A Journey into Ancient Cryptography:
Greek, Roman, and Renaissance Ciphers and their Lasting Influence on Modern Cybersecurity

A Senior Thesis in Classics

Presented to

The Faculty of the Department of Classics

The Colorado College

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Arts

Magdalena Horowitz

May 2020

Introduction

Cybersecurity, a subdivision of computer science, is defined by the National Institute of Standards and Technology as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication..."[1] Cryptography, a subdivision of cybersecurity, is the art of creating and breaking the codes involved in the secure transmission of classified messages. Like cybersecurity, cryptography is associated with emerging technology such as computers and digital communication. Cryptographers are highly valued by top US government agencies such as the DOD, CIA, NSA, FBI, and DHS. They are also coveted internationally by agencies such as China's MSS, Russia's FSB, and Israel's Mossad. Cryptographers manipulate advanced algorithms, secure and transmit digital data, and monitor and neutralize malicious digital threats. Stanford University calls cryptography "an indispensable tool for protecting information in computer systems."[2]

It is hardly surprising, therefore, that the words "ancient" and "cryptography" are rarely used in the same context. However, not only did cryptography exist in ancient Greece and Rome, but the fundamental design and principles of ancient cryptographic devices such as the Spartan Skytale and the Caesar Cipher set the foundation for contemporary encryption algorithms. Accordingly, knowledge of these devices survived throughout Late Antiquity and the Middle Ages, reappearing during the Renaissance in new inventions such as the tabula recta, the Vigenère Cipher, and most importantly, the Alberti Cipher. These new ciphers not only evolved

[1] "cybersecurity, NIST: National Institute of Standards and Technology, https://csrc.nist.gov/
[2] SCPD: Stanford Center for Professional Development

from, but shared the same fundamental functionality, structure, and composition of the Skytale and Cesar Cipher.

This thesis will examine how these ciphers function, their classification into transposition or substitution subcategories, and what defines them as cryptographical devices. I will first analyze and contrast accounts by the classical authors Aulus Gellius and Aeneas Tacticus to show the difference between steganography, or simply concealed communications, and cryptography, or enciphered messages. Then, I will turn to the culmination of ancient cryptography, the Caesar Cipher, described by Gellius and Suetonius. I will then demonstrate Leon Battista Alberti's cipher, described by him in his Latin treatise *De Componendis Cyfris,* as a continuation of and improvement on the Caesar Cipher and determine why it, too, is considered a cryptographic device. Finally, I will discuss how these ciphers from Classical and Renaissance civilizations utilize modular arithmetic and anticipate symmetric public key encryption, two important features of contemporary cryptographic algorithms.

The Skytale and its Predecessors

In order to prove the existence of cryptography in the ancient world, one must first distinguish what is not classified as cryptography, but might be confused with it. Accordingly, in this section I will introduce several Greek technologies that facilitate secret communication, even if most were not actually cryptographic instruments. I will begin with such steganographic devices and then conclude with the Skytale, one of the most renowned ancient cryptographic inventions.

Steganography, or the art of concealing plain text, was a common practice during the transmission of messages in ancient Greece. It is derived from the Greek word στεγανός, meaning "cover," and γράφειν – "writing." The text itself remains unchanged, but various

methods are used to disguise the original message. The earliest records of simple steganography are described by Herodotus in *The Persian Wars,* where three passages document the existence of steganography as early as the 5th century BC. One such event depicts Harpagus, a Median general, sending a message inside the belly of a hare to Cyrus, detailing his secret plan for deposing Astyages, his king. Harpagus slices open the stomach of the animal, slips the paper in, and sews the hare back up.[3] Another occasion for secret communication is depicted in book V when Aristagoras, the leader of Miletus, is sent a message from Histiaeus, his father-in-law, advising him to revolt against Persia. According to Herodotus, the message was tatooed

> on the head of his trustiest slave, and [Histiaeus] waited till the hair grew again; as soon as it was grown, he sent the man to Miletus with no other message save that when he came to Miletus he must bid Aristagoras shave his hair and examine his head.[4]

Herodotus' final reference to concealed messaging, and perhaps the most notable instance, is when the Spartan king Demaratus disguises a common wax tablet with an underlying hidden message describing Xerxes' resolve to attack Hellas. Demaratus warns the Spartans, and Herodotus writes (Hdt 7.239):

> But he [Demaratus] feared to be detected, and had no other way of acquainting them than this trick: — taking a double tablet, he scraped away the wax from it, and then wrote the king's intent on the wood; which done, he melted the wax back again over the writing, so that the bearer of the tablet thus left blank might not be troubled by the way-wardens. When the tablet came to Lacedaemon, the Lacedaemonians could not guess its meaning, till at last (as I have been told) Gorgo, Cleomenes' daughter and Leonidas' wife, discovered the trick herself and advised them to scrape the wax away, when they would find writing on the wood. So doing, they found and read the message, and presently sent it to the rest of the Greeks. This is the story, as it is told.[5]

From this excerpt, it is evident that Demaratus does not obfuscate the letters themselves, as we will shortly see in the Skytale and Caesar Cipher, but instead hides the existence of the message.

---

[3] Hdt, 1.123.3-4, Trans. Godley
[4] Hdt, 5.35.3, Trans. Godley
[5] Hdt, 7.239, Trans. Godley

Aeneas Tacticus, the earliest and one of the most prominent of ancient military writers of the 4th century BC, confirms Herodotus' account of the wax tablet in *How to Survive Under Seige,* a treatise on the art of war. Aeneas matches Herodotus in depicting a scenario where molten wax is poured over a message etched into a wooden tablet.[6] Additionally, he describes the tablet as having "something else [written] on the wax" layer (31.14), as opposed to Herodotus' blank tablet. This significant detail provides an additional layer of security, further disguising the tablet.

As Herodotus precedes Aeneas by a century, one may be inclined to believe that the method used by Demaratus had developed further and the latter author is describing a separate but similar event. However, according to the commentary supplied by both David Whitehead and the Illinois Faculty Greek Club in their translations of Aeneas, this passage's subject is "universally agreed to be that of the crucial letter sent to the Spartans in 481 by their deposed king, Damaratos," confirming that both classical authors are describing the same event even if they disagree about a crucial detail. [7]

Additionally, during the second century AD, a third account is provided by Aulus Gellius, a Roman author and grammarian. He describes the concealed wax tablet technique being employed under different circumstances, but confirming Herodotus' version of the method (Gell. *NA* 17.9):

> *Legebamus id quoque in vetere historia rerum Poenicarum, virum indidem quempiam inlustrem—sive ille Hasdrubal sive quis alius est non retineo—epistulam scriptam super rebus arcanis hoc modo abscondisse: pugillaria nova, nondum etiam cera inlita, accepisse, litteras in lignum incidisse, postea tabulas, uti solitum est, cera conlevisse easque tabulas, tamquam non scriptas, cui facturum id prae-dixerat misisse; eum deinde ceram derasisse litteras-que incolumes ligno incisas legisse.*

[6] Aen.Tact., 31.14 Trans. Godley
[7] Aen.Tact., 31.14 Trans. Illinois Faculty Greek Club

> I also read this in an ancient history of Carthage, that a certain famous man of that country—whether it was Hasdrubal or another I do not remember – concealed a letter having been written about secret writings with this method: he took new writing tablets, with the the wax not yet applied, and cut the letters into the wood. Afterwards he covered the tablet with wax in the usual way and he sent them, as if there was no writing on them, to someone to whom he had told before that he would do this. The recipient then scraped off the wax, found the letters unharmed upon the wood, and read them.

