 Polyalphabetic Substitution Ciphers (1400 -1550 CE)

As history advanced, monoalphabetic substitution ciphers, such as the Caesar cipher became a liability. While they served their purposes in earlier eras, the rise of literacy, knowledge of these encryption schemes, and increasingly sophisticated decryption techniques–most notably, frequency analysis–rendered these classical schemes nonconfidential. The first pillar of cryptography was being directly challenged, and it was the advent of the Vigenère cipher, a *polyalphabetic susbtitution cipher* that marked a pivotal step forward in mathematics-based confidentiality.

The main issue with MASCs were their inability to conceal underlying characteristics of the language that they were encrypting. The logical step forward is to devise an encryption algorithm that appears to generate a completely random ciphertext. For over three centuries, it was *Le Chiffre Indéchiffrable*, or "The Unbreakable Cipher. (Bauer 2021, p. 60)" Although it is named the Vigenère cipher, there are actually many notable cryptographers that made significant advances to creating a polyalpha-

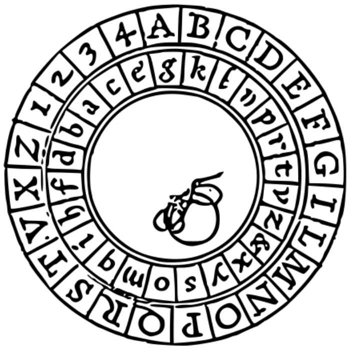
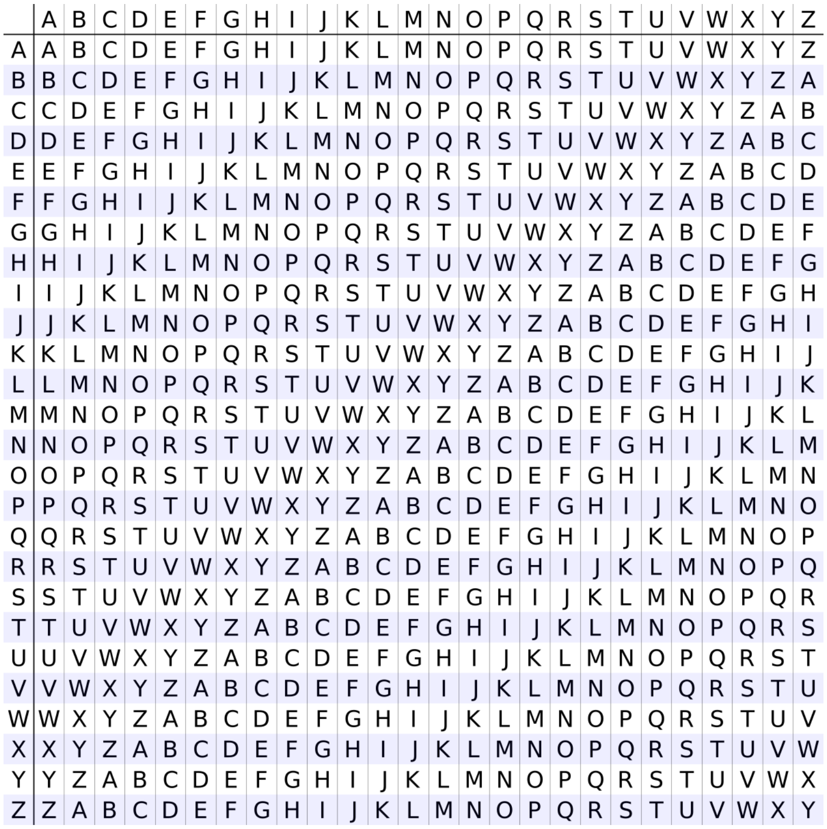

A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
g k l n p r t v z & x y s o m q i h f d b a c e

Figure 3.1: Leon Battista Alberti's Cipher Disk (Wikipedia, the free encyclopedia 2008).

betic substitution cipher.

Rather than using a single alphabet as a cipher, the natural progression was to use multiple rotating alphabets as a cipher. Leon Battista Alberti devised this idea in 1466 with two concentric rings, each with letters upon them. The inner ring would rotate, and the inner letter would be encrypted as the outer letter, which would be differet. After encrypting a few words with this cipher, the encrypter would then rotate the inner ring once more, which would change the cipher. This was the first time more than one cipher alphabet was used. At a cursory glance, this encryption scheme offers a significant security benefit over MASCs, as there is not a singular trivial shift to undo.

