Using Classical Ciphers to Teach Mathematics in Secondary Education

by

Linae M. Jacox

A thesis submitted to the Graduate Faculty of
Elizabeth City State University
in partial fulfillment of the
requirements for the Degree of
Master of Science in Mathematics

Elizabeth City, North Carolina

May 2021

APPROVED BY

Kenneth L. Jones, Ph.D.	Krishna H. Kulkarni, Ph.D.
Debjani Kanjilal, Ph.D.	Shatoya Covert, M.S.

Dipendra C. Sengupta, Ph.D.
Chair of the Committee

ABSTRACT

USING CLASSICAL CIPHERS TO TEACH MATHEMATICS IN SECONDARY EDUCATION

The purpose of this thesis is to give a brief history of cryptology and to show how to incorporate cryptology into secondary mathematics by introducing some of the mathematics used in the making and breaking of codes, with applications to classical ciphers, specifically, the Caesar Cipher, Affine Cipher, and Vigenere Cipher. By incorporating these types of ciphers into the mathematics's curriculum, students will be able to see how it is relevant in real world situations. Students will be able to use the basic mathematics skills they have already learned over the years to encrypt and decrypt different codes. Using these types of ciphers allow students to think critically and analyze data using the information they are given.

DEDICATION

I would like to dedicate this thesis to my children, Ayana, Jayden, and Lauryn.

ACKNOWLEDGEMENT

I would like to thank my advisor, Dr. Dipendra C. Sengupta for helping and assisting me while working on this thesis. I would also like to thank my husband, my mother, the rest of my family, and friends for their encouragement during this process, I could not have asked for a better support system. A huge thank you to my thesis committee and the rest of the Math Department for your teaching and guidance during my time in the masters program. Last but not least, I would like to thank Dr. Kenneth Jones and Dr. Farrah J. Ward for encouraging me to enroll in graduate school and pursue this degree. You have all played a tremendous role in my success up to this point and I am forever grateful.

Contents

List of Figures

1 Introduction

What is cryptography and why is it essential to keeping information secure? Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it (Rouse, 2014). Even though cryptography is associated with computer science, it gets its derivative from algorithms. Algorithms is a mathematical concept that uses rules which must be followed in performing calculations or other problem-solving operations. For example, when scientist need computers to perform complex operations, they use algorithms to make the calculations. The purpose for using cryptography has changed over time to keep up with today's needs. Cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption) (Rouse, 2014). The word cryptography comes from the Greek words kryptos meaning hidden and graphein meaning writing (Pawlan, n.d.). It is the science of encrypting and decrypting information by using algorithms to scramble data and a key for the person unscrambling the information to decrypt it. This is somewhat like working with cryptograms or cryptoquips which is a word puzzle featuring letters of the alphabet that has been encrypted so that the person playing the game has to use critical thinking skills to decrypt it by only knowing what one letter of the encryption represents. Nineteenth century scholars decrypted ancient Egyptian hieroglyphics when

Napoleon's soldiers found the Rosetta Stone in 1799 near Rosetta, Egypt in the tomb of Khnumhotep 11 of Egypt. Rosetta Stone is a piece of steel made from granite that was discovered in 1799 which had an inscription on it that was written in three languages giving an official order issued in Memphis, Egypt during the Ptolemaic dynasty on behalf of King Ptolemy V Epiphanes. The inscription on the Rosetta stone was praising King Ptolemy V but the inscription was written in three ancient languages: Demotic, hieroglyphics, and Greek. The important thing about this message is that it was inscribed three times, hieroglyphs – for the priest, demotic – which was the language of the people, and ancient Greek – the language of the administration. To decipher the meaning on the Rosetta Stone, the scholars who could read ancient Greek, decrypted the other languages by translating the Greek and comparing the three inscriptions (Pawlan, n.d.). The writing on the stone is an official message about King Ptolemy V between 204 – 181 BC). The decree was copied on large stone slabs which were put in every temple in Egypt. It says that the priests of a temple in Memphis supported the king (Walker, 2017). Cryptography has been around for thousands of years to help hide secret messages. Gerhard Strasser traces the development of encryption through the Middle East and Europe, and even to India. He tells of a Medieval German cryptographer accused of black magic, and an 18th-century government minister in France who devised an ingenious way to spy on visitors (Waddell, 2016). Gerhard Strasser gave information that research showed an encrypted message, in which craftsmen camouflaged the recipe for a pottery glaze that was a greatly sort after item during 1500 BC. This showed an early interest in cryptographic communication. Another example of using cryptography is when the exiled Jewish scribes, who wrote the Book of Jeremiah, sometimes obscured the word “Babylon” by using what is now known as the Atbash cipher in which letters at opposite ends of the Hebrew alphabet were swapped (Lester, 2001). There have been many adjustments and names given to ciphers. The ciphers from the classical era used classical algorithms and were not very secure. Some of them were used by people while others were used in the armies. The classical ciphers were used pre WW11 and would be easily broken by computers of today. There were approximately 26 ciphers introduced during this era. The first one was the Atbash Cipher which was a substitution cipher with a specific key where the letters of the alphabet are reversed (Classical, n.d.). This was the simplest and easiest cipher to be broken. Next in line according to simplicity was the ROT13 Cipher, the Caesar Cipher, the Affine Cipher, the Rail-fence Cipher, the Baconian Cipher, the Polybius Square Cipher, and the Simple Substitution Cipher (Classical, n.d.). Around 100 BC, Julius Caesar was known to use a form of encryption to convey secret messages to his army generals posted in the war front. This substitution cypher was known as the Shift or Caesar cipher, which was perhaps the most mentioned historic cipher in academic literature (Sidhpurwala, 2019). The Caesar cipher is one of the earliest known and simplest ciphers because it is a type of substitution which each letter in the plaintext is shifted a certain number of places down the alphabet. To pass on the encrypted message from one person to another, it is necessary that both parties have the key for the cipher so that the sender may encrypt it and the receiver may decrypt it (Cryptography, n.d.). Another type of substitution cipher is the Affine cipher or linear cipher. Even though affine ciphers are examples of substitution ciphers, and are thus far from secure, they can be easily altered to make a system which is secure (Walker, n.d.). If instead of using one letter at a time to decipher the code and we used a block of letters, keeping mathematics the same, the ease of cracking the system would be of a greater challenge. Even though Affine Block ciphers are secure, there is still a problem with them because they are symmetric. In other words, anyone who knows the encryption function also knows the decryption function (Walker, n.d.) During the 16th century, Vigenere designed a cipher that was supposedly the first cipher which used an encryption key. As with the Caesar cipher, Vigener's cipher can also easily be broken; however, Vigenere's cipher brought the very idea of introducing encryption keys into the picture (Sidhpurwala, 2019). The earliest authentic alchemical manuscript recorded is that of St. Marks at Venice which is believed to have been transcribed from earlier writings that were ascertained to have been written at about the end of the third century and considered to be the highest value for the history of chemistry and this throws a whole flood of light upon the origins of the pseudo-science, alchemy, as the researches of Berthelot have so clearly demonstrated (Caley, 1926). This document was used to conceal the crucial portions of important chemical equations which at that time people deemed it to be magic. Another era in history where cryptography was used was during the fourteenth century in Italy where Gabrieli di Lavinde of Parma, a secretary of Pope Clement VII in the latter part of that century, prepared a manual of keys for twenty-four of the Pope's correspondents. This collection contained some keys which combined ciphers and codes and were intended to confuse the cryptanalyst (Belfield, 2007). There were many other people who contributed to the art of cryptography. Johannes Trithemius wrote the first printed book on cryptology where he invented a steganographic cipher in which each letter was represented as a word taken from a succession of columns. Giovan Batista Belaso introduced the notion of using a passphrase as the key for a repeated polyalphabetic cipher while Giovannie Battist Porta wrote a text on ciphers introducing the digraphic cipher which classified ciphers as transposition, substitution, and symbol substitution. In 1623 Sir Frances Bacon described a bilateral cipher which now bears his name known as a 5-bit binary encoding. He advanced it as a steganographic device by using variation in type face to carry each bit of the encoding. While serving as George Washington's secretary of state, Thomas Jefferson devised an ingenious and secure method to encode and decode messages called the "wheel cipher" (Jefferson, n.d.). Before the invention of the wheel cipher, messages were delivered by messengers, but once he became prime minister to France, codes were necessary because European postmasters opened and read letters that passed through their station. To keep the information secret, it was imperative to create a way to divert the information from getting into the hands of the enemy. Jefferson never used the wheel, but it was independently reinvented in the early 20th century designated as M-94. It was used by the army and other military services from 1922 to the beginning of world war 11 (Jefferson, n.d.). During the Civil War, the telegraph made its debut in bringing in cryptology. The telegraph, Morse code, marked the beginning of a century and a half of rapid development of new techniques in both cryptography and cryptanalysis, all starting during the American Civil War (Dooley, 2018). It also presents a description of the biggest cryptanalytic breakthrough of the nineteenth century, the breaking of the unbreakable cipher, the Vigenere (Dooley, 2018). Instead of using alphabets, the Vigenere uses keywords to pick which columns to use. Another cipher was the Homophonic Substitution Cipher which is a substitution cipher in which single plaintext letters can be replaced by any of several different ciphertext letters and are generally much more difficult to break than standard substitution ciphers (Homographonic, n.d.). It is difficult to break homophonic substitution ciphers if the homophones are high. Edward Hebern's machines made it possible for the receiver to penetrate but impossible for anyone else to decipher; however, he never made enough money to live on. He got his idea for his machines while he was in jail. Around 1908 began one of the most important innovations in cryptographic history where he used rotating disks to complicate the encrypting pattern (Zorpette, 1994). These machines were the basis for virtually all enciphering devices used to cloak sensitive diplomatic and military communications the world over (Zorpette, 1994).

