CUBO a Mathematical Journal
Vol. 6, Nº 1, (23-44). March 2004.

Cryptography - A Brief History [1]

R.A. Mollin
Mathematics Department, University of Calgary
Calgary, Alberta, Canada, T2N 1N4
ramollin@math.ucalgary.ca

ABSTRACT

This article is intended to inform the reader of the rich developmental history of cryptography beginning with its first rumblings in ancient Egypt almost four millennia ago, and proceeding to our modern day with the advent of public-key cryptography and its implications for modern life. This exposition was inspired by the author's latest two books [10]-[11].

1 A History of Classical Cryptography

Every area of study has its own language, which includes specific terms that facilitate an understanding of the objects being investigated. The science of *cryptography* refers to the study of methods for sending messages in *secret* (namely, in *enciphered* or *disguised* form) so that only the intended recipient can remove the disguise and read the message (or *decipher* it). The original message is called the *plaintext*, and the disguised message is called the *ciphertext*. The final message, encapsulated and sent, is called a *cryptogram*. The process of transforming plaintext into ciphertext is called *encryption* or *enciphering*. The reverse process of turning ciphertext into plaintext, which is accomplished by the recipient who has the knowledge to remove the disguise, is called *decryption* or *deciphering*. Anyone who engages in cryptography is called a *cryptographer*. On the other hand, the study of mathematical techniques for attempting to defeat cryptographic methods is called *cryptanalysis*. Those practicing cryptanalysis (usually termed the "enemy") are called *cryptanalysts*. The term *cryptology* is used to embody the study of both cryptography and cryptanalysis, and

[1] Mathematics Subject Classification 2000: 94A60; 11T71. Key words and phrases: cryptography, number theory, asymmetric, RSA, PKC, PKI.

the practitioners of cryptology are *cryptologists*. The term *cryptology* was coined by James Howell in 1645. The modern incarnation of the use of the word *cryptology* is probably due to the advent of Kahn's encyclopedic book [8], *The Codebreakers* published in 1967, after which the term became accepted and established as that area of study embracing both cryptography and cryptanalysis. The etymology of cryptology is the greek *kryptos* meaning *hidden* and *logos* meaning *word*.

The first recorded instance of a cryptographic technique was literally written in stone almost four millennia ago. This was done by an Egyptian scribe who used hieroglyphic symbol substitution (albeit at the time not well-developed) in his writing on a rock wall in the tomb of a nobleman of the time, *Khnumhotep*. It is unlikely that the scribe was actually trying to disguise the inscription, but rather was trying to impart some increased prestige (cache) to his inscription of the nobleman's deeds, which included the erection of several monuments for the reigning Pharaoh *Amenemhet* II. In other words, the scribe was attempting to impress the reader, and perhaps impart some authority to his writing, somewhat in a fashion similar to the use of flowery or legalistic language in a modern-day formal document. Although the scribe's intent was not secrecy (the primary goal of modern cryptography) his method of *symbol substitution* was one of the elements of cryptography that we recognize today. The use of substitutions *without* the element of secrecy is called *protocryptography*. Subsequent scribes actually added the essential element of secrecy to their hieroglyphic substitutions (on various tombs), but the end-goal here seems to have been to provide a *riddle* or *puzzle* (and therefore an enticement to read the epitaph) which most readers could relatively easily unravel. Therefore, although the cryptanalysis required was trivial, and the cryptography of hieroglyphic symbol substitution not fully developed, one may reasonably say that the seeds of cryptology were planted in ancient Egypt. Given that cryptology was born quite early, it did not mature rapidly or continuously. It had several incarnations in various cultures, with probably fewer methods extant than the number lost in antiquity.

The oldest extant cryptography from ancient Mesopotamia is an enciphered cuneiform tablet, which has a formula for making pottery glazes, and dates from around 1500 B.C., found on the site of Seleucia on the banks of the Tigris river. Also, the Babylonian and Asyrian scribes occasionally used exceptional or unusual cuneiform symbols on their clay tablets to "sign-off" the message with a date and signature, called *colophons*. However, again, these substitution techniques were not intended to disguise, but rather to display the knowledge of cuneiform held by the individual scribe for later generations to see and admire.

In the Hebrew literature, there is also evidence of letter substitution. The most common is a technique called *atbash*, in which the last and the first letters of the Hebrew alphabet are interchanged, and the remaining letters similarly permuted, namely the penultimate letter and the second are interchanged, the antepenultimate letter and the third are interchanged, and so on. This early form of protocryptography, which was used in the Bible, had a profound influence upon monks of the Middle Ages, and contributed to the evolution of the modern use of *ciphers*, which we may regard as a given "method" for transforming plaintext into ciphertext. In the Bible, there is

a well-known "cryptogram". It occurs in the Old Testament in the *Book of Daniel*, which was originally written in Aramaic, a language related to Hebrew. The scene is the great banquet given by King Balshazzar for a thousand of his lords. As it says in *Daniel 5:5*, "Suddenly, opposite the lampstand, the fingers of a human hand appeared, writing on the plaster of the wall in the king's palace." Needless to say, this distressed the king in a major way, and he sought his wise men to "decipher" the message. Either they could not or would not do so, since the message was bad news for the king, who was slain that very night. In any case, Daniel was brought before the king and easily interpreted the words for him. Daniel's accomplishment made him the first cryptanalyst, for which he became "third in the government of the kingdom". (*Daniel 5:29*)

There is also reference in the classical literature to secret writing. In Homer's *Iliad*, Queen Anteia, the wife of King Proteus of Argos, had failed to seduce the handsome Bellerophon (also known as *Bellerophontes*, one of the heros of Greek literature). Not taking rejection well, she lied to the king, telling him that he had tried to "ravish" her. The enraged king, not willing to go so far as to put him to death directly, instead sent him to his father-in-law, the Lycian king, with an enciphered message in a folded tablet that was to ensure Bellerophon's death. The Lycian king deciphered the tablet sent to him by his son-in-law Proteus, and sent Bellerophon on several dangerous tasks intended to result in his death. However, Bellerophon prevailed in each of the tasks, which ranged from slaying monsters to defeating Lycia's greatest warriors. Proteus's father-in-law concluded that he must indeed be under the protection of the gods, so the Lycian king gave him not only his daughter but half of his kingdom. This story contains the only reference in the *Iliad* to secret writing.