About 50 years later, Johannes Trithemius (1462–1516) wrote a book on cryptology–*Polygraphiae*. It describes a *tabula recta*, a matrix that is composed of 26 columns and rows. Each row is the alphabet, where each subsequent row is shifted by one additional letter. The matrix can be imagined as 26 MASC ciphers. Given a plaintext message, the first letter would be encrypted using the Caesar cipher in the first row and the column of the plaintext letter. The second letter would be encrypted by the Caesar cipher of the second row and the column of the second plaintext letter. This repeats for the entire plaintext message, and the key is repeated if it is smaller than the plaintext



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

Figure 3.2: Johannes Trithemius' *tabula recta* (Wikipedia, the free encyclopedia 2021).

message.

In 1553, Giovan Batista Belaso introduced the idea of a keyword to determine the shifting table. The *tabula recta* essentially had a keyword of length 26, which was the entire alphabet. Belaso specialized this to any secret word. Giovanni Batista Porta, another Italian cryptographer, was the one who put all of these prior advancements together. By synthesizing Alberti's polyalphabetic cipher, Trithemius' table cipher, and Belaso's keyword innovation, Porta was able to devise the prototype for the Vigenère cipher.

To help visualize a basic Vigenère cipher in action, consider an example with the plaintext message `HELLO` and the key `KEY`. The key must be repeated to match the value of the plaintext message. To encrypt the first letter of the message, locate the row in the *tabula recta* that corresponds to the first letter in the key, `K`. Then locate the letter in the column that corresponds to the first letter in the plaintext, `H`. Carrying out this process results in the ciphertext `RIJVA` (feel free to try it out yourself).

```
Plaintext:  HELLO
   Key:  KEYKE
Ciphertext:  RIJVA
```

Although still vulnerable to frequency analysis, this cipher significantly "flattens" the character distribution in the ciphertext, making it nontrivial to decrypt the ciphertext.

3.2 Vigenère's Autokey Cipher (1523-1596 CE)

Blaise de Vigenère, born in 1523, is credited with the Vigenère cipher, but his contribution actually lies in the development of the *autokey cipher*. It is an extension of Porta's prototype, which relies on a repeating polyalphabetic substitution key. Vigenère suggested the use of a single priming letter for the key, and the rest of the key is actually the message itself!

Intuitively, if the recipient of a message knows the first letter of the key, they can invert the first letter of the ciphertext by using the aforementioned process of searching the table. This gives them the second letter of the plaintext. The recipient can now use the second letter of the plaintext as the key to deduce the third letter. This process can be used to inductively demonstrate the invertibility of the Vigenère cipher (Vigenère). This is a significant improvement over the repeating keyword used by Belaso, as the non-repeating nature of the keyword further flattens the character distribution of the ciphertext–bolstering the resistance of the encryption scheme to frequency analysis.

3.3 Uses and Downfall of the Vigenère Cipher (1600-1900 CE)

The Vigenère cipher would see significant use in popular media, warfare, and espionage for the next few centuries. Although there are anecdotes of the cipher being broken throughout this time period (for example, Casanova purportedly stole a woman's heart by performing cryptanalysis on her secret messages), it seemed fairly secure (Bauer 2021, p. 65). It would be used throughout the American Civil War by the Confederacy, as it offered confidentiality, integrity, and availability. Rather than sharing common code book to substitute words and needlessly long keywords, it made more sense to have a predetermined keyword used to encrypt and decrypt messages. If these were compromised, it would be much faster to change the keyword than an entire code book. Still, the Vigenère cipher was tedious to use, and small mistakes during encryption would often render the ciphertext illegible.

The Vigenère cipher also had inherent weaknesses due to its repeating keyword. In 1863, Freidrich Kasiski, a cryptanalyst, discovered a method to deduce the length of the secret key. From this, frequency analysis could be applied to recover the plaintext message. Intuitively, Kasiski saw that the English language had repetitive letter pairings, such as `TH` and `THE`. By looking for repeated ciphertext patterns and calculating the distances between them, Kasiski could make educated guesses about the lengths of the repeating secret key (Hananto et al. 2019). In 1920, William Friedman created an innovative statistical attack that further signaled the death of the Vigenère cipher. Recall that the use of the Vigenère cipher flattens the distribution of characters that appear in the ciphertext. Using a metric called the *index of coincidence*, which measured the likelihood that two random letters with a fixed key length will be the same. Friedman could estimate the number of alphabets in use (the length of the keyword)

(Friedman 1987).