Cryptography played an important role during world war 1 which lasted from July 28, 1914 to November 11, 1918. Zimmerman was instrumental in creating the Zimmerman telegram. This telegram was from Germany to Mexico containing important information that was crucial for the winning of world war 1. The information, however, was intercepted and decrypted by the British, led by Admiral Hall. The information included German's plans for unrestricted submarine warfare, as well as a proposal asking Mexico to ally with the Germans and invade the US (Miles, 2019). Admiral Hall decided not to tell the Americans about the information because he knew the US would condemn Germany's acts and Germany would know that their encryption system had be compromised and would strengthen it (Miles, 2019). During world war 1 countless lives were compromised, but by knowing the plan, Germany did not win the war and the US, and their allies were victorious. During the first two years of world war 1, code systems were used for high-command and diplomatic communications and cipher systems were used almost exclusively for tactical communications (Simmons, n.d.). to form a more intelligent device that would help them know the plans of their enemies. William Frederick Friedman was a cryptologic officer during World War 1 and it was the beginning of his career which he was later viewed as the US Father of Cryptanalysis. Friedman's contributions are prolific author, teacher, and practitioner of cryptology (Friedman, n.d.). His greatest achievements were introducing mathematical and scientific methods into cryptology and producing training materials used by several generations of pupils (Friedman, n.d.). Friedman's work enhanced signals intelligence and information security and much of what is done today at NSA. Friedman was the chief cryptanalyst of the war department in Washington, DC from 1941 to 1947 (Colonel, 2006). He led the US army team (Special Intelligence Service) which broke the major Japanese diplomatic code in 1940 (Purple Code) and subsequently remained a key member of the Operation Magic teams which decoded Japanese ciphers and enabled US military commanders to read Japanese intercepts on Japanese military movements (Colonel, 2006). His most important contribution made by Magic was to the US victory in the Pacific was the decoding of ciphers that revealed the Japanese attack plan for the Battle of Midway in mid-1942 (Colonel, 2006). Vital to victory in world war 11, wireless radio communication was very important for directing military forces that were spread all over the world, but radio messages could be intercepted so secret information had to be transmitted in secret codes (Secrets, 2015). Every major country uses machinery that turns simple text into secret codes to protect their military plans. On the same way you have cryptanalysts – code breaking experts – working on decrypting their codes. Polish and British mathematicians were able to read the German messages early in the war by copying the German Enigma machine and solved its letter-scrambling patterns (Secrets, 2015). Cryptanalysts also exploited Japanese codes and by late 1940, the US army and navy could read Japanese diplomatic messages between Tokyo and embassies in London, Washington, Berlin, and Rome