Gellius adds a further detail that contradicts both previous accounts. Herodotus claims that the Lacedaemonians initially did not know the purpose of the tablet or that it concealed any message at all. Aeneas simply adds

> Then when it subsequently reached its destination the recipient scrapped off the wax, read the message, wrote a reply in the same way, and sent the tablet back again.[8] It is unclear from his account whether the recipient was aware that a secret message would be arriving.

It is only Gellius who specifies that "to one to whom he had previously told his plan."[9]

As *How to Survive Under Seige* highlights the best techniques to defend a fortified city, Aeneas Tacticus also describes several other forms of steganographic messaging. First, he mentions a boxwood tablet covered in whitewash. The recipient must simply wash the tablet to reveal the text. Another method is sending a book marked with tiny dots above certain letters. The recipient would piece together the marked letters to reveal the hidden message. The treatise also includes several sections describing inconspicuously located messages such as those hidden in the sole of one's shoe, etched into the inner lining of a silver earring, and tattooed onto the shaved head of a slave, similar to Histiaeus in Herodotus.[10]

Finally, Aeneas describes a more complex form a secret messaging, the twenty-four-holed disk called an "astragal." According to him, it is "the most secret and most troublesome

[8] Aen.Tact., 31.14 Trans. Godley
[9] Gell, *Attic Nights,* 17.9
[10] Aen.Tact., 31Trans. Godley

method of all" because no actual writing is involved.[11] This device works by threading a cord through the holes, each of which represents a letter of the alphabet. The resulting ball of thread must be unraveled by the recipient and deciphered in reverse order, from the end of the string to the beginning. This method is certainly more secret, yet it is also tedious. Thus, it was used for short phrases or at most a sentence. Since the astragal involves no written text and is more complex than previously mentioned concealed communications, it is often misclassified as an encryption device. However, it is still simply a form of "secret" communication. What one does not know are the physical steps to reveal the message. It must simply be disassembled. Once unwound, the plaintext message is apparent without the need for further decryption.

While steganography continued to develop in complexity throughout ancient Greece and is still employed today in various digital forms, it still falls short of cryptography. Regardless of how thoroughly the message is concealed, anyone can comprehend its meaning once found. Cryptography, unlike steganography, alters the content of a message rather than camouflaging its existence.[12] Discovering the text has no impact on secrecy, for only deciphering the code using a specific key will reveal its meaning. Cryptography is thus both more secure and more complex.

There are two main cipher techniques: transposition and substitution. Transposition jumbles the letters of the original message, the "plaintext." A simple example of transposition is a word scramble: converting the word "Greek" to "kereg." The alphabet remains fixed and the identity of each symbol survives, but the position is lost. Historically, one of the most famous, and earliest, devices classified as a transposition cipher is the Spartan Skytale. Both Aulus Gellius and Plutarch provide firsthand accounts of how the Skytale works. Plutarch, in

[11] Aen.Tact., 31.16 Trans. Godley
[12] Singh, *The Code Book,* Loc 227/5939 *(Digital Edition)*

Lysander[13], describes a dispatch scroll sent by the Lacedaemonian ephors ordering Lysander home. First, he specifies who will be using the Skytale:

> The dispatch-scroll is of the following character. When the ephors send out an admiral or a general, they make two round pieces of wood exactly alike in length and thickness, so that each corresponds to the other in its dimensions, and keep one themselves, while they give the other to their envoy.

Then he gives a detailed account of the physical traits of the apparatus:

> These pieces of wood they call "scytalae." Whenever, then, they wish to send some secret and important message, they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their "scytale" leaving no vacant space thereon, but covering its surface all round with the parchment."

Finally, he describes the encryption technique:

> After doing this, they write what they wish on the parchment, just as it lies wrapped about the "scytale"; and when they have written their message, they take the parchment off, and send it, without the piece of wood, to the commander. He, when he has received it, cannot otherwise get any meaning out of it,—since the letters have no connection, but are disarranged,—unless he takes his own "scytale" and winds the strip of parchment about it, so that, when its spiral course is restored perfectly, and that which follows is joined to that which precedes, he reads around the staff, and so discovers the continuity of the message. And the parchment, like the staff, is called "scytale," as the thing measured bears the name of the measure.[14]

Plutarch claims that the material wrapped around the round pieces of wood is a scroll of parchment. Aulus Gellius, however, challenges this statement in his own account of the skytale. He begins by describing the purpose of these secret letters and then gives a detailed description of the device itself. This first section confirms Plutarch's version: (Gell. *AN* 17.9):

> *Lacedaemonii autem veteres, cum dissimulare et occultare litteras publice ad imperatores suos missas volebant, ne, si ab hostibus eae captae forent, consilia sua noscerentur, epistulas id genus factas mittebant. Surculi duo erant teretes, oblonguli, pari crassamento eiusdemque longitudinis, derasi atque ornati consimiliter; unus imperatori in bellum proficiscenti dabatur, alterum domi magistratus cum iure atque cum signo habebant. Quando usus venerat litterarum secretiorum, circum eum surculum*

[13] Plt, Lysander 19.5, Trans. Perrin
[14] Plt, Lysander 19.6, Trans. Perrin

> *lorum modicae tenuitatis, longum autem quantum rei satis erat, conplicabant, volumine rotundo et simplici, ita uti orae adiunctae undique et cohaerentes lori, quod plicabatur, coirent.*
>
> But the ancient Lacedaemonians, when they wished to disguise and conceal the letters sent publicly to their generals, so that, if they were to have been captured by the enemy, their plans might not be found out, used to send letters written in this mode. There were two smooth shoots, oblong, with equal thickness and of the same length, having been smoothed and furnished very similarly. One of these was given to the general departing into to war, the other the magistrates were holding at home under their control and seal. When the need of more secret letters arose, they wound about the stick a leather strap of moderate thickness, but long enough for the purpose, with a circular and simple fold, so that the edges of the leather strap joined completely and were held together.