The first known establishment of *military cryptography* was given to us by the Spartans, who used one of the first transposition cipher devices ever devised, called a *skytale*, which consisted of a wooden staff around which a strip of parchment was tightly wrapped, layer upon layer. The secret message was written on the parchment lengthwise down the staff. Then the parchment (which could also be replaced by papyrus or leather) was unwrapped and sent. By itself, the letters on the parchment were disconnected and made no sense until rewrapped around a staff of equal circumference, at which point the letters would realign to make sense once again. There are several instances of the Spartans using skytales, mostly to recall recalcitrant generals from the field. One of the most notable such uses occurred around 475 B.C. with the recalling of general Pausanius, who was also a Spartan prince, since he was trying to make alliances with the Persians, upon which the Spartans did not look kindly. Over a hundred years later, general Lysander was recalled, using a skytale, to face charges of sedition.

The first use of substitution ciphers in both domestic and military affairs is due to Julius Caesar, and it is called the *Caesar Cipher* to this day. In *The Lives of the Twelve Caesars*, Suetonius [14, p. 45] notes that Caesar wrote "to Cicero, and others to his friends, concerning domestic affairs; in which, if there was an occasion for secrecy, he wrote in ciphers; that is, he used the alphabet in such a manner, that not a single word could be made out. The way to decipher those epistles was to substitute

the fourth for the first letter, as d for a, and so for the other letters respectively." He also used secret writings in his military efforts, which is documented in his own writing of the *Gallic Wars*.

The Julius Caesar's Cipher is illustrated by the following. Suppose that we know that

NQRZOHGJH LV SRZHU

has been enciphered using the Caesar Cipher, which is manifested in the cipher table below.

Table 1 The Caesar Cipher

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

The plaintext is given by:

KNOWLEDGE IS POWER

There were numerous isolated incidents involving the use of cryptography in Egypt, Persia, and Anglo-Saxon Britain, among others. However, with the fall of the Roman empire, Europe descended into the "Dark Ages", with illiteracy rampant, and both art and science a faded memory, including of course any development of cryptography. In the Middle Ages, one of the few authors to discuss cryptography was Roger Bacon. In the *Epistle on the Secret Works of Art and the Nullity of Magic*, written around 1250, he describes shorthand, invented characters, and even "magic figures and spells". To this day cryptography still has an air of the occult attached to it, which is partly due to the history of its association with secret spells and incantations that bestowed power upon the "sorcerer" who voiced them. However, the extraction of information by cryptographic techniques has become an objective science, whereas its unfortunate associate *divination*, or insight into the future, usually by "supernatural" means (such as *astrology* and *numerology*, for instance), is subjective and at best an amusing distraction in our modern world. However, the history of cryptography has rendered an association with magic, largely fostered by the perception that the removal of a disguise from a deeply buried secret is somehow miraculous or magical. Thus, through education about cryptography, we can remove the aura of magic attached to it and better understand it as a science with a fascinating history.

Perhaps more famous than Bacon's brief discussion of cryptography, was the use of ciphers by another writer of the Middle Ages, Geoffry Chaucer. In his work, *The Equatorie of the Planetis*, he included six brief, enciphered passages. What sets this apart is that the cryptograms are in Chaucer's own handwriting, thus rendering them to be more illustrious than other enciphered documents in the history of the subject. In his cryptograms, Chaucer described a simplified means for the use of an astronomical instrument called the *equatorie*.

Nowhere in the preceding history do we see a marriage of cryptography and cryptanalysis. In fact, the first to actually record methods of cryptanalysis (and therefore

create what we now call cryptology) were the Arabs. The immensely rich civilization created by the Arabs in the seventh century A.D. meant that science and creative writing flourished, and this included the study of secret writing. However, it was not until 1412, with the publication of the fourteen-volume work *Ṣubḥ al-a 'sha* that the complete documentation of the Arabic knowledge of cryptology appeared. One of the important features of this great work was that it contained the first systematic explanation of cryptanalysis in recorded history.

Once Europe exited from the Middle Ages, the study of cryptology began in earnest. In Pavia, Italy on July 4, 1474, Cicco Simonetta (a secretary to the Dukes of Sforza, oligarchs of Milan) wrote the first known manuscript devoted solely to cryptanalysis. He wrote thirteen rules for symbol substitution ciphers. Later, another Italian, Giovanni Soro, was appointed *Cipher Secretary* for Venice in 1506. His success at cryptanalysis was so great that by 1542 Soro was given two assistants and an office in the Doge's Palace above the Sala di Segret. There they worked in the highest security deciphering all dispatches from foreign powers that were obtained by the Venetians. Soro died two years later.

Among other authorities who had cryptologic assistants by their side were the popes. Ultimately, the practice became so common and of such importance that the office of *Cipher Secretary* to the pontiff was created in 1555. The first to have the title bestowed upon him was Triphon Bencio de Assisi. In 1557, King Philip II of Spain was warring with Pope Paul IV, who had deep-seated anti-Spanish sentiments, and under the leadership of de Assisi, one of the King's cryptograms was deciphered by the cryptanalysts. Peace was finally made on September 12, 1557.

By the late 1580's the Argentis, a family of cryptologists, took over the cipher secretariat. Matteo Argenti, for instance, wrote a 135-page leather-bound book on cryptology, which is purported to describe and summarize the height of Renaissance cryptology. The Argentis also were the first to institute certain cryptographic processes, which later became widespread in use, such as using a mnemonic (memory aid) key to mix a cipher alphabet. We will think of a *key* as a parameter or set of parameters that determines which cipher we will use. For instance, a key may specify the pattern of moving letters around in a transposition. A *cipher alphabet* is a list of equivalents used to transform the plaintext into secret form.

In Spain, Philip II ascended to the throne in 1556. In that same year, he decided to discard the (much compromised) ciphers used during the reign of his father Charles V. He emulated Soro by dividing his cipher systems into two classes: the *cifra general*, used for correspondence between the king and various ambassadors; and the *cifra particular*, used by an individual messenger and the king. Philip's new general cipher was one of the strongest of its day, and became the template for Spanish cryptography far into the seventeenth century. Cryptography even found its way to the *New World*. The oldest remaining record of this *New World cryptography* is a letter dated June 25, 1532 sent by Cortés from Mexico.