Despite its historical prominence, the Vigenère cipher ultimately could not withstand increasingly sophisticated cryptanalysis techniques. However, its legacy should not be overlooked. It remains a significant stepping stone of cryptography from linguistic camouflage to mathematically-grounded security.

Chapter 4

Cryptography During WWI

The year is 1917, and you are sequestered in a dank room in the old British building at the Admirality. Around you curls cigarette smoke that coils like the secret messages that you unravel in your office. Outside is the Great War–the war to end all wars. While soldiers are dying on the Western Front, you are fervently working to find some piece of information in intercepted German telegrams that might help Britain gain an edge in the war. Stumped, you light another cigarette hoping to find some inspiration in the smoke's ephemeral wisps.

❖❖❖

4.1 The Zimmerman Telegram (1917 CE)

To understand the increasing stakes and necessity for secure ciphers, consider the story of the Zimmermann Telegram. The Zimmermann Telegram was message from Arthur Zimmermann, the Director of the German Ministry of Foreign Affairs, to Felix von Eckhardt, the German foreign ambassador in Mexico. In it, Germany requested assistance from Mexico in WWI in exchange for assistance in reclaiming lost territories,

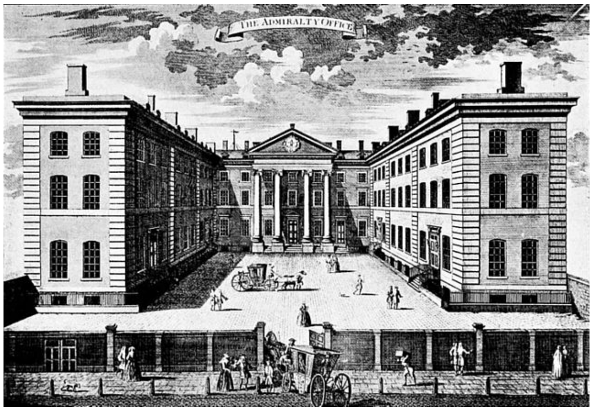


Figure 4.1: Office of the admiralty controlling the Royal navy in Whitehall, London where the *Room 40* codebreaker worked (Wikipedia, the free encyclopedia 1760).

such as Texas, New Mexico, and Arizona. About 50 amateur cryptanalysts in Britain worked on deciphering encrypted messages from Germany and were able to inform the United States about this message (Bauer 2021, p. 166). Subsequently, the United States joined the war on the side Allies, turning the tides in the war. The interception and decryption of a single nonconfidential message can shift alliances, mobilize nations, and ultimately redefine history.

4.2 The ADFGX Cipher (1918 CE)

The ADFGX cipher was the most famous cipher of WWI and was developed by the Germans to be confidential and easily transmittable over Morse code. Despite its sophistication, ADFGX was deciphered by the greatest French cryptanalyst at the time, Georges Painvin, who laboriously worked towards decrypting German messages and reportedly lost 33 pounds over three months while working on this task. The breaking of the ADFGX cipher not only thwarted a major German advance but also marked a turning point in the war, demonstrating how signals intelligence could influence battlefield outcomes. It also foreshadowed the increasingly critical role cryptanalysis would play in future conflicts, especially during World War II (Dooley 2018, p. 108).

The ADFGX cipher uses a 5x5 Polybius square with the letters A, D, F, G, and X as both row and column labels. Within the Polybius square, there is a matrix of plaintext letters. A plaintext letter can be encrypted by replacing it with the pair of letters that comprise its row and column. The pair created is known as a *digraph*. Notice that this will double the length of the plaintext.

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

Suppose that the plaintext is `ATTACK`. Using the Polybius square would yield `AF AD AD AF FC FX`.

Now, choose a keyword, say `CARGO`. Write the text row by row into columns under the keyword:

C	A	R	G	O
A	F	A	D	A
D	A	F	F	X

Now rearrange columns alphabetically by keyword, and read down each column to get the final ciphertext: `FAADDFAXAF`. This final step is known as transposition and it splits the digraphs up. Altogether, deciphering this cipher is extremely difficult without knowing the transposition cipher used on top of the Polybius square.