However, he then proceeds to add further details that aren't included in Plutarch's depiction of the Skytale:

> *Litteras deinde in eo loro per transversas iuncturarum oras versibus a summo ad imum proficiscentibus inscribebant; id lorum litteris ita perscriptis revolutum ex surculo imperatori commenti istius conscio mittebant; resolutio autem lori litteras truncas atque mutilas reddebat membraque earum et apices in partis diversissimas spargebat; propterea, si id lorum in manus hostium inciderat, nihil quicquam coniectari ex eo scripto quibat; sed ubi ille ad quem erat missum acceperat, surculo conpari, quem habebat, a capite ad finem, proinde ut debere fieri sciebat, circumplicabat, atque ita litterae per eundem ambitum surculi coalescentes rursum coibant integramque et incorruptam epistulam et facilem legi praestabant. Hoc genus epistulae Lacedaemonii σκυτάλην appellant.*
>
> Then they wrote the dispatch on that thong across the connected edges of the joints, with the lines running from the top to the bottom. With the letter having been written in this way, the leather strap was unrolled from the wand and sent to the general, who was aware of the device. But the unravelling of the leather strap yielded letters that were cut short and maimed and it [the unravelling] was scattering into the most distant parts the elements and outlines of the letters. Therefore, if the leather strap had fallen into the hands of the enemy, nothing at all could be interpreted from the writing; but when the one to whom the letter was sent had accepted it, with the matching stick, which he was holding, he wound around from the head to the end just as he knew that it should be done and thus the letters, united by encircling a similar staff, came together again, rendering the dispatch entire and uncorrupted, they were easy to read. The Lacedaemonians called this method of letter the Skytale.

Comparing the two accounts, it is important to note the similarities and differences. Plutarch and Gellius both claim that the two devices on each end of the message are of equal thickness and length. This is a critical detail that defines the cryptographic element of the Skytale. If the wands are not exactly the same size and width, the message will be incoherent. The wand itself acts as a decryption key, the primary element necessary for a device to be considered cryptographic and not simply steganographic. However, Gellius, unlike Plutarch, adds that once unraveled, the leather strap itself no longer yields complete characters. The letters themselves are incomplete. Gellius is attempting to convey that because the sender writes across the cracks in the leather, once unrolled, even single letters would be disfigured and broken adding a further layer of encryption to the message.

These discrepancies are significant because they determine the complexity of the device. If one agrees, as Gellius claims, that writing was indeed positioned over the joints (locations where the paper was separated), it is likely that the Greeks recognized the limits of a transposition cipher and sought to further complicate the encryption technique. Once the leather strap was unrolled, the letters would be disfigured in addition to being out of order, rendering the message entirely unintelligible; no further concealment would be necessary. Without this additional feature, the Skytale seems too simplistic. However, it is also possible, if one accepts Plutarch's version, that the Skytale may have been combined with further concealment, such as the steganographic methods that have been discussed, or additional encryption techniques, like substitution – to which I will now turn.

The Caesar Cipher

The culmination of ancient cryptography was the Caesar Cipher. In almost every modern article and history on cryptography, the Caesar Cipher is mentioned as one of the earliest and most influential ciphers. In *Serious Cryptography: A Practical Introduction to Modern Encryption,* the Caesar Cipher is called the most famous of all classical ciphers[15]. Twenty-first century mathematicians Dennis Luciano and Gordon Prichett highlight the cipher as "one of the earliest known cryptographic systems" in an article published by the Mathematical Association of America.[16] Joshua Holden, author of *The Mathematics of Secrets,* calls Julius Caesar, the "creator" of the cipher, not only a "*dictator perpetuus* of Rome, [but] also a military genius, a writer, and a cryptographer." In the article "Historical Ciphers and Ancient Languages," Sarah Spence Adams claims it is one of 'the first documented attempts at scrambling or encrypting military communications'[17] Finally, *Number Theory,* an advanced mathematics textbook on the existence, function, and theory of numbers, devotes an entire section to the cipher, entitled "From the Caesar Cipher to Public Key Cryptography[18]."

While the Caesar Cipher, initially used by Julius Caesar in his secret correspondence with Cicero[19], may not have been the very first ancient cryptographic device, it is certainly the most prominent of the classical era based on existing ancient and contemporary sources. [20]It differs

---

[15] Aumasson, *Serious Cryptography,* 28
[16] Luciano, Prichett *From Caesar Ciphers to Public-Key Cryptosystems* , 4-7
[17] Adams, *Historical Ciphers and Ancient Languages*, 5-7
[18] Burton, *Elementary Number Theory,* 197
[19] Textual evidence from Caesar himself in *De Bello Gallico* ,Suetonius' *Divus Julius,* and Aulus Gellius' *Attic Nights* show Julius Caesar's correspondence between both Marcus and Quintus Tullius Cicero, among others.
[20] Simon Singh claims in *The Code Book* that the Kāmā-Sūtra, a text written in the 4th century A.D. by Brahmin scholar Vātsyāyana was "one of the earliest descriptions"[20] of the substitution technique. However, there is some dispute on the date of the text, as it falls between 400 BC and AD 300. Singh claims that the Kāmā-Sūtra devotes an entire section to the "art of secret writing, advocated in order to help women conceal the details of their liasons." However, it is unclear whether this form of writing was ever implemented. Singh proceeds to clarify that the The Caesar Cipher was the first ancient cipher that was actually used.

from the previous cipher we have discussed, the Skytale, because it uses substitution, not transposition.

The substitution enciphering technique modifies the original letters. They are replaced with other symbols, numbers, or letters. For example, the message "Caesar" transforms into either "Dbftbs" or "13 10 4 3 10 6." Letters from the same alphabet can be used, or an entirely new system of symbols or codes can be implemented. Notice that the two a's in "Caesar" are substituted with the same replacements, either b's in the alphabetical replacement or 10's in the numerical version. The positions are kept, but the original alphabet and value are disguised.

While it is unanimously agreed that the Caesar Cipher is a fundamental and exemplary substitution cipher, there remains some confusion surrounding the first true appearance of the cipher and how it was used. Simon Singh, a prominent British author and mathematician, claims that the first documented use of a substitution cipher, specifically for military purposes, appears in Julius Caesar's *De Bello Gallico*. In book 5.48, Caesar, in battle, moves into the territory of the Nervii and learns about the crisis at Cicero's[21] camp. Caesar writes:

> *Ibi ex captivis cognoscit, quae apud Ciceronem gerantur, quantoque in periculo res sit. Tum cuidam ex equitibus Gallis magnis praemiis persuadet uti ad Ciceronem epistolam deferat. Hanc Graecis conscriptam litteris mittit, ne intercepta epistola nostra ab hostibus consilia cognoscantur. Si adire non possit, monet ut tragulam cum epistola ad amentum deligata intra munitionem castrorum abiciat.*
>
> There he learned from the prisoners what was taking place at the home in Cicero's area and in how much danger his situation was. He persuaded a certain one of the Gallic horsemen with great recompense to deliver a letter to Cicero. He sent this letter with Greek characters, in order that if the letter were intercepted by the enemy, our plans would not be figured out. If (he) could not approach, he [the messenger] was advised to throw a spear, with the letter attached to the thong, inside the entrenchment of the camp.