(Secrets, 2015). As the war continued, the allies combined their intelligences and were able to defeat their enemies because of the use of ciphering systems. The Enigma ciphering system enabled the western allies in World War 11 to read substantial amounts of Morse-coded radio communications of the Axis powers that had been enciphered using Enigma machines and other decrypted Axis radio and teleprinter transmissions and was the decisiveness of the Allied victory according to Commander Dwight D. Eisenhower (Enigna, n.d.). The Enigma is shaped like a huge typewriter that is both mechanical and electrical in its workings. The person encrypting the message enters the letters of the message and a letter lights up showing the replacement for each letter of the message. Once inside, the system is built around three physical rotors that the letters pass through and bounce off a reflector at the end and passes back through all three rotors in the other direction. When the first rotor has turned through all 26 positions, the second rotor clicks round, and when that's made it round all the way, the third does the same, leading to more than 17,000 different combinations before the encryption process repeats itself (Hern, 2014). The person receiving the message sees the coded message, but when they type in "ciphertext," they see the decoded one. The ROT13 Cipher is a substitution cipher with a specific key where the letters of the alphabet are offset 13 places (ROT, n.d.). It is sometimes called a Caesar Cipher 13 because it moves 13 spaces down the alphabet to match the corresponding letter. For example, a "C" would be replaced with a "P" and a "D" would be replaced with a "Q." Once someone finds the first letter substitution, it is easy to find the other letters of the message to be encrypted so this cipher is considered to not be one with a lot of dependence because it can be easily broken. As cryptography continued the rise with better machines and different types of information it can decode, the business world came on board to connect the world around us. The exchange of sensitive information is a constant of 21st Century life. We withdraw cash form ATMs, make purchases with credit and debit cards, shop online, send and receive emails, and conduct business on smartphones. Cryptography helps to keep all that data private and secure (World, n.d.). IBM chairman Thomas J. Watson, Jr. set up a cryptography research group and the purpose of the group was to protect the data from cash-dispensing systems. They named the method, "Lucifer," which was bought by the United Kingdom and in 1971, Lloyds Bank bought the code, and IBM worked to turn Lucifer into a commercial product (World, n.d.). Since Lucifer had already been published, its algorithms already examined, the US National Security Agency contributed to consulting and technical advice, and the final version reduced key size was still strong, the algorithms lent itself to implementation in the hardware and software of computers (World, n.d.). On January 15, 1977, the NBS adopted IBM's cryptographic algorithm as the first-ever Data Encryption Standard (DES) for the United States, and the world would soon follow. Security technology expert Bruce Schneier said almost all the encryption algorithms can trace their roots back to DES (World, n.d.). As the arms race came into view, the info section of the industry began to look at quantum cryptography and quantum key distribution. Quantum cryptography, also called quantum encryption, applies principles of quantum mechanics to encrypt messages in a way that is never read by anyone outside of the intended recipient (Korolov & Drinkwater, 2019). In addition, a quantum computer which can encrypt, and decrypt data must be used to perform these tasks. Around the world there are companies in a race to build the first usable quantum computer because this technology promises to solve the more intricate computing problems than with today's computers (Korolov & Drinkwater, 2019). The plan for the quantum computer is to be able to solve thousands of problems at the same speed with the same processing power instead of solving one problem at a time. This would cut the time it takes to do a task in a record amount of time, as we know it today. The quantum computers that are on the market today have not been able to complete the task that programmers are seeking, but they are continuing to work on it and test their theories. Who knows what kind of technology isn't available on the public market, or is operated in secret by foreign governments (Korolov & Drinkwater, 2019)? The fear of the cryptanalyst is that things may happen before they are aware they have been done. Professor Ronald Rivest author of the earlier RC2 and RC4 algorithms included in RSADSI's BSAFE cryptographic library, published a proposed algorithm, RC5, on the Internet. This algorithm uses data-dependent rotation as its non-linear operation and is parameterized so that the user can vary the block size, number of rounds and key length (Kahn, n.d.). He is an inventor of the RSA public-key cryptosystem, and founder of RSA Data Security (Rivest, 2020). Professor Rivest has a repertoire of experience in the fields of computer science and engineering. He also has extensive experience in cryptographic design and cryptanalysis, as well as published numerous papers in these areas (Rivest, 2020). One of the papers he and some colleagues wrote was Cryptographic Communications System and Method. This paper showed how the system includes a communications channel coupled to at least one terminal having an encoding device and to at least one terminal having a decoding device. Another paper he wrote with other colleagues was A Method for Obtaining Digital Signatures and Public-key Cryptosystems. In this paper it stated there are two important consequences: 1) Couriers or other secure means are not needed to transmit keys, and 2) A message can be signed using a privately held decryption key (Citations, 2009). There are numerous crypt-analysts doing research to better improve the security system and keep our nation safe. Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems (Definition,n.d.).

2 Caesar Cipher

The Caesar Cipher or Shift Cipher as it is sometimes called, is another monoalphabetic substitution cipher (Clark, 2017). The Shift Cipher is a monoalphabetic cipher or a substitution cipher in which the cipher alphabet for each plain alphabet is fixed throughout the encryption process (Ciphers, n.d.). This means that whatever alphabet you exchange another alphabet for, it will remain constant throughout the encryption process. The Shift Cipher is one of the easy and most famous encryption systems that use the substitution of a letter by another one further in the alphabet (Caesar, n.d.). Even though it is famous, it is not very secure. A cipher should prevent an attacker from discovering the contents of the message, but since we only have 26 choices for the keys someone can easily try all the keys until they come to one that decrypts the message. The Shift cipher or Caesar cipher is named after Julius Caesar, who used it with a shift of three to protect messages of military significance. He used this method to communicate with his generals (Cipher, 2017). Even though Julius Caesar is one of the first known to be recorded use coding, other ciphers are known to have been used earlier. No one knows how effective the coding was for Julius Caesar but is likely to have been secure because the kings that were his enemies were not illiterate. They had kingdoms that they ran; therefore, it can be assumed that they had leadership skills and knowledge of how to run their kingdoms to not allow the enemy to overthrow them. Using the Caesar Code that Julius Caesar used years ago is easy to encrypt and decrypt which makes it easy for anyone to decipher or interpret the code making the code unusable in today's world of technology. For example, if you were to decipher BARZXQFLK with a shift of 3, you would look 3 letters after each letter to find the code. The B = E; A = D; R = U; Z = C X = A Q = T; F = I; L = O; K = N: The decrypted word would be "Education." Once you find the first letter and which shift is used, it is easy to decrypt the word. Another way this can be explained is to crypt the letter (of value 3), add the shift 3: B is the 2nd letter of the alphabet, so (2 + 3 = 5) the 5th letter of the alphabet is E. The code would decrypt the same alphabet as using the first code.

2.1 How to encrypt a Caesar Cipher (Shift Cipher)

To encrypt a message using modular math and the shift cipher, there are several steps you need to take. First, convert the letter into the number that matches its order in the alphabet starting from zero, and call this number "X." For instance, (A=0, B=1, C=2, . . . , Y=24, and Z=25). Next, calculate using the formula Y = (X + K) mod 26. Last convert the number "Y" into a number that matches its order in the alphabet starting from "0" (Khan, n.d.). Word length and punctuation provide patterns that permit us to quickly make sense of plaintext. Usually cryptographers do not give word length and punctuation (Christensen, 2006). Without word length and punctuation, even plaintext can be difficult to read and therefore to give more security to the message.

2.2 How to decrypt a Caesar Cipher (Shift Cipher)

To decrypt a message using modular math and the shift cipher, you must convert the letter into the number that matches its order in the alphabet starting from "0," and call this number 'Y." To do this, (A=0, B=1, C=2, . . . , Y=24, and Z=25) as stated in encrypting a message. Next, calculate X = (Y − K) mod 26. Last, convert the number "X" into a letter that matches its order in the alphabet starting from "0" (Khan, n.d.) To pass an encrypted message from one person to another, it is first necessary that both parties have the "key" for the cipher, so that the sender may encrypt it and the receiver may decrypt it (Cryptography, n.d,). As stated earlier, one way of decoding the message is finding out the number of times the alphabet is shifted. This shift can be positive or negative.

2.3 Examples

Example 1: Shift 3 The easiest way to understand the Caesar cipher is to think of cycling the position of the letters. In a Caesar cipher with a shift of 3, "A" becomes "D," "B" becomes "E." "C" becomes "F" and so on that when you get to the end of the cycle, "Y" becomes "A," and "Z" becomes "B" (Decoder et.al, n.d.).

The plaintext and the cipher are listed below.

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
Cipher	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

Table 1: Shift 3 Equivalents of Letters in the Alphabet

DREAMS DONT WORK UNLESS YOU DO

The cipher text for all letters are given below

GUHDPV GRQW ZRUN XQOHVV BRX GR

Because of the simplicity of this cipher, there is not much security against those who may try to decode it.