In France, Henry IV was able to decipher letters sent between Philip and his officers in France, who were at war with Henry. He did this with the assistance of François Viète, who was a Huguenot sympathizer with cryptanalytic skills. The

Spanish, on the other hand, despite their cryptographic skills were sadly lacking in cryptanalytic abilities. For instance, Viète cryptanalyzed a Spanish letter destined for Alessandro Farnese, the Duke of Parma, who headed the Spanish forces of the *Holy League*, a Catholic faction opposed to the protestant king on the throne of France. When Philip found out about Viète's cryptanalysis of other letters to his commanders in France, he was stunned, having thought they were unbreakable. This failure to understand cryptanalytic techniques was to have disastrous consequences for Philip and his greatest dream, which was to overthrow Queen Elizabeth, establish a marriage with Mary, Queen of Scots, and thereby secure a shared Catholic crown with her.

Philip supported the siege of Paris against the Duke of Mayenne, who headed the French forces of the Holy League. Henry intercepted a Spanish cryptogram from Commander Juan de Moreo to King Philip. Philip van Marnix, who had joined Henry's forces at the siege, was able to decipher it. A report of the decrypted Spanish letter, which revealed Philip's plans for England, reached Sir Francis Walsingham, minister to Queen Elizabeth, who headed a secret intelligence organization in England. Although Philip did not invade England until eleven years later, this cryptanalyzed report prepared them. Moreover, Walsingham employed a man in Paris, named Thomas Phelippes, who became England's first eminent cryptanalyst. This alliance was to prove fatal for Mary. Phelippes was able to cryptanalyze messages sent between herself and one of her pages, which outlined the plot to assassinate Queen Elizabeth. Ultimately, on July 17, 1586, Walsingham had sufficient evidence to submit. Mary, Queen of Scots, was put to death by the axman on February 6, 1587 — an axe set in motion by a cryptanalyst's skills.

The fifteenth and sixteenth centuries also saw the establishment of numerous classical developments in cryptology. The title: *Father of Western Cryptology* goes to an architect named Leon Battista Alberti. In 1470, he published his *Trattati in cifra* in which he describes the first *cipher disk*, a mechanical tool for general substitution with shifted mixed alphabets. Thus, Alberti gave rise to the notion of *polyalphabeticity*. This is distinct from *homophonic substitution* in which a plaintext letter is always represented by the same ciphertext equivalent, such as 5 for the letter C.

On his disk, Alberti has an outer ring consisting of twenty letters and the numbers $1, 2, 3, 4$, and an inner disc, which was a movable circle, consisting of 24 characters in the Latin alphabet. The plaintext letters were chosen from the inner disc and the ciphertext letters corresponded to the character on the outer ring. With Alberti's disk, the word *hit* might be encrypted as *med* on one setting of the disc, then at a new setting, might be represented by *suf*, for instance. As well as this first polyalphabetic cipher, Alberti is responsible for inventing the *enciphered code*. This was the reason that Alberti put the numbers on the outer ring. In a table he had 336 codegroups corresponding to the use of the numbers 1 to 4 in two-, three- and four-digit groups, from 11 to 444. (Note that $336 = 4^2 + 4^3 + 4^4$.) The codegroups would have some preassigned meaning for the plaintext such as: "We attack at dawn." for the number 434. Hence, 434 would be perhaps enciphered as *rad* in one position and as *bro* in another. This was a concept that was four centuries ahead of its time. In fact, when

code enciphering began in earnest at the end of the nineteenth century, the codes used were simpler than his.

In 1553, a small book entitled *La cifra del. Sig. Giovan Batista Belaso*, by Giovan Batista Belaso was published. In this booklet, he introduced the notion of an easily remembered and easily changed key, which he called a *countersign*, for a polyalphabetic cipher. However, Belaso used standard alphabets in his ciphers. The use of mixed alphabets in a polyalphabetic cipher was developed by the next character to enter the stage.

In 1563, a respected work on cryptology entitled *De furtivis Literarum Notis* by Giovanni Battista Porta was published. In it he planted the seeds for the modern division of ciphers into transposition and substitution. The major contribution of this work is that it was the first time that polyalphabeticity was fully enunciated, and it contained the first *digraphic* cipher, in which two letters were used as a single symbol. His book went through several editions, culminating in a 1593 edition, published under the title *De Occultis Literarum Notis*, which included the first synoptic (comprehensive overview) tables ever made for cryptology. This outlined the various paths that a cryptanalyst could traverse in the analysis of a cryptogram. Thus, many historians consider Porta to be the most outstanding cryptographer of the Renaissance.

The following example of a digraphic cipher will illustrate the above. The idea behind the following cipher was conceived by Sir Charles Wheatstone, and was sponsored at the British Foreign Office by Lord Lyon Playfair. Thus, it has become known as the Playfair cipher.

Table 2

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

Pairs of letters are enciphered according to the following rules.

(a) If two letters are in the same row, then their ciphertext equivalents are immediately to their right. For instance, VC in plaintext is RV in ciphertext. (This means that if one is at the right or bottom edge of the table, then one "wraps around" as indicated in the example.)

(b) If two letters are in the same column, then their cipher equivalents are the letters immediately below them. For example, ZF in plaintext is UR in ciphertext, and JB in plaintext is GI in ciphertext.

(c) If two letters are on the corners of a diagonal of a rectangle, then their cipher equivalents are on the other corners, and the cipher equivalent of each plaintext letter is on the same row as the plaintext letter. For instance, UL in plaintext becomes GF in ciphertext and SZ in plaintext is FD in ciphertext.

(d) If the same letter occurs as a pair in plaintext, then we agree by convention to put a Z between them and encipher. Also, if a single letter remains at the end of the plaintext, then a Z is added to it to complete the digraph.

Example 1 *Suppose that we wish to decipher:* **BP DV GW VY FD OE HQ YF SG RT CF TU WC DH LD KU HV IV WG FD**, *assuming that it was encrypted using the Playfair Cipher. One merely reverses the rules to decipher. For instance, the first pair BP of ciphertext letters occurs on the same row. So we choose the letters to their left, PR. The second set DV occurs on a diagonal with AC as the opposite ends (respectively) of the other diagonal. Then GW occurs in diagonal with TI, which is chosen as plaintext, and so on to get:* **practices zealously pursued pass into habits**, *where the last letter Z is ignored as the filler of the digraph. Such fillers are called* nulls.

One of the most clever innovations created in sixteenth century cryptological studies was the *autokey*, which was the ingenious idea of using the message as its own key. The inventor of the first such autokey was Girolamo Cardano.