[21] Here however, the Cicero mentioned is Quintus Tullius Cicero (and not Marcus Tullius Cicero) who served as a *legatus* under Caesar.

Singh translates this passage similarly with no additional detail, confirming that there is no evidence that the message itself was encrypted. Therefore, we cannot use *De Bello Gallico* as a source to illustrate the first use of the Caesar Cipher. Oddly enough, David Kahn, another contemporary author on cryptography, makes a similar claim. He says, "These Greek authors never said whether any of the substitution ciphers they described were actually used, and so the first attested use of that genre in military affairs come from the Romans—and from the greatest Roman of them all, in fact. Caesar tells the story himself in his Gallic Wars" before proceeding to recount the same passage from *De Bello Gallico* that Singh uses.[22]

While disguising the letter in Greek characters indicates some method of concealment, Caesar still does not directly specify that he is writing in cipher. However, both Singh and Kahn are correct that there exists a correspondence between Cicero and Julius Caesar. It is not until we examine further texts from the classical authors Suetonius and Gellius that we can fully confirm the existence of Caesar's enciphered messages.

Gaius Suetonius Tranquillus, a Roman historian of the first century AD, is known for *de vita Caesarum,* his most important surviving work. Suetonius provides biographies on twelve Roman rulers from Julius Caesar to Domitian. In *Divus Julius,* he describes Caesar's correspondence with Cicero[23], specifically in cipher text (Suet. *DivJul.* 56.6):

> *Extant et ad Ciceronem, item ad familiars domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scriptsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.*

---

[22] Kahn, *The Codebreakers,* 83.

[23] Although Caesar was previously mentioned writing to Quintus Tullius Cicero, here Suetonius is talking about Marcus Tullius Cicero, the older brother. Two such sources supporting that Suetonius' Cicero is the older brother, Marcus are Alan G. Konheim in *Computer Security and Cryptography* Chapter 3.2 and Adolph, F. Pauli in "Letters of Caesar and Cicero to Each Other" (128)

> [The letters] to Cicero exist, as do letters to family and intimate friends about personal affairs, in which, if anything had to be conveyed more secretly, he wrote in ciphers[24], in such a way that the order of the letters were jumbled so that no word could be made out; which things, if anyone may wish to investigate and understand them, might change the fourth letters of the alphabet, for example D instead of A and [change] the remaining letters in the same way.

From this passage, the reader obtains a clear description of how the substitution technique works. Caesar replaces *quartum elementorum litteram*, or the fourth letter for the first. Every letter in message is accordingly shifted three places over to the right. For example, "battle beginning" would become "edxxoh ehjlqqlqj."

In *Divus Augustus,* Suetonius again mentions the Caesar Cipher, but this time it is Augustus who is writing in ciphers, and uses a variation on the original method. Suetonius notes that *quotiens autem per notas scribit, B pro A, C pro B ac deinceps eadem ratione sequentis letteras ponit; pro X autem duplex A.* ("however as often as he writes in cipher, he puts B for A, C for B and successively with the same method used for the following letters; for X, however, a double A" Suet. *DivAug* 88). Here we see a simpler, but similar cipher. Instead of shifting the positions of the letters three places over in the alphabet, Augustus moves the letters over by one. For X, since it is at the end of the alphabet, the cipher loops back to the beginning of the alphabet and the letter is replaced with an A.

Suetonius' accounts may initially appear to be straightforward, but upon further analysis, we can deduce further hidden implications in the text. Suetonius is specific in using the plural with *epistulae* ("multiple letters") and not *epistula*, and writes *extant ad Ciceronem* ("they exist") instead of *extat* ("it exists") which indicates that Julius Caesar consistently used encryption in

[24] *Per notas* can be translated "in ciphers", rather than its literal meaning "through letters" or "through writing/words" refer to *Oxford Classical Dictionary*

his communication. Additionally, in *Divus Augustus,* Suetonius writes "as often as he writes in cipher," implying that Augustus has also used this technique on multiple occasions.

Suetonius is not the only author who describes Caesar's cipher method. Aulus Gellius devotes an entire section to the cipher in *Attic Nights* 17.9:

> *Libri sunt epistularum C. Caesaris ad C. Oppium et Balbum Cornelium, qui rebus eius absentis curabant. In his epistulis quibusdam in locis inveniuntur litterae singulariae sine coagmentis syllabarum, quas tu putes positas incondite; nam verba ex his litteris confici nulla possunt. Erat autem conventum inter eos clandestinum de commutando situ litterarum, ut in scripto quidem alia aliae locum et nomen teneret, sed in legendo locus cuique suus et potestas restitueretur; quaenam vero littera pro qua scriberetur, ante is, sicuti dixi, conplacebat qui hane scribendi latebram parabant.*
>
> There are Gaius Caesar's books of letters to Gaius Oppius and Cornelius Balbus, who were taking care of his things while he was absent. In certain parts of these letters, individual letters are found which are not connected to form syllables, which you may believe to have been placed randomly; for no word can be made out from these letters. But there was a secret agreement made between [the correspondents] about the replacement of the position of the letters such that, in writing, one letter would hold the name and place of another letter, but in reading, each one's own position and meaning could be restored to it. But indeed, as for what letter was written for which, as I have said, it was agreed by them beforehand, who were preparing the secret of the writing.

Notice that Gellius also uses the plurals *libri sunt, epistulis,* and *parabant.* Gellius goes on to mention in the same passage e*st adeo probi grammatici commentarius satis curiose factus De Occulta Litterarum Significatione in Epistularum C. Caesaris Scriptura.* (*"*There is, indeed, a treatise of the Grammaticus Probus, having been assembled very carefully: 'On the hidden meaning of letters in the writing of the epistles of Gaius Caesar'*"*AulGel. *Attic Nights* 17.9) Gellius takes special care to emphasize the quality of the work by Probius. It is unlikely that Valerius Probus, a well-known grammarian and commentator on significant Latin texts, would have devoted an entire treatise on Caesar's encrypted letters if the secret method had not been well known in ancient Rome.

Both Suetonius' and Gellius' testimonies reveal that Caesar commonly wrote in cipher, especially to Cicero. Their accounts provide support that Caesar's letter to Quintus Cicero while approaching the Nervii most likely used the very same encryption technique described by Suetonius and Gellius: the Caesar Cipher. This is why Simon Singh and David Kahn claim that the earliest record of the cipher appears first in book V of *De Bello Gallico.*

The Caesar Cipher described by Suetonius, Gellius, and Caesar himself was not only extant in ancient times, but is classified today as a linear cipher that uses a fundamental mathematical division technique called modular arithmetic. As I will discuss later, modular arithmetic is present not only in the formula of the Caesar Cipher, but also in such leading contemporary cryptographic algorithms as the Diffie-Helman Public Key Exchange Protocol (1976) , RSA Encryption(1977), and the New Modified Caesar Cipher (2015).