Example 2: Modular Math and Caesar Cipher (Shift Cipher) To encrypt using math, we assign a number to each letter of the plaintext alphabet, beginning with “0” and ending with “25” because there are only 26 letters of the alphabet. The numerical value of the letter A is 0 and each letter of the alphabet thereafter goes in ascending order with B’s value being 2, C’s value being 3 and continuing until Y’s value is 24 and Z’s value is 25. The letter or plaintext is referred to as the number “X” in the equation and the numerical value is “Y.” The formula is Y = (X + K) mod 26 with a shift key of 19. The letter of the alphabet’s equivalent is posted in the chart below.

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
Numerical Equivalent	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Numerical Equivalents of Letters in the Alphabet

ENCRYTION

E C S U

4 2 18 20

+ 19 19 19 19

$(23\ 21\ 37\ 39) \bmod 26 = 23\ 21\ 11\ 13$

X V L N

After applying the Shift Cipher with key K = 19, our message text for "ECSU" is "XVLN." "XVLN" is the message given to the person to decode along with the key. Note if the mod 26 is larger than "25," then you start back to the beginning and count the number of excess spaces needed. Do not forget to factor in the fact that "A" is "0."

Example 3: Negative Shift with Block 5 Giving word length and punctuation gives the cryptanalyst too much information. Because it hides word length, blocking makes the ciphertext harder to cryptanalyze (Christensen, 2006). By using blocking, it makes it harder for someone to break the code. An example of a message to be decrypted using a -2 or subtracting 2 shifts is as follows. The message to be decrypted is: "Mathematics is essential to education."

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
Cipher	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

Table 3: Shift Equivalents of Letters in the Alphabet

MATHE MATIC SISES SENTI ALTOE DUCAT ION

The cipher equivalents for all letters are given below.

OCVJG OCVKE UKUGU UGPVK CNVQG FWECV KQP

2.4 Cryptanalysis (How to Break the Code)

A message encoded with the Caesar cipher has a shift in its frequency analysis diagram (equal to the selected shift) and a coincidence index like the one of the plaintexts (Caesar, n.d.). If it is known that a Shift Cipher has been used, but the key is unknown, it is still simple to break the code by a simple means using a trial and error approach to the attack the cipher. The main weakness of the Shift cipher is that fact that there are only 26 keys one of which is the identity mapping that leaves the plaintext unaltered. For example, given the intercepted ciphertext "RFWHZX HWFXXZX," where the key used is unknown, but the Shift cipher has been implemented can be found by trial and error method. So, you try a key of 1, then a key of 2, then a key of 3 and so on, until a plaintext that makes sense is returned. For this ciphertext we would get:

•A key of 1 gives the plaintext "gevgyw gvewwyw." This doesn't make sense, so try the next one.

•A key of 2 gives the plaintext "pdufxv fudvvxv." This also does not make sense, so you go to the next one.

•A key of 3 gives the plaintext "octewu etcuuwu." Again, this does not make sense, so you go to the next key.

•A key for 4 gives the plaintext "nbsdvt dsbttvt." Still this does not make sense, and you continue to the next key. Remember this is a trial and error type of cipher.

●A key of 5 gives the plaintext “marcus crassus.” This makes sense in that it is a person’s name. So, a key of 5 is used for this code (Clark, 2017)

3 Affine Cipher

The Affine Cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter (Zafar, 2019). This cipher provides a little more security than the Caesar cipher because it uses multiplication and addition to find the ciphertext. Affine Cipher is another type of shift or substitution cipher that uses encryption that gives value to a letter or number. Each time a given letter occurs in the plaintext, it always is replaced by the same ciphertext letter. For example, if the plaintext letter "m" is replaced by the ciphertext letter "p," the letter "m" will always be replaced by the "p" each time it is in the message.

3.1 How to encrypt an Affine Cipher

The encryption key for an affine cipher is an ordered pair of integers, both of which come from the set (0, . . . , n – 1), where n is the size of the character set being used and in this case n = 26 because of the number of the letters of the alphabet (Affine, n.d.).

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
Numerical Equivalent	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 4: Numerical Equivalents of Letters in the Alphabet

If we were to encrypt the message "mail" using an affine cipher with encryption key (2,1), we would use the following instructions to find the ciphertext.

1. the table, we replace the letters in our message "mail" with their corresponding numbers: 12 0 8 11.

2. Now multiply each of the numbers from step by the first number in the encryption key, (2 in this case), to get: 24 0 16 22.

3. Next, add the second number in the encryption key, (1 in this case), to each of the numbers from step 2 to get: 25 1 17 23

4. Now use the table to replace the numbers from step 3 with their corresponding letters to obtain the ciphertext: Z B R X

As with shift ciphers, there is a small complication when the arithmetic we do in steps 2 and 3 produces a number that is larger than 25 (Affine, n.d.). For instance, if we were to use the word "encrypt," and use the same encryption key of (2,1), how would the encryption look? First, you would perform steps 1,2, and 3 the same as in the word "mail."

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
Numerical Equivalent	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 5: Numerical Equivalents of Letters in the Alphabet

1. Replace the letters in the word "encrypt" with the corresponding numbers: 4 13 2 17 24 15 19.

2. Now multiply each of the numbers in step 1 by the first number in the encryption key to get: 8 26 4 34 48 30 38.

3. Next, add the second number in the key to each of the numbers in step 2: 9 27 5 35 49 31 39.

4. Because some of the numbers are larger than the numbers in your character set, we have to replace each number from the set (0,. . ., 25) that is congruent to it in modulo 26.

In summary, affine encryption on the English alphabet using the encryption key (a,b) is accomplished by the formula E(x) = (ax + b) mod m where a and b are the key for the cipher (Rodriguez, 2019). To get the ciphertext you must do the following:

$E = 4 = 4 \text{ x } 2 + 1 = 9 \text{ (mod 26)} = J$

$N = 13 = 13 \text{ x } 2 + 1 = 1 \text{ (mod 26)} = B$ (Hint: 27 – 26 = 1)

$C = 2 = 2 \text{ x } 2 + 1 = 5 \text{ (mod 26)} = F$

$R = 17 = 17 \text{ x } 2 + 1 = 9 \text{ (mod 26)} = J$ (Hint: 35 – 26 = 9)

$Y = 24 = 24 \text{ x } 2 + 1 = 23 \text{ (mod 26)} = X$ (Hint: 49 – 26 = 23)

$P = 15 = 15 \text{ x } 2 + 1 = 5 \text{ (mod 26)} = F$ (Hint : 31 – 26 = 5)

$T = 19 = 19 \text{ x } 2 + 1 = 13 \text{ (mod 26)} = N$

The ciphertext for “encrypt” using (2,1) mod 26 would be “jbfjxfn”. When using a key that creates a situation where more than one plaintext letter is encrypted to the same ciphertext letter, this means that when it comes to decrypting, the recipient will be unable to know which one of the plaintext letters has been used thus making the encryption more problematic for someone trying to get the code.