There is a cipher called the *Vigenère cipher*. However, Blaire de Vigenère, after whom it is named, had nothing to do with it. Misattribution has stuck him with a relatively minor system when he was responsible for the invention of a more important system — the first *valid* autokey system. Vigenère's autokey system used the same principle as Cardano's system, namely the plaintext was to be the key. However, his method did not have the inherent flaws attributed to Cardano. Vigenère provided a primer key consisting of a single letter that would be known to the sender and the receiver. This would allow the receiver to decipher the first letter of the cryptogram. Then this now known first letter of the plaintext could be used to decipher the second cryptogram letter, which in turn could be used to decipher the third cryptogram letter and so on. Unfortunately, his invention was forgotten and reinvented in the late nineteenth century. The cipher with his name attached to it is a very elementary, degenerate version of his original idea, having only one repeating keyletter and a direct standard alphabet. This means the ordinary alphabet (standard) in its usual order (direct).

As mentioned earlier, the first use of two-part codes began in seventeenth-century France. France's first recognized full-time cryptologist was Antoine Rossignol, who served both Louis XIII and XIV. He also assisted Cardinal Richelieu with his cryptanalytic skills, by ensuring that the Catholic armies under Richelieu prevailed over the Huguenots in southern France in 1628. His cryptographic abilities were also important since he helped develop technical improvements in nomenclatures that were the most vital in over four centuries.

During Rossignol's service, the practice of using two-part nomenclatures went into high gear. This involved a first part called a *tables à chiffer*, consisting of plaintext letters in alphabetical order, and ciphertext symbols in random order, whereas the second part, called the *tables à déchiffer*, consisted of the plaintext letters jumbled.

while the ciphertext symbols were in alphabetical or numerical order. Rossignol died in 1682 at the age of eighty-two.

One of the most noteworthy cryptanalysts of the eighteenth century was Edward Willes who was a minister at Oriel College in Oxford in 1716 when he was hired with the title of *Decypherer* for the English crown. He solved a cipher that revealed Sweden's plan to create an uprising in England. For this and other feats, he rose to become Cannon of Westminister in short order, and ultimately in 1742 was made Bishop of St. David's. He died in 1773, and was buried at Westminister abbey.

An amusing anecdote concerning cryptanalysis of a polyalphabetic cipher in the eighteenth century occurred in 1757. The central character was the famous Casanova, who received a cryptogram for safekeeping from his wealthy friend, Madame d'Urfé. She believed that the cryptogram could never be broken given that she held the keyword in her memory and had never written it down or disclosed it to anyone. Nevertheless, Casanova was able to cryptanalyze the enciphered manuscript, which contained a description for the transmutation of baser metals into gold. He was also able to recover the key via his calculations. She was incredulous at the revelation. Casanova later wrote in his memoirs: "I could have told her the truth—that the same calculation which had served me for deciphering the manuscript had enabled me to learn the word—but on a caprice it struck me to tell her that a genie had revealed it to me." The keyword?— NEBUCHADNEZZAR, or in Italian *NABUCODONOSOR*.

Meanwhile, in the seventeenth-century American colonies, cryptology was not as sophisticated as that in Europe. Nevertheless, after some preliminary difficulties with secret writing, the Founding Fathers sought to improve their means of secret communication. The chief proponent of that improvement was Thomas Jefferson. Jefferson compiled a nomenclature in 1785 for the purpose of communicating secretly with Madison and Monroe, and this was used until 1793. More importantly for history, just prior to the dawn of the nineteenth century, Jefferson created what he called his *wheel cypher*, which was far ahead of its time. Unfortunately, Jefferson filed away his idea and forgot about it. It was not rediscovered until 1922 among his papers in the Library of Congress. Some departments of government agencies and the military used it thereafter since modern cryptanalysts often could not defeat it! Hence, Jefferson has been rightly termed *The Father of American Cryptography*.

By the time of the American Civil War, the Union Army was using relatively advanced cryptography, while the Confederate Army used the Vigenère cipher with standard substitution. It gets worse — much worse. On one occasion, a Confederate General, Albert S. Johnson, decided to use a Caesar substitution! Of course, the cryptography used by the Confederate Army was a disastrous failure. Regularly, Confederate troops were being captured with cryptograms that President Lincoln's youngest cryptanalysts could solve. On the other hand, rarely could the Confederates decipher a union cryptogram. A Vigenère cipher was even found in John Wilkes Booth's hotel room after he was shot. This was used at trial to convict not only Booth, but also eight other Southern sympathizers, all of whom were hanged, even though the connection of the eight with Booth and his cipher was not established.

By the end of the nineteenth century, cryptography was nearing maturity and

showed up in some famous cases. In what came to be known as the *Dreyfus Affair* in France, cryptology played a crucial role. On October 15, 1894, Captain Alfred Dreyfus of the French general staff was arrested and charged with high treason. They suspected him of giving military secrets to German or Italian officials. Later, the Italian military attaché, Colonel Alessandro Panizzardi, sent a cryptogram to Rome. The French cryptanalysts, who regularly got copies of such cryptogams, began to work on deciphering it. They deciphered it as: "If Captain Dreyfus has not had relations with you, it would be wise to have the ambassador deny it officially, to avoid press comment." This suggested that Panizzardi disavowed any contact with Dreyfus. Those who were convinced of Dreyfus's guilt were skeptical. Thus, the French decided to trick Panizzardi into sending a telegram whose contents were known to them. In this way, they would have certain access to decryption. Panizzardi fell for a ruse, enciphered the telegram and sent it to Rome. The French were able to use it to verify the decryption of the original message. This should have exonerated Dreyfus, but again those who were convinced of his guilt, or would rather that an innocent man go to jail than admit an error, refused to let the telegram be admitted at his first trial. Dreyfus was convicted of treason and sent to Devil's Island. Upon appeal, the telegram was admitted into official evidence, but it would take several years before Dreyfus got true justice, which would include reinstatement and the Legion of Honour. The true culprit, Major Ferdinand Walsin Esterhazy, was arrested with several cardboard grilles that implicated him in having secret communication with the German military attaché.

In the dawn of the twentieth century, with a world war brewing, cryptology was headed for a major turning point. In the years 1914–18, World War I saw the use of small codes for low-level communications, and certain complicated cipher systems for high-level communications. For example, the first version of the famous ADFGVX cipher was introduced by the Germans on March 1, 1918. It was named in this fashion since only those six letters were used in the cryptogram. These letters were chosen since the Morse code equivalents were sufficiently dissimilar to minimize errors. The presence of only six letters ensured that the system was quick and easy for the Germans. The Allies could not crack the first cryptograms sent by this cipher system, so it turned out to be the toughest field cipher known to that date. Then the first such messages were brought to the attention of Georges Jean Painvin who was the best cryptanalyst in France's Bureau du Chiffre. Ultimately, he did decrypt them, and later was able to decipher even more. His cryptanalytic efforts ultimately saved French forces and helped to turn the tide for the Allies.