The Alberti Cipher

Before moving on to modern cryptography, I will describe one final cipher. It is a device that builds upon the foundation of the Caesar Cipher and sets the stage for modern cryptographic algorithms. Known as the Alberti Cipher, this apparatus was designed by a true renaissance man, Leon Battista Alberti: a humanist author, architect, poet, priest, linguist, philosopher, polymath, and cryptographer. It first appeared in 1467 during the Italian Renaissance. Alberti was inspired by his friend Leonardo Dati, a pontifical secretary, who told him that he couldn't decode important messages regarding political affairs without the help of an interpreter.[25] Dati added *nam interdum ab exploratoribus intercepta deferuntur ad nos artibus scripta istius modi, quae*

[25] Alberti, *De Componendis Cyfris,* 2.4

nequaquam negligenda putemus ("such messages are sometimes intercepted by spies and there arrive coded messages that should not be overlooked" *DeCyfr.* 2.4). This sentence establishes that Dati was not satisfied with the clarity and security of the current cipher system, leading Alberti to implement his own solution.

Alberti decided to create a new method of encryption, pompously claiming that none before was as great. He even composed an entire treatise on the matter, entitled "*De Componendis Cyfris.*" Alberti there writes, with confidence, *postremo producam a nobis inventam cyfram quam cum intellexeris admirabere, congratulabere* ("Finally, I will produce a cipher invented by me, which, when you have understood [it], you will admire/wonder at [and] congratulate [me for]." *Alberti, 3.30*). The word *inventam* clearly shows that Alberti is claiming his device as novel.

Despite Alberti's claims to originality, his cipher resembles the Caesar Cipher in that it, too, is a substitution cipher and therefore shares the same foundational methods of encryption. Both devices involve two alphabets: the plaintext and the ciphertext. The ciphertext alphabet is the collection of symbols and letters displayed in the final transmitted message while the plaintext consists of the original letters that reveal the meaning of the text. In both inventions, to encrypt the message, the writer must sequentially replace each plaintext character contained in the original message with its corresponding cipher character. To decrypt the message, the recipient must reverse this process. Finally, and perhaps most importantly, both the Caesar Cipher and the Alberti Cipher require the sender and recipient to have agreed upon a secret key. This key, or "index" as Alberti calls it, is the crux.

While the Alberti Cipher shares the same basic design principles as the Caesar Cipher, it surpasses its predecessor in complexity and security. As we have discussed, the Caesar Cipher

follows a simple technique of replacing every first letter with a letter three places further along in the alphabet: *a* becomes *d, e* becomes *h,* and so on. This type of substitution cipher is further classified as monoalphabetic. The prefix "mono" most commonly means "singular" or "one" and thus corresponds with a cipher that has only one alphabet. In the Caesar Cipher, each letter from plaintext message maps to only one option in ciphertext. Without exception, an *a* becomes a *d,* and an *e* becomes an *h*. One could make a simple table aligning the plaintext alphabet to its ciphertext equivalent. This technique leaves the message subject to common interception techniques such as a "brute force attack" or "frequency analysis."

A brute force attack is when the adversary attempts to crack the code by trying every possible combination of letters. As the classical Latin alphabet consisted of twenty-three letters[26], a brute force attack on the Caesar Cipher would only take twenty-three shifts to discover the original message. In ancient times, decoding a message, especially a long message, may have taken hours. Most likely, by the time the message was discovered it would be too late to do anything about it. Today, in the digital age, a twenty-three-step brute force attack would take under a second.

The second interception technique, frequency analysis, is extremely effective on monoalphabetic ciphers. During frequency analysis, the adversary gathers information specific to the language used in a cipher. In Latin, the most common letters are "a", "e", and "i" at 8.90, 11.38, and 11.44 percent, respectively.[27] Therefore, in a triple shift Caesar Cipher message, the three most commonly found letters in the decoded message will now be "d", "h", and "l". By methodically parsing through the text, letter by letter, the most common ciphertext letters will

[26] Encyclopedia Britannica
[27] Stefan Trost , *Alphabet and Character Frequency: Latin*

become apparent and the adversary will slowly be able to substitute back the original letters. Eventually, he may even use word frequencies and patterns found in common vowel combinations. Especially in conjunction with a brute force attack, frequency analysis renders a monoalphabetic cipher such as the Caesar Cipher almost ineffective.

The Alberti cipher, on the other hand, is a polyalphabetic cipher. It is the first of its kind and is able to resist both brute force and frequency analysis attacks. The prefix "poly" means "many," "more than one," or "much," suggesting that a plaintext letter can have multiple corresponding ciphertext characters. For example, an *a* in plaintext can be encrypted as a *d* at some point, a *g* at another point, or even an *&* symbol. The rules governing the correct replacement are contained in the previously mentioned key. Not only is Alberti's device the first polyalphabetic cipher, but it also implements an additional layer of security: a codebook.

This is precisely why David Kahn, author of *The Codebreakers,* calls Alberti's achievement "critical in the history of cryptology." Kahn credits Alberti with "three remarkable firsts – the earliest Western exposition of cryptanalysis, the invention of polyalphabetic substitution, and the invention of ciphered code – [making] him the Father of Western Cryptology."[28] To an observer, these three "firsts" may seem surprisingly similar if not indistinguishable. However, there are several important differences between the three achievements which I will clarify. But first, I must explain how the Alberti cipher works.

Alberti's cipher consists of two concentric disks. The larger outer disk is called the *stabilis* or "non-moving or stable" disk, and the smaller central disk is called the *mobilis* or "movable" disk. The two disks are connected by a common pin through their centers that makes

[28] Kahn, 129

them a cohesive unit that moves and operates as one. This apparatus is also known as the *Formula.* The stabilis contains 24 cells with the uppercase set of letters from Latin in alphabetical order – not including “j”, “u”, and “w” as expected from today’s version of this alphabet, but also without the letters “h”, “k”, and “y.” Alberti believed that these last three letters were not needed and instead choose to insert four numbers, one through four, into the last cells of the outer ring. The smaller mobilis also has 24 cells, each of which corresponds to one of the stabilis’ cells. These compartments contain the complete lowercase Latin alphabet and the “&” symbol in a random arrangement.

> Both the sender and recipient shall have identical apparatuses. Alberti says (*DeCyf. 13)*:
>
> *Et formulam hanc geminatam habere oportet, ut sit earum altera apud te, altera vero apud amicum in provinciam ad quem tu scripturus sis, eruntque ambae forumulae isthaec penitus similes positionibus litterarum et numero earum et ordine ita ut in nullo discrepent.*
>
> It is fitting to have a two matching formulas: in order that one of them rests with you and the other one however [exists] with your friend in the country to whom you will write, and both of the formulas will be alike in their terms of the position, number, and order of the letters such that they disagree in no way.