3.2 How to decrypt an Affine Cipher

To decrypt the ciphertext, we must perform the opposite (or inverse) functions on the ciphertext to retrieve the plaintext (Rodriguez, 2019). As with encrypting a code, to decrypt you must also follow a set of steps. The first step is to convert each letter of the ciphertext into their integer values just as was done in encrypting the code. We must perform the following calculation on each integer:

$$\mathrm{D(x) = c\ (x - b)\ mod\ m}$$

Where "c" is the modular multiplicative inverse of "a." This means where a x c = 1 mod m (c is the number such that when you multiply "a" by it, and keep taking away the length of the alphabet, you get 1) (Rodriguez, 2019). To decrypt the ciphertext, you must follow the steps below:

1. Find the inverse of "a."
2. Now perform the inverse calculations on the integer values of the ciphertext.
3. Next, find the answers in modulo 26.
4. Convert the integers back to plaintext letters.

3.3 Examples

Example 1: In deciphering the ciphertext, we must perform the inverse or opposite functions to retrieve the plaintext. Just to recall the procedure, we need to convert each of the ciphertext letters into their integer values. Next, perform the calculations and last find the modulo 26 and last convert the numbers into letters.

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
Numerical Equivalent	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption: Key values (17, 20)

Original Text	A	C	T	I	O	N
x	0	2	19	8	14	13
(ax + b) mod 26	20	2	5	0	24	7
Encrypted Text	U	C	F	A	Y	H

Decryption: $(a)^{-1} = 23$

Encrypted Text	U	C	F	A	Y	H
Encrypted Value	20	2	5	0	24	7
23 (x-b) mod 26	0	2	19	8	14	13
Decrypted Text	A	C	T	I	O	N

Example 2:

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
Numerical Equivalent	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption: Key values (5, 8)

Original Text	S	Q	U	A	R	E
x	18	16	20	0	17	4
(ax + b) mod 26	20	10	4	8	15	2
Encrypted Text	U	K	E	I	P	C

Decryption: $(a)^{-1} = 21$

Encrypted Text	U	K	E	I	P	C
Encrypted Value	20	10	4	8	15	2
21 (x-b) mod 26	18	16	20	0	17	4
Decrypted Text	S	Q	U	A	R	E

3.4 Cryptanalysis (How to Break the Code)

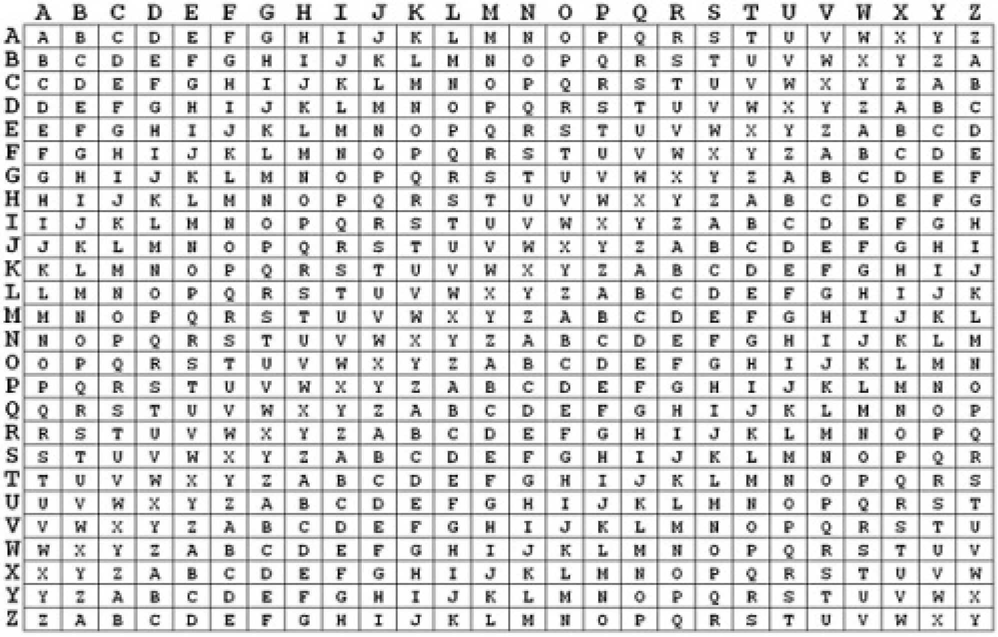
The Affine cipher is a very insecure cipher, with the Caesar cipher possibly being the only easier cipher to crack (Cryptography, n.d.). Because the Affine cipher is a monoalphabetic substitution cipher, the methods used to crack their codes can also be used to crack the Affine cipher. Also, if you know the formula and any two characters, you can crack the code. Another way is break the code of an Affine cipher is to analyze the frequency of certain letters, or pairs of letters, or from a known or guessed part of the original message (which is called a "crib") (Oxford, n.d.). When breaking an Affine code, you can also start by taking the ciphertext and correspond it to the number equivalent. Then, you would produce the sequence and finally you interpret the numbers again as letters to produce the plaintext.

4 Vigenere Cipher

The Vigenere Cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets (Geeks, 2020). This cipher was invented by the 16th-century French cryptographer Blaise de Vigenere and used for data encryption in which the original plaintext structure is somewhat concealed in the ciphertext by using several different monoalphabetic substitution ciphers rather than just one (Simmons, 1987) . This substitution cipher uses a one-to-many relationship between the letter and the one they substitute instead of a one-to-one relationship between the letter and its substitute as most substitution ciphers do.

4.1 How to encrypt an Vigenere Cipher

The Vigenere Cipher uses a 26x26 table and a keyword which is repeated until it equals the plaintext it is supposed to represent. In addition to the plaintext, the Vigenere cipher also requires a keyword, which is repeated so that the total length is equal to that of the plaintext (MTU, 2020). The 26x26 table starts with the letters of the alphabet going across and then coming down as the headers. The first row of the table is uses the 26 letters in their original position. The next row shifts to the left one position, therefore starting the second row with a “B” and ending with an “A.” On the third row the first letter is a “C,” and the last letter is a “B.” This pattern continues until the entire table has been completed. The keyword is a word used over and over until it reaches the end of the selected plaintext. The strength of the Vigenere cipher is that the same letter can be encrypted in different ways depending on the keyword. Vigenere-like substitution ciphers were regarded by many as practically unbreakable for 300 years (Morelli, 2014).



	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 1: Vigenere Cipher 26x26 Table

For example, suppose the plaintext was ELIZABETH CITY STATE UNIVERSITY and the keyword is MATHEMATICS, then the keyword would be repeated at follows:

ELIZABETH CITY STATE UNIVERSITY

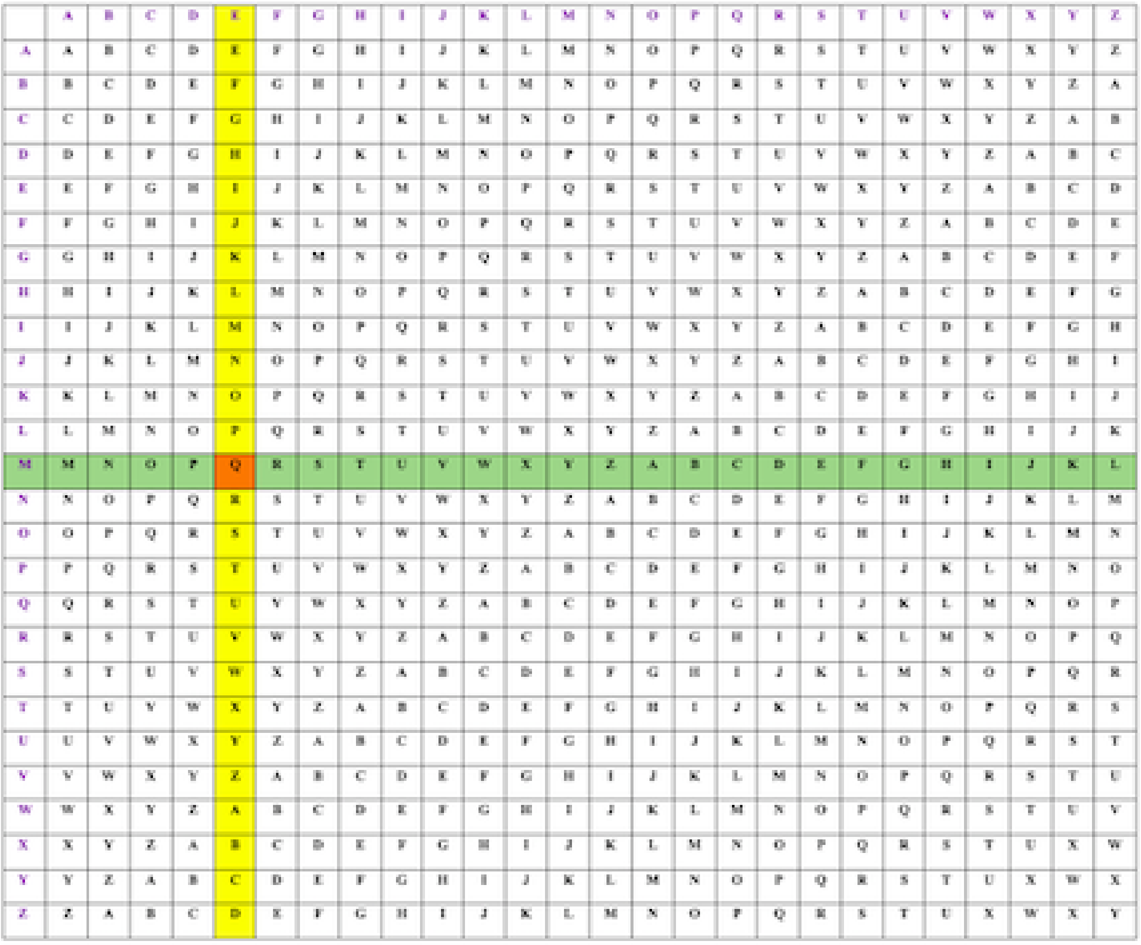
MATHEMATI CSMA THEMA TICSMATICS

Now we remove all spaces and punctuations, if there be any, and divide the result into 5-letter blocks. The result is as follows:

ELIZA BETHC ITYST ATEUN IVERS ITY

MATHE MATIC SMATH EMATI CSMAT ICS

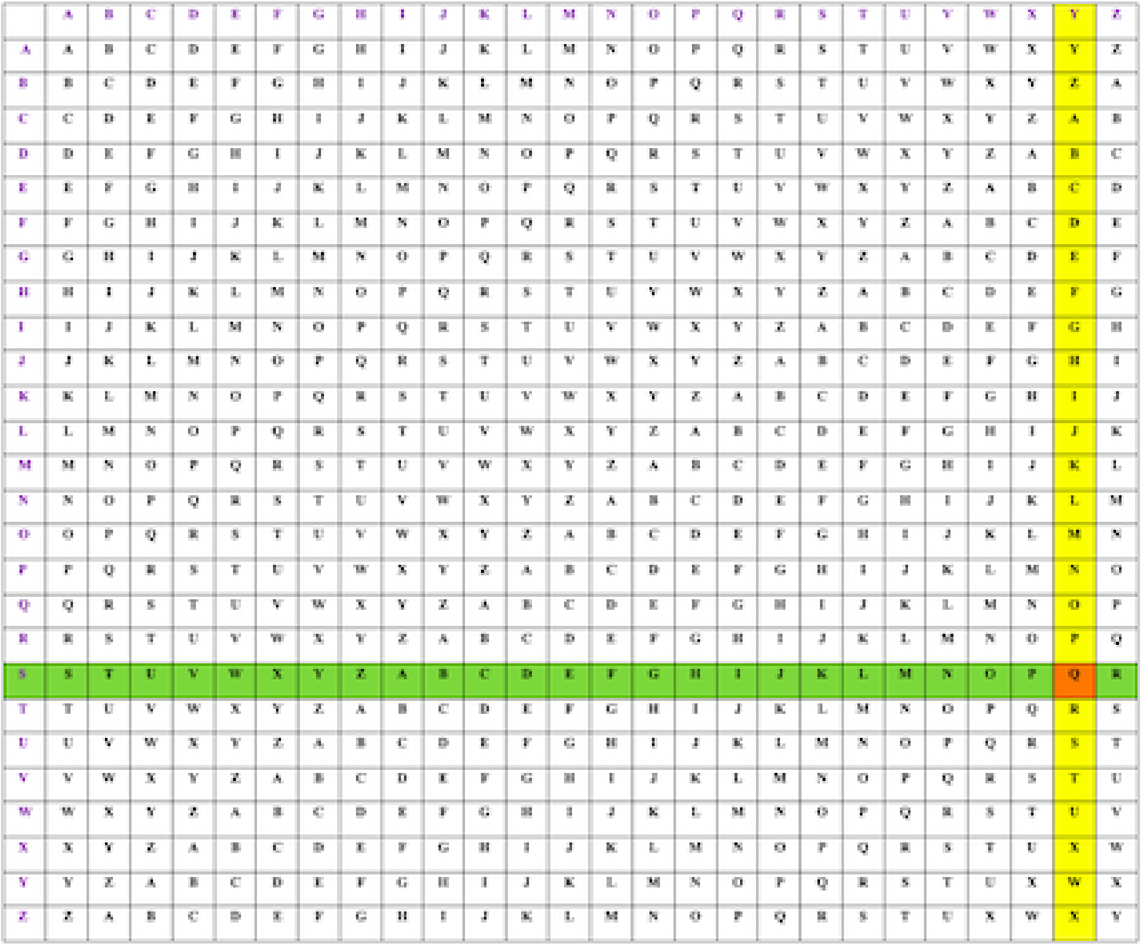
To encrypt, you take the letter in the plaintext and its corresponding letter and find the intersection in the Vigenere Table. The first two letters are "E" and "M." When you intersect the two letters you get the letter "Q." You continue this pattern until all plaintext letters are processed.



	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	X	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	X	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	X	W	X	Y

Figure 2: Example Vigenere Cipher 26x26 Table 1

The last two letters are “Y” and “S.” When you intersect these two letters you get the letter “Q.”