An example of the German ADFGVX field cipher is given as follows. This cipher used a table such as the following where the twenty-six letters of the alphabet plus the ten digits (with 10 represented by ϕ) populate the six-by-six square, where the coordinates of each letter and digit uniquely determined by the six letters. For instance, the coordinate of H is FX.

Table 3

	A	D	F	G	V	X
A	*B*	3	*M*	*R*	*L*	*I*
D	*A*	6	*F*	ϕ	8	2
F	*C*	7	*S*	*E*	*U*	*H*
G	*Z*	9	*D*	*X*	*K*	*V*
V	1	*Q*	*Y*	*W*	5	*P*
X	*N*	*J*	*T*	4	*G*	*O*

Thus, for instance, *The British have landed* would be enciphered as:

XF FX FG AA AG AX XF AX FF FX

FX DA GX FG AV DA XA GF FG GF

However, this is only the *transitional* ciphertext, which was then placed in another rectangle to be transposed into the *final* ciphertext using a numerical key as follows. We think of the letters of *GERMAN* as having numerical equivalents according to the alphabetic order of the letters, namely A corresponds to 1 since it is the letter in GERMAN that appears first in the alphabet, then E corresponds to 2, and so on. Then place the above transitional ciphertext by rows into a matrix as follows.

Table 4

G	E	R	M	A	N
3	2	6	4	1	5
X	*F*	*F*	*X*	*F*	*G*
A	*A*	*A*	*G*	*V*	*A*
X	*F*	*V*	*A*	*F*	*F*
F	*X*	*F*	*X*	*D*	*A*
G	*X*	*F*	*G*	*A*	*V*
D	*A*	*X*	*A*	*G*	*F*
F	*G*	*G*	*F*		

Now the final ciphertext is obtained by "peeling off" the *columns* in the above rectangle according to the order of the numbers as follows and grouping the letters in convenient five-letter pieces.

FVFDA GFAFX XAGXA XFGDF

XGAXG AFGAF AVFFA VFFXG

The reader may also verify, using the above cipher, that the ciphertext:

VVFDVVFAA XXXXAGAFG

AXAVFADDV FVFGGGGXA

FGXAXXGGG DFFFFFAXD

has plaintext:

IF YOU WISH PEACE PREPARE FOR WAR.

Despite the aforementioned successes, there were failures that amounted to defeat in battle for some during the war, because of poor cryptography. For instance, the Russians lost the battle of Tannenberg in August 1914, because of failure of their cryptographic communications. The reason for this failure deserves some elucidation as follows. The Russian Second Army was planning to come up behind the Germans, cut off their retreat, and destroy them. However, Russian communications were, at best, inadequate. They ran out of wire to string, so there was no communication between army headquarters and core headquarters, which were the two highest levels of field command. This was compounded by the fact that inept distribution of military ciphers and their keys meant they did not have the cryptographic tools. Hence, Russian signalmen were sending messages over the radio in the clear, without even attempting to encipher. Thus, the Germans knew the Russian military plans in advance. When it was over, roughly 100,000 Russians were taken prisoner, 30,000 were dead or missing, so the Russian Second Army had ceased to exist. Hence, Tannenberg became the first battle in history to be determined by cryptographic failure. On the other hand, the deciphering of one of the most famous telegrams in history was accomplished by the British, namely the *Zimmerman Telegram*, of January 16, 1917 that offered Mexico territorial gains if it would enter the war on the side of Germany. This was a major contributing factor to the United States entering the war on April 6, six weeks after President Wilson learned of its contents.

In the postwar years, considerable advances were made in cryptography, most especially with cipher machines, which were used extensively in World War II. Shortly before World War II, the United States was was able to reconstruct the Japanese cipher machine that was used for diplomatic communication. Thus, the American cryptanalysts enjoyed tremendous success in deciphering Japanese cryptograms during the war. One incident that goes down in infamy deserves special mention — Pearl Harbour.

It was November 19, 1941, when the U.S. Navy intercepted a diplomatic radio message sent from Tokyo to Washington. By the twenty-eighth of the month, they had cryptanalyzed the message, which indicated that there would follow an cryptogram announcing intention of hostilities. This resulted in a flurry of activity to intercept Japanese radio traffic for the cue. It came on December seventh, several hours *after* the attack on Pearl Harbour, and the message only mentioned intended hostilities toward Great Britain. However, even this message was intended as a signal to some Japanese outposts, who had not already done so, to burn their codes. Hence, Japan had commenced hostilities without a prior declaration of war, an act that would make up some of the charges laid against Japanese war criminals after the war.

Due to the nature of the Pearl Harbour attack, the Joint Congressional Committee met for an investigation, which concluded that the efforts of the American cryptanalysts had shortened the war, and saved thousands of lives. For instance, cryptanalysts helped to ensure that Japan's lifeline was rapidly cut, and that German U-boats were defeated. Another incident involved the downing of the plane carrying the commander-in-chief of the Combined Fleet of the Japanese Navy, Admiral Isoruko Yamamoto. The American cryptanalysts had been able to decipher a

highly secret cryptogram, giving the itinerary of Yamamoto's plane on a tour of the Solomon Islands. Of vital importance was the Battle of Midway, which was a stunning victory by American cryptanalysts since they were able to give complete information on the size and location of the Japanese forces advancing on Midway. This enabled the Navy to concentrate a numerically inferior force in exactly the right place at the right time, and prepare an ambush that turned the tide of the Pacific War.

World War II saw another outstanding achievement in cryptanalysis by the Allies. Essentially, the story begins with the invention of the electric typewriter, which provided the means for the introduction of electromechanical enciphering machines. Credit for inventing the first electric contact rotor machine goes to the American, Edward Hugh Hebern. In 1915, he used two electric typewriters (randomly) connected by twenty-six wires. Hence, a plaintext letter key hit on one typewriter would result in a ciphertext letter to be printed on the other machine. These wire connections provided the seed idea for a rotor, namely a way of varying the monoalphabetic enciphering. By 1918, Hebern had a device that embodied the rotor principle. Also, in that year, the German Arthur Scherbius applied for a patent on a rotor enciphering machine using multiple rotors. In 1923, a corporation was formed to manufacture and sell his machine, which he called the *Enigma*. In 1934, the Japanese Navy bought the Enigma for their own use, and it developed into the Japanese cryptosystem called *Purple* by the Americans. This was a polyalphabetic cipher cryptanalyzed in August 1940 by the U.S. Signal Intelligence Service.