Decrypting the ADFGX cipher was no easy task, especially given the combinatorial explosion of possible permutations introduced by the transposition step. A keyword with just 10 letters results in 10! (3,628,800) possible column arrangements. Painvin painstakingly worked by hand and was able to use frequency analysis and notice similar code prefixes and suffixes to make educated guesses on possible column arrangements. Considering the limited computational power at the time 10! is non-trivial, and the Germans further bolstered their cipher by adding an extra dimension to the Polybius square.

Painvin's success, despite the overwhelming number of possibilities and lack of mechanical aids, highlighted the limits of mechanical cryptanalysis. It underscored the need for a more systematic, computational method for code breaking. Thus, the cracking of the ADFGX cipher not only thwarted a German offensive but also signaled the dawn of computational cryptanalysis.

Chapter 5

Cryptography During WWII

5.1 The Rotor

Within years after the end of WWI, the field of cryptography experienced a tremendous leap forwards with the invention of the rotor–a mechanical component that could apply polyalphabetic substitution ciphers. Ciphers that could be broken by hand and basic computational power were too weak, and to combat this, exponentially increasing the *key space* of a cipher (the possible secret keys that can be used to encrypt a message) was of the utmost importance. To put into perspective the strength of mechanical rotors, consider the following example. Each rotor can be considered as a polyalphabetic substitution cipher with 26 alphabets. Through intricate machinery, combining just five rotors results in 26^5 (11,881,376 possible alphabets). Rotors were independently created by Edward Herbern (1915), Hugo Koch (1919), and most notably, Arthur Scherbius (1918), who called his rotor cipher machine, the Enigma (Bauer 2021, p. 153)

5.2 The Enigma Machine (1920-1945 CE)

Scherbius' Enigma machine would be adapted into an encryption device used by Germany during WWII. It was composed of movable rotors, cables, and rings. The Enigma machine's encryption relied heavily on principles that can be understood through the lens of group theory, a branch of abstract algebra. Each rotor would apply a composition of permutations or swaps. To use it, a user would enter the ciphertext on a keyboard, which would cause the inner mechanisms to shift and output the plaintext.

5.2.1 Setting up an Enigma Machine

To set up an Enigma machine, operators would choose from 5 rotors and insert them into 3 possible slots. Moreover, recall each rotor has 26 faces and can start on any of their 26 faces. Next, the rightmost rotor would turn one position at every key press. Every 26 presses, it would complete one full *revolution*, and the rightmost rotor would turn the middle rotor on place. Similarly, every time the middle rotor completed a revolution, it would cause the leftmost rotor to turn once. The specific location of when a rotor would cause the next rotor to turn is called the ring and could be adjusted. Finally, there is a "plugboard" that permuted pairs of letters with each other and ranged between 6-10 pairs (Ellis 2005).

- $5 \times 4 \times 3 = 60$ possible rotor locations.
- $26 \times 26 \times 26 = 17,576$ possible starting rotor faces.
- $26 \times 26 = 676$ ring configurations.
- The number of ways to choose k pairs from n items is $\frac{n!}{(n-2k)!k!2^k}$. With $n = 26$ letters and $k = 10$ cables to form pairs, there are around 150 trillion possible combinations.

- In total, there are at least

  $60 * 17,576 * 676 * 150,000,000,000,000 = 106,932,384,000,000,000,000,000$

  combinations. *This is massive.*

Therefore, the setup of the machine itself was the secret key, and the dynamic nature of its internal mechanism posed a serious obstacle for Allied cryptanalysts.

5.3 Breaking the Enigma Machine

The Allies were working feverishly on breaking the Enigma machine at Bletchley Park since the war began in 1939. The effort was led by a team of cryptanalysts, many of whom were women, and contributed to ending the war up to 2 years earlier (Bauer 2021, p. 251). Among them was Alan Turing, a genius mathematician offered his invaluable insights to break the cipher. Turing had notably eccentric habits, such as wearing a gas mask while bicycling to Bletchley Park. His contributions advanced the effort to crack the Enigma machine, as well as laying the groundwork for foundational computer science theories on computability.