	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	X	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	X	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	X	W	X	Y

Figure 3: Example Vigenere Cipher 26x26 Table 2

ELIZA BETHC ITYST ATEUN IVERS ITY

MATHE MATIC SMATH EMATI CSMAT ICS

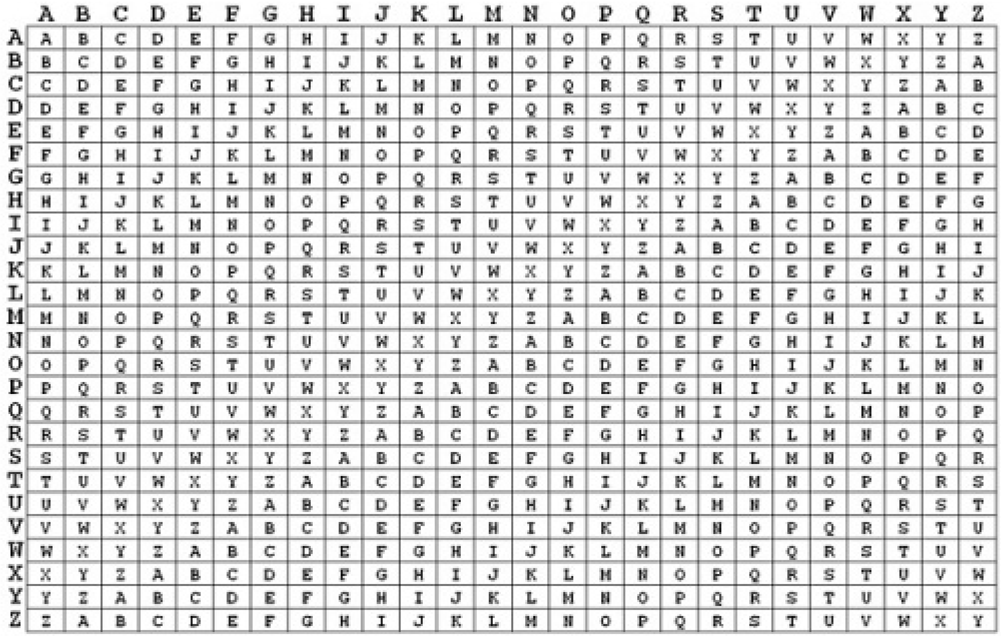
QLBGE NEMPE AFYLA EFENV KNQRL QVQ

4.2 How to Decrypt a Vigenere Cipher

To decrypt the ciphertext, pick a letter in the ciphertext and its corresponding letter in the keyword, use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter (MTU, 2020). For example, to decrypt the first letter “Q” in the ciphertext, we find the corresponding letter “M” in the keyword. Then, the row of “M” is used to find the corresponding letter “Q” and the column that contains “Q” provides the plaintext “E” (MTU, 2020).

4.3 Examples

Example 1: In deciphering the Vigenere ciphertext, we must perform the the steps in inverse or opposite functions to retrieve the plaintext. In other words, using the Vigenere table, find the row of the first letter of the keyword. Look along it to find the first letter of the ciphered text in that row. Now follow the column up to find the first letter of the encoded phrase at the top of the chart. Continue this pattern until you have completely deciphered the text (wikiHow, 2020).



	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

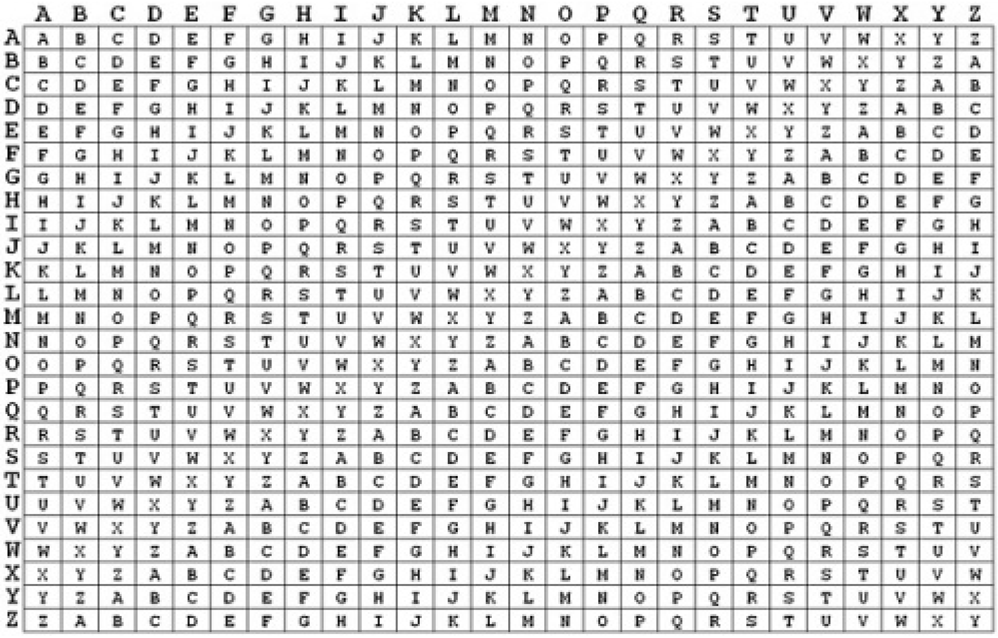
Figure 4: Vigenere Cipher 26x26 Table

The first thing you do is start with the "U." You find the "J" on the horizontal line and go across until you find the "U." Once you find the "U" you trace the letter up to find its vertical equivalent which in this case is the "L." Continue this pattern until you decode the message.

UWTNZ MESJJ IEQ

LIVEL OVELA UGH

Example 2:



	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 5: Vigenere Cipher 26x26 Table

The first thing you do is start with the "U." You find the "S" on the horizontal line and go across until you find the "U." Once you find the "U" you trace the letter up to find its vertical equivalent which in this case is the "C." Continue this pattern until you decode the message.

UIPHM VWFWG DVWWV MJQTW

CONFI DENCE BREED SHOPE

4.4 Cryptanalysis (How to Break the Code)

The Vigenere Cipher was thought to be unbreakable for over two hundred years. At first glance the Vigenere Cipher appeared to be unbreakable, due to its use of up to 26 different cipher alphabets (Chamber, 2000). Ciphers which use more than one alphabet to cipher are known as Polyalphabetic ciphers because it uses multiple substitution alphabets. These types of ciphers are extremely difficult to decode. Even though running-key or autokey ciphers eliminate periodicity, two methods exist to cryptanalyze them. The first one the cryptanalyst proceeds under the assumption that both the ciphertext and the key share the same frequency distribution of symbols and applies statistical analysis. The second is known as the probable-word method where words are thought most likely to occur in the text are subtracted from the cipher (Simmons, 1987). The important thing about this is the reoccurrence of the English language is high enough that the information conveyed by every ciphertext component is greater than the rate at which equivocation is introduced by the running-key (Simmons, 1987).

5 Conclusion

Upon reflection, the Caesar, Affine, and Vigenere Ciphers are all great ciphers to use to introduce students to the science of cryptography. This century has been titled, the digital century, with home banking, online transactions, secure telephone conversations, and online gaming among the many aspects that represent that the digital revolution is growing. Within all these classical ciphers the need to understand pattern recognition and algorithms is essential to encrypt and decrypt these “secret messages”. Students always say, “When will I ever use this math?” By introducing these ciphers, students are able to relate them to real life situations, thus capturing the student’s interest. These ciphers are used in entertainment with escape rooms and video games, in government agencies for sending and receiving messages with tools such as Morse Code for sending and receiving messages and surveillance tools that intercept messages and change the content. We were introduced to such a tool with our voting system where other countries were trying to change the outcome of the election. Cryptography knowledge is critical in this age, yet it has not become one of the school subjects. Instead, it is taught in both Mathematics and Computer Science classes. As the need increases for more security in our lives, cryptography will become indispensable.