By the time of Hitler's arrival on the scene, the cryptographers of the Wehrmacht made a (fateful) decision that the Enigma would work well for their security purposes, so the German forces were supplied with it. The German Enigma cryptosystem was cryptanalyzed by the researchers at Bletchley Park, which was a Victorian country mansion in Buckinghamshire, halfway between Oxford and Cambridge, England. This is the place to which the Government Code and Cypher School was seconded in August 1939. Most important among these researchers was Allan Turing. Turing designed a machine for cryptanalyzing Enigma. Based upon his ideas, a machine was built, called the *BOMBE*, which was operational on March 18, 1939. In early 1940, the researchers at Bletchly Park were routinely breaking the Enigma cryptograms sent by the Luftwaffe. By September of 1941, Field Marshal Rommel's Enigma cryptograms to Berlin were being cryptanalyzed. In 1942, the British had dug deeply into cryptanalyzing Enigma, and the Russians were also deciphering such cryptograms. This played a major role in the Allied victory. World War II saw cryptology reach adulthood, with mathematics as its firm foundation.

In the United States, the National Security Agency (N.S.A.) can be said to have arisen out of the attack on Pearl Harbour. Given the official secret work of governments around the globe, the development of cryptographic techniques in modern times is often cloaked in official secrecy. Nevertheless, there have been astounding cryptographic techniques, which were developed in the public domain, and deserve to be better understood by the greatest number of people.

2 The Advent of Public-Key Cryptography

All of the above involves symmetric-key cryptography, where both the enciphering and eciphering keys must be kept secret. However, with the advent of the notion of a *public* enciphering key in the 1970s, cryptography was about to receive a radical face-lift. Although M. Hellman, W. Diffie, and R.C. Merkle were credited (in the public domain) with the discovery of the notion of public-key cryptography, it is now *public* knowledge that the notion had already been discovered years earlier by British cryptographers, but not *officially* released until relatively recently. Here are the known facts.

Public-key methodologies were first discovered by the Communications-Electronics Security Group (CESG) in the early 1970s. The function of CESG, as a branch of the British Government Communications Headquarters (GCHQ), is to ensure information security for the British government, which regards CESG as their technical authority on official cryptographic applications.

In December of 1997, five papers, [4], [6]–[7], [16]–[17], were released by CESG, which the reader may download from:

http://www.cesg.gov.uk/publications/index.htm#nsecret.

In January of 1970, J. Ellis established the fundamental ideas behind public-key cryptography in [6]. He called his method *non-secret encryption* (NSE). Hence, the discovery of the idea of public-key cryptography predated Diffie, Hellman, and Merkle by more than a half dozen years. In [4], dated November 20, 1973, C. Cocks essentially describes what we now call the RSA cryptosystem, with any differences being entirely superficial. In [16], dated January 24, 1974, Williamson describes what we now call the Diffie-Hellman key-exchange protocol. In [17], dated August 10, 1976, Williamson improved upon the ideas [16] he put forth in 1974.

In [7], published (internally) in CESG in 1987, Ellis describes the history of NSE. In this paper, he says: "The task of writing this paper has devolved to me because NSE was my idea and I can therefore describe their developments from personal experience." Also, in this paper Ellis cites the 1944 publication [15] (by an unknown author for Bell Laboratories) which he describes as an ingenious idea for secure conversation over a telephone. This was his inspiration for NSE. Ellis states, in the aforementioned paper, that this is how the idea was born, that secure communication was possible if the recipient took part in the encryption process. At the end of his paper Ellis concludes that the Diffie-Hellman idea: "was the start of public awareness on this type of cryptography and subsequent rediscovery of the NSE techniques I have described."

In an interview in the the *New York Times* in December of 1997, Williamson said that he felt badly knowing that others were taking credit for solutions found at CESG. However, he concluded that this was just one of the restrictions to which you agree and accept when you work for a government agency on secrecy projects. On the other hand, Hellman has said that these things are like stubbing your toe on a gold nugget left in the forest: "If I'm walking in the forest and stub my toe

on it, who's to say I deserve credit for discovering it?" Hellman's philosophical bent here is that of a *Platonist* in the sense that all discoveries are assumed to be just that — *discoveries*, rather than creations. Hellman also stated that he, Diffie, and Merkle were all "working in a vacuum". He claimed that if they had had access to the classified documents over the previous three decades, it would have been a great advantage. Diffie commented that the history of ideas is hard to write because people find solutions to different problems and later find out that they have discovered the same thing as someone else. It is up to historians to sort out the details and the claims, but it is certain that the ideas for public-key cryptography were known (in the classified domain) well in advance of the (publicly acknowledged) efforts of Diffie, Hellman, and Merkle. CGHQ/CESG have stated that more documents are scheduled for release.

Now that we have some background, we may formalize what we mean by a public-key cryptosystem. A cryptosystem consisting of a set of enciphering transformations $\{E_e\}$ and a set of deciphering transformations $\{D_d\}$ is called a Public-key Cryptosystem or an Asymmetric Cryptosystem if, for each key pair (e, d), the enciphering key e, called the public key, is made publicly available, while the deciphering key d, called the private key, is kept secret. The cryptosystem must satisfy the property that it is computationally infeasible to compute d from e.

We use the convention that the term *private key* is reserved for use in association with public-key cryptography, whereas the term *secret key* is reserved for use in association with symmetric-key cryptosystems. This convention is used in the cryptographic community because it takes two or more entities to share a secret, but a key is truly private when only one entity knows about it.

A standard analogy for public-key cryptography is given as follows. Suppose that Bob has a wall safe with a secret combination lock known only to him, and the safe is left open and made available to passers-by. Then anyone, including Alice, can put messages in the safe and lock it. However, only Bob can retrieve the message, since even Alice, who left a message in the box, has no way of retrieving the message.

The first to (publicly) provide a complete solution to the notion given above of a public-key cryptosystem were Ronald Rivest, Adi Shamir, and Leonard Adleman, for which their names are attached to the cryptosystem we now describe.

◊ The RSA Public-Key Cryptosystem

We break the algorithm into two parts with the underlying assumption that Alice wants to send a message to Bob.