If the devices are dissimilar in any way, the message cannot be decoded. The sender and receiver are aware of the secret index – i.e. the key – determining where the decryption should begin. The index is identified in the inner, or ciphertext disk, and is aligned with the letter indicated in the ciphered message, usually by a capital letter. After the starting point is identified, the recipient can follow the device and correctly substitute the corresponding plaintext letters with their matching cells on the cipher disk. The physical disk acts as a dictionary, and the user must simply look up the values that align with the key: the enciphered letter. However, what is unique about the Alberti cipher is its constantly changing key. Alberti writes (*DeCyf. 14):*

> *Cum autem tres quottuorve dictiones exscripsero mutabo nostra in formula situm indicis versione circuli, ut sit index ipse k fortassis sub R. Ergo in epistola inscribam maiusculam R inde igitur k significabit non amplius B sed R et quae sequentur singulae superiorum stabilum novissima suscipient significata.*
>
> However, after I will write three or four words, I shall shift the position of the index in our formula by a turn of the circle, so that index 'k' itself may be perhaps under 'R'. Therefore in the letter I will write a capital 'R' , from this place on 'k' will accordingly signify no longer 'b', but 'r' and those that will follow [based on the pattern you build from the letters above][29] and each one of the letters which follow will receive new meanings.

The critical statement here is that "each one of the letters which follow will receive new meanings." By repositioning the disks[30], the plaintext letters will now have entirely new ciphertext equivalents. For example, if the letter on the outer disk is "R" and the inner disk is "k", "S" may correspond to an inner disk reading of "m", "T" to "p" and, "U" to "i." Therefore, the unencrypted message "RUST" would read "kmpi" in encrypted text. However, let us imagine that we rotate the inner disk clockwise two space after writing two letters. Now, the capital "T" aligns with the lowercase "k" and the encrypted text is "kmkm." Without knowing how much to rotate the disk, the recipient would be unable to deduce anything from the ciphertext, let alone begin to recognize any frequency analysis patterns.

The detail provided in this excerpt supports Kahn's first claim that Alberti has demonstrated "the earliest Western exposition of cryptanalysis." Alberti has created a complex substitution cipher; not only does it encrypt, but it is unique in providing multiple ways to encrypt the same word, therefore ensuring the utmost secrecy. In his treatise, Alberti spends ample time simply describing the theory of cryptanalysis. In section X, he states (Alberti. *DeCifris 10.5):*

---

[29] *Superiorum stabilium* - each of the letters of the one's mentioned above become discernible (based on the pattern you build)

[30] See Appendix 1.3 for a diagram of the Alberti cipher.

> *sed prius quod ad universas cyfras offuscatiores dandas faciat, iuvet paulo apertius explicasse. Namque currandum quidem es tut vocalium atque item consonantium quae frequentiores scribendo veniant characteres nobis suppeditent plures atque dissimiles*
>
> But first, it will help a little bit to explain slightly more clearly that which we need to do in the creation of universally obscure ciphers. For care must certainly be taken so that the characters of the vowels and likewise of the consonants that appear rather frequently in the writing should supply to us more and different characters.

This sentence indicates that Alberti has taken frequency analysis into consideration, as he specifically highlights some consonants and vowels that "appear rather frequently" and proposes a solution. He suggests that "more and different characters" be used, meaning that one should shuffle the corresponding characters of the cipher disk so that the common letters consistently have different representations in the cipher text. This technique will prevent an adversary from decrypting the message.

Kahn's second claim, that Alberti has invented the first polyalphabetic substitution, is self-evident.

Finally, I will consider Kahn's third assertion, that Alberti is the first to incorporate "ciphered code – [making] him the Father of Western Cryptology." "Ciphered code" seems at first to be simply text that is encrypted by substitution, a method we have covered extensively. However, code is entirely different from ciphertext. A code in this case is a number. While it is similar to a key, instead of dictating where to begin in the cipher disk, it leads to a set of instructions. Along with the physical apparatus called the Formula, Alberti provided a book of codes consisting of 336 code groups. For example, a "112" code could mean: every time you decrypt a 1 in plaintext, shift the inner disk clockwise by three spaces, but if you see a two, shift the disk counterclockwise two spaces. Alberti documents these codes and pattern shifts in a table. As he states in *DeCyfris 16.8:*

> *Scripturus ergo ad te quam instituerim orantionem eam ex tabula disquiro qua inventa sub litterum titulo cui supposita est, specto ex fine numeros annotatos. Hos ea re ipse ex formula cyfrae nostris litteris illic eos numeros significantibus pono in epistola.*
>
> Therefore, I am about to write to you, I first investigate the phrase which I want to use from the table, and having found it under the corresponding label, which it was placed under, I look at the numbers from the end having been noted. And with our encrypted *formula*, I put the letters that signify those numbers into the letter.

The variance and combination of codes, ciphertext, and randomness in Alberti's cipher are what perhaps make it the apex of pre-modern cryptography and, as Kahn claims, "critical in the history of cryptology."

The Alberti cipher is no longer used to communicate, but its lasting influence remains apparent in today's cryptographic algorithms. As the first polyalphabetic cipher, it catalyzed the advancement of cryptography and the development of an unbreakable system.

Modern Encryption: Diffie-Hellman Key Exchange and RSA

"The basic framework of performing cryptography has remained more or less the same, of course, with a lot of improvements in the actual implementation," stated Benni Purnama and Hety Rohayani at the 2015 International Conference on Computer Science and Computational Intelligence.[31] In this spirit, I claim that modern encryption shares surprising similarities not only with past practice, but specifically with the previous ciphers mentioned. In this regard, I will refer to two techniques essential to contemporary cryptographic methods: Diffie-Helman Public

[31] Purnama and Rohayani, "A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From a Message To Be Encrypted", 196

Key Exchange and RSA encryption. Both involve public key encryption and modular arithmetic, two methods that first appeared in the Caesar and Alberti ciphers.[32]

The purpose of the Diffie-Helman Key Exchange (DHKE) is to allow two correspondents, let's say Cicero and Caesar, to securely share a secret message. In order to send the message, they must agree upon a secret number, called a "key." Let Brutus be the adversary attempting to intercept the message. Prior to the invention of this technique, if Brutus were to obtain the key, he would be able to decode the entire letter. With the DHKE, however, Cicero and Caesar can pass the key right under Brutus' nose, hence the title "public" key encryption. Due to modular arithmetic[33] and the laws of prime numbers, Brutus will be unable to understand what is being sent.

Generally, this is how the exchange works: Cicero and Caesar agree, publicly, on two positive integers: a single prime number *p*, and a generator *g*. A generator, in cryptography, has a complex definition, but for this purpose all one must know is that g remains constant[34] and is a fixed number. Cicero selects a private random number *n* and calculates the formula: $g^n \pmod p$ Let *x* be the result of this calculation. Caesar then sends *x* to Caesar. Next, Caesar selects his own random secret number *m* – not even Cicero knows what this is – and calculates the same formula, but with an *m* in the place of Caesar's *n*. Let *y* be the result of Caesar's calculation. Now Caesar sends *y* publicly to Cicero. The trick of the Diffie-Helman Key Exchange is that Cicero takes

[32] *Modular arithmetic* is a cyclical system where numbers are recycled and replaced within a set range. Often, it is referred to as "clock arithmetic." Take a number, raise it to some exponent, and divide by the "modulus" (some number) and output the remainder. The remainder of the division is the number that will always be used. Public key encryption will be explained shortly as part of the Diffie-Hellman Key Exchange.