The Enigma machine had weaknesses in its ciphertext, as the Germans would frequently encrypt phrases know as *cribs*, such as routine information like *Keinebesondere Ereignisse* and ending with *Heil Hitler*. This non-uniformity of the ciphertext is a weakness (similar to the Vigenère cipher) that would lead to the decryption of some German messages. Turing, along with other cryptanalysts at Bletchley Park would develop a machine called the *Bombe* that would greatly eliminate the key space using cribs into messages that could be decrypted by hand. This was still an extremely tedious task, but its importance can not be overstated (Ellis 2005). The stakes were immense: during periods when Enigma messages were decrypted, Allied naval losses dropped to around 600,000 tons, compared to 2,600,000 tons when the messages remained unreadable.

As a response, the Germans would adjust the Enigma machine to use 4 rotors, which inhibited the Allies' decryption mechanisms. The results would be bloody, leading to a dramatic increase Allied losses. This dynamic showcases the introduction of computationally advanced decryption techniques in the arms race to maintain confidentiality in cryptographic algorithms.

Chapter 6

Contemporary Cryptography

6.1 Modern Cipher Algorithms

To stand against modern attack techniques, contemporary encryption algorithms must have a sufficiently large *keyspace*, possible secret keys to decrypt a message. Beginning in the 1970s, the creation of the Data Encryption Standard (DES) was the first serious symmetric block cipher algorithm. It would encrypt chunks of messages with a Feistel cipher network, a sort of interleaving of rounds of encryption. However, DES only had about a quintillion keys, which on average, half would need to be tried to decrypt a ciphertext message. By 1998, a special purpose computer could crack DES in three days. Subsequently, *Rijndael*, a group from Belgium, developed the Advanced Encryption Standard (AES). It was open source, and is considered to be relatively secure with a sufficient secret key length. Moreover, it is composed of simple operations, such as shifts and XORs, which make it fast (Dooley 2018, p. 212).

6.2 Public-Key Cryptography

Before the 1970s, encryption systems like Enigma, DES, and other ciphers relied on symmetric keys—the same key had to be known by both the sender and the receiver. This posed a major problem: how do you securely share the secret key in the first place? If someone intercepted the key over an insecure network, they could decrypt every message.

This challenge was solved with the invention of public-key cryptography, introduced by Whitfield Diffie and Martin Hellman in 1976 (Dooley 2018, p. 215). Imagine a situation where Bob has a public mailbox that anyone can send letters, but only Bob has the key to open it. Alice wants to send Bob a secret message. She uses Bob's public encryption method, such as slipping the message into his locked mailbox. Even if someone sees the message going in, they can't read it, because they don't have Bob's private decryption key. When Bob checks his mailbox, he uses his private key to unlock it and read the message.

This is the basic idea of asymmetric encryption:

- Public key = mailbox anyone can use to send you secrets
- Private key = key only you have to unlock those secrets

This innovation made secure communication over the internet possible. There is no longer a need to meet in person to share a secret code.

Bibliography

Bauer, Craig (2021). *Secret history: The story of cryptology.* Chapman and Hall/CRC.

Dooley, John F (2018). "History of cryptography and cryptanalysis". In: *History of Computing.*

Easttom, William (2022). *Modern cryptography: applied mathematics for encryption and information security.* Springer.

Ellis, Claire (2005). "Exploring the enigma". In: *University of Cambridge.*

Friedman, William Frederick (1987). *The index of coincidence and its applications in cryptanalysis.* Vol. 49. Aegean Park Press California.

Hananto, April Lia et al. (2019). "Analyzing the Kasiski method against Vigenere cipher". In: *arXiv preprint arXiv:1912.04519.*

Wikipedia, the free encyclopedia (1760). *Admiralty.* [Online; accessed April 30, 2025]. URL: `https://commons.wikimedia.org/wiki/File:Admiralty_office_Whitehall_1760_D_Cunego.jpg`.

— (2007). *Scytale.* [Online; accessed April 30, 2025]. URL: `https://commons.wikimedia.org/wiki/File:Skytale.png`.

— (2008). *Alberti's Cipher Disk.* [Online; accessed April 30, 2025]. URL: `https://commons.wikimedia.org/wiki/File:Alberti_cipher_disk.svg`.

Wikipedia, the free encyclopedia (2021). *Johannes Trithemius' Tabula Recta*. [Online; accessed April 30, 2025]. URL: `https://commons.wikimedia.org/wiki/File:Vigen%C3%A8re_square_shading.svg`.