(I) RSA Key Generation

(1) Bob generates two large, random primes $p \neq q$ of roughly the same size.

(2) He computes both $n = pq$ and

$$\phi(n) = (p-1)(q-1),$$

where $\phi(n)$ is the Euler totient. The integer n is called his (*RSA*) *modulus*.

(3) He selects a random $e \in \mathbb{N}$ such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The integer e is called his (*RSA*) *enciphering exponent*.

(4) Using the extended Euclidean algorithm, he computes the unique $d \in \mathbb{N}$ with $1 < d < \phi(n)$ such that

$$ed \equiv 1 \pmod{\phi(n)}.$$

(5) Bob publishes (n, e) in some public database and keeps d, p, q, and $\phi(n)$ private. Thus, Bob's (*RSA*) *public-key* is (n, e) and his (*RSA*) *private key* is d. The integer d is called his (*RSA*) *deciphering exponent.*

(II) RSA Public-Key Cipher

enciphering stage:

In order to simplify this stage, we assume that the plaintext message $m \in \mathcal{M}$ is in numerical form with $m < n$. Also, $\mathcal{M} = \mathcal{C} = \mathbb{Z}/n\mathbb{Z}$, and we assume that $\gcd(m, n) = 1$.

(1) Alice obtains Bob's public-key (n, e) from the database.

(2) She enciphers m by computing $c \equiv m^e \pmod{n}$.

(3) She sends $c \in \mathcal{C}$ to Bob.

deciphering stage:

Once Bob receives c, he uses d to compute $m \equiv c^d \pmod{n}$.

Example 2 *Suppose that Bob chooses* $(p, q) = (1759, 7487)$. *Then* $n = 13169633$ *and* $\phi(n) = 13160388$. *If Bob selects* $e = 5$, *then by solving* $1 = 5d + \phi(n)x$ *he gets* $d = 7896233$ (*for* $x = -3$). *Thus,* $(13169633, 5)$ *is his public key and* $d = 7896233$ *is his private key. Alice obtains Bob's public key and wishes to send the message* $m = 7115697$. *She enciphers using Bob's public key to get*

$$c \equiv m^5 \equiv 10542186 \pmod{n},$$

which she sends to Bob. He uses his private key d to decipher via

$$c^d \equiv 10542186^{7896233} \equiv 7115697 \equiv m \pmod{n}.$$

We exchange roles if Bob wants to send a message to Alice. In this case, the above key generation is performed by Alice to generate her own RSA public and private keys, and Bob performs the enciphering stage sending his message to her for deciphering using her private key.

We have not addressed the issue of what occurs if the plaintext message unit is a numerical value $m \geq n$. In this case, we must subdivide the plaintext numerical equivalents into blocks of equal size, a process called *message blocking.* Suppose that we are dealing with numerical equivalents of the plaintext in base N integers for some fixed $N > 1$. Message blocking may be achieved by choosing that unique integer ℓ such that such that $N^\ell < n < N^{\ell+1}$, then writing the message as blocks of ℓ-digit, base N integers (with zeros packed to the right in the last block if necessary), and encipher

each separately. In this way, since each block of plaintext corresponds to an element of $\mathbb{Z}/n\mathbb{Z}$ given that $N^\ell < n$; and since $n < N^{\ell+1}$, then each ciphertext message unit can be uniquely written as an $(\ell+1)$-digit, base N integer in $\mathcal{C} = \mathbb{Z}/n\mathbb{Z} = \mathcal{M}$.

Example 3 *Suppose that Bob chooses* $n = 1943 = 29 \cdot 67$. *Then* $\phi(n) = 1848$, *and if he chooses* $e = 701$, *then* $d = 29$ *is a solution of* $1 = 5d + 1848x$ *with* $x = -11$. *Therefore,* $(n, e) = (1943, 701)$ *is his public key and* $d = 29$ *is his private key. Now suppose that Alice wants to send the message* **power** *to Bob. She must first convert this to numerical equivalents. She chooses the following table:*

Table 5

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

so we are using base 26 *integers. Since* $26^2 < n < 26^3$, *then* $\ell = 2$ *and we write the message as* 2*-digit, base* 26 *integers. First, via Table 5, we get the base* 26 *equivalents for the plaintext as* $15, 14, 22, 4, 17$, *so we break this up as follows:* $m_1 =$ **po** $= 15 \cdot 26 + 14 = 404$; $m_2 =$ **we** $= 22 \cdot 26 + 4 = 576$; *and* **ra** $= 17 \cdot 26 + 0 = 442$, *with the* **a**$= 0$ *packed to the right in the last block. Thus, Alice enciphers:*

$$404^{701} \equiv 1419 \,(\text{mod } 1943), \quad 576^{701} \equiv 344 \,(\text{mod } 1943),$$

$$\textit{and} \quad 442^{701} \equiv 210 \,(\text{mod } 1943).$$

Bob recovers the plaintext via his private key:

$$1419^{29} \equiv 404 \,(\text{mod } 1943); \quad 344^{29} \equiv 576 \,(\text{mod } 1943);$$

$$\textit{and} \quad 210^{29} \equiv 442 \,(\text{mod } 1943).$$

He then rewrites each deciphered block as 2*-digit base* 26 *integers and recovers the English plaintext via Table 5. Note that in Example 2,* **power** *was enciphered using only one block since we had the use of a much longer modulus, hence a longer block, given that* $\ell = 5$ *in that case.*

Now let us look at what would happen if Bob did not do any message blocking. Then since **power** *may be represented as the* 5*-digit, base* 26 *integer* m *as follows:* $m = 15 \cdot 26^4 + 14 \cdot 26^3 + 22 \cdot 26^2 + 4 \cdot 26 + 17 = 7115697$, *a single enciphering would yield* $m^{701} = 7115697^{701} \equiv 1243 \,(\text{mod } 1943)$, *which is* $1 \cdot 26^2 + 21 \cdot 26 + 21$ *as a base* 26 *integer and via Table 5, this yields* **BVV**, *having nothing to do with the original plaintext. Too much information is lost. Hence, the message blocking above is necessary. Moreover, the choice of* ℓ *is maximal (and therefore optimal for encryption), as well as necessary for a unique decryption.*

We now look at a slightly more complicated example (see [3]). On April 2, 1994, the authors of this paper factored the RSA-129 challenge number, for which RSA had

offered \$100.00(US) as a prize in 1977. (RSA challenge numbers, for factoring algorithms, are denoted by RSA-n for $n \in \mathbb{N}$, which are n-digit integers that are products of two primes of approximately the same size. These RSA challenge numbers are published on the web and one may send a request for a copy of the list to: challenge-rsa-list@rsa.com.) The plaintext they deciphered is the one given in the example, with of course, a much different modulus. They factored the number using a variation of the Multiple Polynomial Quadratic Sieve (MPQS) (see [11]), which took eight months and more than 600 researchers from more than twenty countries around the globe. This method is called *factoring by electronic mail*, a term used by Lenstra and Manasse in [9] to mean the distribution of the quadratic sieve operations to hundreds of physically separated computers all over the world. The unit of time measurement for factoring is called a *mips year*, which is defined to being equivalent to the computational power of a computer rated at one million instructions per second (mips) and used for one year, which is tantamount to approximately $3 \cdot 10^{13}$ instructions. The RSA-129 challenge number took 5000 mips years.