[33] See Appendix 1.1 for an explanation of modular arithmetic

[34] A *constant* is a number in mathematics that stays the same throughout calculations. It is unlike a *variable* that may change depending on subsequent manipulation.

Caesar's public result, the *y* that everyone can see, and raises this number to the power of his private number, *n* – which is a number that no one but he himself can see – and calculates the value. Caesar does the same, except he raises *x* to his own private number, *m*. Both correspondents thereby obtain the same shared secret key value, since by the laws of mathematics, they are performing the same calculation with the exponents in a different order.[35] However, from the public eye, it is impossible to decrypt. Without one of the private numbers, Brutus, the adversary, will not be able to find the solution.

In an example provided in my appendix, I have, for simplicity, employed small numbers. In modern cryptography, however, with large enough numbers, the code is almost cryptographically impossible to break. Even for modern supercomputers, attempting a brute force attack (in this case, one in which you attempt to compute the secret by testing all potential secret numbers *m* and *n*) would be computationally expensive; an infeasible allotment of time and resources, about one year and a 100 million dollars, would be required to decrypt the key.[36] With a time-sensitive message, this is impractical and almost useless.

Another modern cryptosystem, RSA, was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology. This method uses asymmetric public-key cryptography, or two-key cryptography. One of the keys can be viewed by everyone while the other remains secret. The mathematics of RSA are complex, involving public and private keys, generating large random prime numbers, and power multiplication. The critical feature of RSA (the technical details do not matter) is that it uses modular arithmetic in

[35] See Appendix 1.2 for an illustrated step-by-step example
[36] Ars Technica , https://arstechnica.com/information-technology/2015/11/op-ed-how-did-they-break-diffie-hellman/

its key exchange, allowing both parties to obtain the same result, as with the Diffie-Hellman Key Exchange.

As one may recall, modular arithmetic is a primary technique also implemented in the Caesar Cipher.[37] Caesar uses the triple shift in his substitution cipher, where letters are replaced by their ciphertext equivalent (a letter that is moved forward three positions). Mathematically, this shift can be expressed with modular arithmetic. The formulas for encrypting and decrypting a message are:

$$E(x) = (x + 3)(mod 23)$$
$$D(x) = (x - 3)(mod 23)$$

In this case, the modulus is 23, formatted for the twenty-three-letter ancient Latin alphabet. The variable x is the original letter and the plus and minus three represents the triple shift of the cipher's algorithm. One could sequentially assign each letter a number, starting with "a" as 0 and ending with "z" as 22. If one adds three to 0, the result is 3, which corresponds with a "d".

So much for the Caesar Cipher. The Alberti cipher employs a similar variation on public-key encryption. Remember, that in the Diffie-Helman Key Exchange, the two public numbers are the prime number *p* and the generator *g* while the two private numbers are Cicero's *n* and Caesar's *m*. In the Alberti cipher, the public components are instead the capital letters written in the ciphertext. The private numbers become a combination of Alberti's "index" and the

[37] See appendix 1.1 for a detailed description and example of *modular arithmetic*

codebook. In this case, Brutus could have access to the Alberti device itself, but remain unable to operate the device or decrypt the message.

Conclusion

In the age of digital technology, cryptography continues to develop at an exponential rate. After examining the Diffie-Hellman Key Exchange and the RSA Encryption Algorithm, one may assume that the ancient ciphers and Alberti's renaissance cipher merely set the stage for techniques used in today's technology, and that the devices themselves are remnants of the past. However, this is not the case.

The Skytale was the earliest transposition cipher that catalyzed the development of true encryption over steganography. It is still consistently referenced in modern literature and provides a blueprint for every transposition device and algorithm that continues to emerge, as transposition is still used today in combination with other substitution methods. Subsequently, the Alberti Cipher revolutionized cryptography by introducing the polyalphabetic cipher and a complex key. Polyalphabetic ciphers transformed cryptography and prompted the transition from a physical key exchange to modern digital public-key cryptography.

The Caesar Cipher is still chosen in situations where more complex and newer options are readily available. In *the Codebreakers,* Kahn mentions the return of the Caesar Cipher during World War I: "when activity quickened in the spring of 1915, the Russians were using a simple Caesar Cipher."[38] Undoubtedly, newer and stronger cryptographic methods had been developed since, but in this case "the daily shift of keys, had evidently proved too difficult to handle for the

[38] Kahn, 631

half-illiterate muzhiks,"[39] so the Russians reverted back to the trusted and reliable ancient algorithm.

As recently as 2015, the Caesar Cipher was revived at the International Conference on Computer Science and Computational Intelligence. It was presented as a "New Modified Caesar Cipher Cryptography."[40] The ancient algorithm transformed from

$$E(x) = (x + 3)(mod 23)$$

$$D(x) = (x - 3)(mod 23)$$

to a significantly more complex variation of the original

$$C_{vc} = \{(p_v+b_{kx1})+(p_c+ b_{kx1})\}\text{mod}70+\{(p_v+b_{kx2})+(p_c+ b_{kx2})\}\text{mod}70+(p_v+b_{kxn})+(p_c+ b_{kxn})\} \text{ mod } 70)\}$$

$$P_{vc} = \{(C_v-b_{kx1})+(C_c- b_{kx1})\}\text{mod}70+\{(C_v-b_{kx2})+(C_c- b_{kx2})\}\text{mod}70+\{(C_v-b_{kxn})+(C_c-b_{kxn})\} \text{ mod } 70)\}$$

Here C stands for the ciphertext, output by the encryption component, and P stands for the plaintext, or result yielded by the decryption algorithm.

The purpose of the upgraded algorithm is only to further encrypt the message beyond a simple triple shift. The "new" Caesar Cipher yields an entirely legible message in its ciphered form, whereas the old model produced gibberish. Basically, it is a Caesar Cipher operating in two pieces. The modified Caesar Cipher replaces the alphabet in two parts: one pattern for the vowels and another for the consonants. A table is created in which every possible substitution is laid out.[41] The author of the secret message then searches for a combination of text that results in

[39] Kahn, 631
[40] Purnama and Rohayani, 195
[41] Purnama and Rohayani, 195

a legible message. Two words in the same message may not follow the same substitution rules based on their consonant and vowel composition. The resulting ciphertext is therefore much more secure than that of the text yielded by the original Caesar Cipher.

Purnama and Rohayani state that "the ciphertext produced by this method can be read properly, thus certain parties would not be suspicious of [any] messages that have been encrypted."[42] Note that the function of the new Caesar Cipher matches that of the old one. It is not a novel device, but rather an upgrade.