The Caesar Cipher is very basic and the student should be able to encrypt and decrypt the code with ease requiring little computation and number sense. This is a great way to pull the students into the coding world. The students can use the shifting method to create base codes that are not difficult for encryption or decryption. The Affine Cipher is a bit more complex. It uses algebraic expressions to encrypt and decrypt the code. The Affine Cipher can be presented as an introduction to linear functions and systems. When presenting this code, students should notice its similarity to the slope formula which is y = mx +b. In the decryption of this code, this is where students will use their critical thinking to analyze the key to decipher the code.

In conclusion, cryptology is the process of hiding information which correlates to students finding the value of a variable or unknown. Reflecting on using ciphers in secondary education provides students an opportunity to discover key mathematical concepts and techniques that are fascinating and more likely to appreciate the beauty it possesses. Students are able to see how math applies in the real world.

References

[1] Arlington. (2006, December 24). William Frederick Friedman, Colonel US Army. Retrieved from http://www.arlingtoncemetery.net/wfried.htm

[2] Belfield, R. (2007). What Did Gabrieli di Lavinde Do with Cryptography? Retrieved from https://books.google.com/books

[3] Caley, E.R.(1926). The Leyden Papyrus X: An English Translation with Brief Notes. Retrieved from https://pubs.acs.org/doi/pdf/10.1021/ed003p1149

[4] Cryptography for a connected World. (n.d.). Retrieved from https://www.ibm.com/ibm/history/ibm100/us/en/icons/cryptography/

[5] Dooley, J. (2018, August). Crypto Goes to War: The American Civil War 1861 – 1865: Codes, Ciphers, and Their Algorithms. Retrieved from https://www.researchgate.net/publication/327195569_Crypto_Goes_to_War_The_American_Civil_War_1861-1865_Codes_Ciphers_and_Their_Algorithms

[6] Friedman, W.F. (n.d.). NSA/CSS. Retrieved from https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1623026/william-f-friedman/

[7] Google Scholars. (2009). Ronald L. Rivest. Retrieved from https://scholar.google.com/citations?user=6qEOtdAAAAAJ&hl=en

[8] Hern, A. (2014, November 14). How did the Enigma Machine Work? Retrieved from https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game

[9] Kahn, P. (n.d.). Cryptology Timeline. Retrieved from http://pi.math.cornell.edu/~morris/135/timeline.html

[10] Korolov, M., & Drinkwater, D. (2019, March 12). What is Quantum Cryptography? No Silver Bullet, But Could Improve Security. Retrieved from https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security html

[11] Lester, T. (2001, March). Open Secrets. Retrieved from https://www.theatlantic.com/magazine/archive/2001/03/open-secrets/376392

[12] Miles. (2019, October 2). Cryptography: The History and Mathematics of Codes and Code Breaking. Retrieved from https://derekbruff.org/blogs/fywscrypto/tag/world-war-i/

[13] National Museum. (2015, May 1). War of Secrets: Cryptology in World War 11. Retrieved from https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196193/war-of-secrets-cryptology-in-wwii/#:~:text=Cryptology

[14] Pawlan, M. (2005). Cryptography: The Ancient Art of Secret Messages. Retrieved from http://www.pawlan.com/monica/articles/crypto/

[15] Practical Cryptography. (n.d.). Caesar Cipher. Retrieved from http://practicalcryptography.com/ciphers/caesar-cipher/

[16] Practical Cryptography. (n.d.). Homophonic Substitution Cipher. Retrieved from http://practicalcryptography.com/ciphers/homophonic-substitution-cipher/

[17] Practical Cryptography. (n.d.). ROT 13 Cipher. Retrieved from http://practicalcryptograhy.com/ciphers/rot13-cipher/

[18] Robert Rivest. (2020, April 27). Retrieved from https://www.csail.mit.edu/person/ronald-rivest

[19] Rouse, M. (2014, August 19). What is Cryptography? – Definition. Retrieved from http://searchsecurity.techtarget.com/definition/cryptography

[20] Savarese,C. & Hart,B.(2010, April 25). Cryptography. Retrieved from http://www.cs.trincoll.edu/~crypto/historical/intro.html

[21] Security Tech. (n.d.). What is Cryptography? Definition. Retrieved from https://www.searchsecurity.techtarget.com/definition/cryptography

[22] Sidhpurwala, H. (2013, August 14). A Brief History of Cryptography. Retrieved from http://access.redhat.com/blogs/766093/posts/1976023

[23] Simmons, G.J. (n.d.). Cryptology. Retrieved from https://www.britannica.com/topic/cryptology/Developments-during-World-Wars-I-and-II

[24] Thomas Jefferson Encyclopedia. (n.d.). Retrieved from https://www.monticello.org/site/research-and-collections/wheel-cipher

[25] Waddell, K. (2016, January 13). The Long and Winding History of Encryption. Retrieved from https://www.theatlantic.com/technology/archive/2016/01/the-lone-and-winding-history-of-encryption/423726/

[26] Walker, J. (n.d.). Affine Ciphers. Retrieved from https://www.math.ust.hk/~yangwang/Course/2016FSMath4999

[27] Walker, S. (2017, July 12). The British Museum. Retrieved from https://blog.britishmuseum.org/everything-you-ever-wanted-to-know-about-the-rosetta-stone/

[28] Wikipedia. (n.d.). Cryptanalysis of the Enigma. Retrieved from https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma

[29] Zorpette, G. (1994, Summer). The Edison of Secret Codes. Retrieved from https://www.inventionandtech.com/content/edison-secret-codes-1

[30] Morelli, R. (n.d.). Vigenere Cipher. Computer Science - Computer Science. Retrieved from http://www.cs.trincoll.edu/~crypto/historical/vigenere.html

[31] Simmons, G. J. (n.d.). Vigenère cipher. Encyclopædia Britannica; Encyclopædia Britannica. Retrieved from https://www.britannica.com/topic/Vigenere-cipher

[32] The Black Chamber - Cracking the Vigenère Cipher. (n.d.). Simon Singh — Simonsingh.Net. Retrieved from https://www.simonsingh.net/The_Black_Chamber/vigenere_cracking.html

[33] The Vigenère Cipher Encryption and Decryption. (n.d.). Article - Managing Your Personal Web ... Retrieved from `https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html`

[34] Vigenère Cipher - GeeksforGeeks. (2016, October 7). GeeksforGeeks. Retrieved from `https://www.geeksforgeeks.org/vigenere-cipher/`

[35] wikiHow. (2006, June 14). 3 Ways to Encode and Decode Using the Vigènere Cipher - wikiHow. WikiHow; wikiHow.Retrieved from `https://www.wikihow.com/Encode-and-Decode-Using-the-Vig`