Not only has the essence of the device survived, but the Caesar Cipher – the culmination of encryption technology in antiquity – is still used in the twenty-first century.

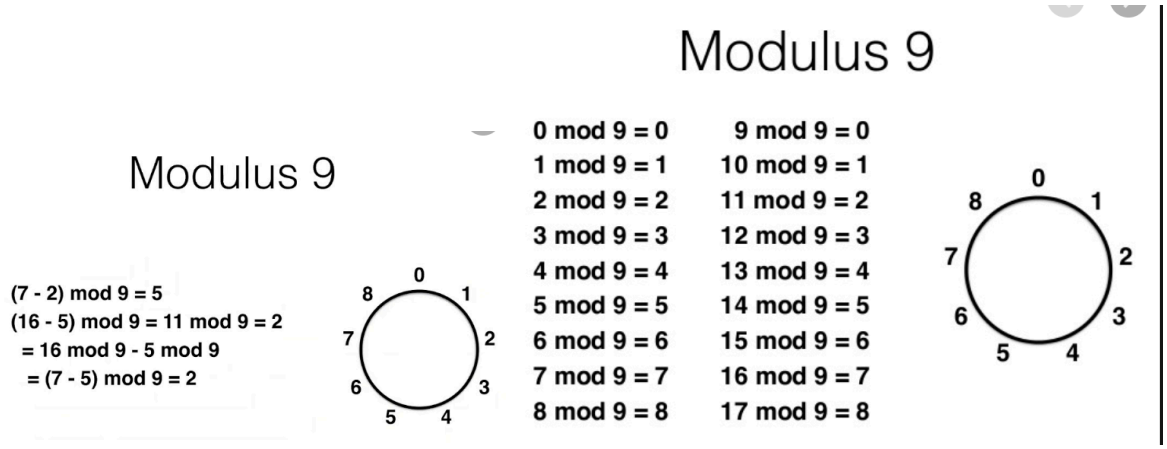
[42] Purnama and Rohayani, 203

Appendix

1.1 Explanation and example of modular arithmetic

Modular arithmetic is a cyclical system where numbers are recycled and replaced within a set range. Often, it is referred to as "clock arithmetic."
Take a number, raise it to some exponent, and divide by the "modulus" (some number) and output the remainder. The remainder of the division is the number that will always be used.

Given the remainder, it is almost impossible to reverse the calculation. Therefore, it is a one-way function that is easy to perform and difficult to reverse, making it a perfect encryption scheme.



1.2 Example of a Diffie-Hellman Key Exchange

General Formula: $g^n \pmod p$

Public Information: Everyone can see this

- Prime number p = 17
- Generator g = 3
- Caesar's calculation x
- Cicero's calculation y

Private Information (Only Cicero can see this)

- Cicero's private number n = 15
- He calculates: $x = 3^{15} \pmod{17}$

- $x = 6$
- He then sends x publicly to Caesar. (EVERYONE knows x)

Private Information (Only Caesar can see this)

- Caesar's private number $m = 13$
- He calculates: $y = 3^{13} \pmod{17}$
- $y = 12$
- He then sends y to Caesar.

How it works:

Cicero calculates: $a = y^n \pmod{17}$

and y = 12 and n = 15, so… $a = 12^{15} \pmod{17}$

Caesar calculates: $b = x^m \pmod{17}$

and x = 6 and m = 13, so… $b = 6^{13} \pmod{17}$

The trick??? Cicero calculates *a* and Caesar calculates *b* , but…..

a = 10
b = 10

a=b
HOW?!

The trick explained:

Even though Cicero and Caesar are doing different calculations, by the laws of exponents and mathematics, both of them get the same number, or the same *secret key.* All the information except the private numbers *m* and *n* are passed in front of Brutus, the adversary, publicly. However, Brutus has no way of getting the secret key without knowing Cicero and Caesar's private numbers. Even Caesar does not know Cicero's private number, or vice versa.
Magic!

1.3 Diagrams of the Alberti Cipher

1.4 Illustrations of the Skytale

Bibliography

Adolph F. Pauli. “Letters of Caesar and Cicero to Each Other.” The Classical World, vol. 51, no. 5, 1958, pp. 128–132.

Aumasson, Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, USA. 2017.

Burton, David M. *Elementary Number Theory*. McGraw-Hill Education, 2016.

Cimino, Al. *The Story of Codebreaking: from Ancient Ciphers to Quantum Cryptography*. Arcturus, 2017.

Dupont, Quinn. The Printing Press and Cryptography: Alberti and the Dawn of a Notational Epoch, Dupont, Quinn. 2017.

Reinke, Edgar C. "Classical Cryptography." *The Classical Journal* 58, no. 3 (1962): 113-21

Jain, Atish, et al. “Enhancing the Security of Caesar Cipher Substitution Method Using a Randomized Approach for More Secure Communication.” *International Journal of Computer Applications*, vol. 129, no. 13, 2015, pp. 6–11.

Kahn, David. “On the Origin of Polyalphabetic Substitution.” Isis, vol. 71, no. 1, 1980, pp. 122–127.

Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner's and Sons, 1997.

Láng, Benedek, and Teodóra Király. "Theory and Practice of Cryptography in Early Modern Europe." In Real Life Cryptology, 31-50. Amsterdam: Amsterdam University Press, 2018.

Leighton, Albert C. "Secret Communication among the Greeks and Romans." *Technology and Culture* 10, no. 2 ,1969, 139-54.

Luciano, Dennis, and Gordon Prichett. "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems." *The College Mathematics Journal* 18, no. 1 (1987): 2-17.

Sarah Spence Adams (2006) Historical Ciphers and Ancient Languages, Math Horizons, 13:4, 5-7

Purnama, Benni, and A.h. Hetty Rohayani. “A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext From a Message to Be Encrypted.” Procedia Computer Science, vol. 59, 2015, pp. 195–204

Williams, Kim, et al. *The Mathematical Works of Leon Battista Alberti.* Birkhäuser, 2010.

Jocelyn, H. D. “The Annotations of M. Valerivs Probvs [The Annotations of M. Valerius Probus].” The Classical Quarterly, vol. 34, no. 2, 1984, pp. 464–472.

Singh, Simon. *The Code Book: the Science of Secrecy from Egypt to Quantum Cryptography.* Anchor Books, 2000.

Trost, Stefan. “WordCreator.” *Alphabet and Character Frequency: Latin (Latina)*, Stefan Trost, www.sttmedia.com/characterfrequency-latin.

Godley, A.D. *Herodotus: The Persian Wars*. Digital Loeb Classical Library, 1920

Whitehead, David. *Aeneas Tacticus: How to Survive under Siege*. Bristol Classical, 2002.

Perrin, Plutarch, and Bernadotte. *Plutarch: Plutarchs Lives: Lysander*. Harvard University Press, 1982.