Example 4 *Suppose that Alice wants to send the message*

The magic words are squeamish ossifrage,

and that Bob has chosen $n = 131369633 = 57593 \cdot 2281$, *and* $e = 7$, *from which we get* $d = 112551223$ *via* $7d + 131309760x = 7d + \phi(n)x = 1$ *with* $x = -6$. *Since* $26^5 < n < 26^6$, *then we choose* $\ell = 5$, *so the message will be blocked using* 5*-digit, base* 26 *integers via Table 5 as follows.*

$$\textbf{thema} = 19 \cdot 26^4 + 7 \cdot 26^3 + 4 \cdot 26^2 + 12 \cdot 26 + 0 = 8808592,$$

$$\textbf{gicwo} = 6 \cdot 26^4 + 8 \cdot 26^3 + 2 \cdot 26^2 + 22 \cdot 26 + 14 = 2884402,$$

$$\textbf{rdsar} = 17 \cdot 26^4 + 3 \cdot 26^3 + 18 \cdot 26^2 + 0 \cdot 26 + 17 = 7833505,$$

$$\textbf{esque} = 4 \cdot 26^4 + 18 \cdot 26^3 + 16 \cdot 26^2 + 20 \cdot 26 + 4 = 2155612,$$

$$\textbf{amish} = 0 \cdot 26^4 + 12 \cdot 26^3 + 8 \cdot 26^2 + 18 \cdot 26 + 7 = 216795,$$

$$\textbf{ossif} = 14 \cdot 26^4 + 18 \cdot 26^3 + 18 \cdot 26^2 + 8 \cdot 26 + 5 = 6726413,$$

$$\textbf{ragea} = 17 \cdot 26^4 + 0 \cdot 26^3 + 6 \cdot 26^2 + 4 \cdot 26 + 0 = 7772752.$$

Now enciphering is accomplished by the following where each congruence is understood to mean modulo n*:*

$$8808592^7 \equiv 56806804; \quad 2884402^7 \equiv 65895615; \quad 7833505^7 \equiv 45842787;$$

$$2155612^7 \equiv 43647783; \quad 216795^7 \equiv 123817334; \quad 6726413^7 \equiv 110825702;$$

$$\textit{and} \quad 7772752^7 \equiv 48882513.$$

Then Alice converts to 6*-digit, base* 26 *integers and produces ciphertext via Table 5 as follows.*

$$56806804 = 4 \cdot 26^5 + 20 \cdot 26^4 + 8 \cdot 26^3 + 1 \cdot 26^2 + 19 \cdot 26 + 2 = \textbf{EUIBTC}.$$

$$65895615 = 5 \cdot 26^5 + 14 \cdot 26^4 + 5 \cdot 26^3 + 4 \cdot 26^2 + 18 \cdot 26 + 19 = \textbf{FOFEST},$$

$$45842787 = 3 \cdot 26^5 + 22 \cdot 26^4 + 8 \cdot 26^3 + 6 \cdot 26^2 + 20 \cdot 26 + 3 = \textbf{DWIGUD},$$

$$43647783 = 3 \cdot 26^5 + 17 \cdot 26^4 + 13 \cdot 26^3 + 9 \cdot 26^2 + 18 \cdot 26 + 23 = \textbf{DRNJSX},$$

$$123817334 = 10 \cdot 26^5 + 10 \cdot 26^4 + 24 \cdot 26^3 + 17 \cdot 26^2 + 19 \cdot 26 + 4 = \textbf{KKYRTE},$$

$$110825702 = 9 \cdot 26^5 + 8 \cdot 26^4 + 13 \cdot 26^3 + 13 \cdot 26^2 + 9 \cdot 26 + 0 = \textbf{JINNJA},$$

$$48882513 = 4 \cdot 26^5 + 2 \cdot 26^4 + 25 \cdot 26^3 + 5 \cdot 26^2 + 10 \cdot 26 + 17 = \textbf{ECZFKR},$$

which Alice sends to Bob who may decipher using his private key d. The reader may verify this by doing the computations.

The *RSA Conjecture* says that cryptanalyzing RSA must be as difficult as factoring the modulus. However, there is no known proof of this conjecture, although the general consensus is that it is valid. The reason for the consensus is that the only known method for finding d given e is to apply the extended Euclidean algorithm to e and $\phi(n)$. Yet to compute $\phi(n)$, we need to know p and q, namely, to cryptanalyze the RSA cryptosystem, we must be able to factor n. To ensure security of RSA or any other public-key cryptosystem, we must ensure that it is properly set up. We cannot devote a discussion to this topic and the related notions surrounding it. The interested reader may consult [11].

The advantages of public-key cryptosystems are: only the private key needs to be kept secret; key pairs may be used without change in most cases over long periods of time; in a multi-user large network that does not have a key server, fewer private keys will be required with a public-key cryptosystem than with a symmetric-key cryptosystem; and no key-exchange between communicating entities is required in a public-key cryptosystem.

The disadvantages of public-key cryptosystems are that they are slower than symmetric-key, sometimes by a factor of a thousand times. Moreover, the key sizes for a public-key cryptosystem are significantly larger than those required for a symmetric-key cryptosystem. For instance, the private key in the RSA cryptosystem should be 1024 bits, whereas with a symmetric-key cipher, generally 128 bits will suffice.

Public-key cryptography, given its disadvantages, is not meant for enciphering the bulk of a given communication. In other words, public-key cryptography is not meant to replace symmetric-key cryptography, but rather to supplement it for the goal of achieving more security.

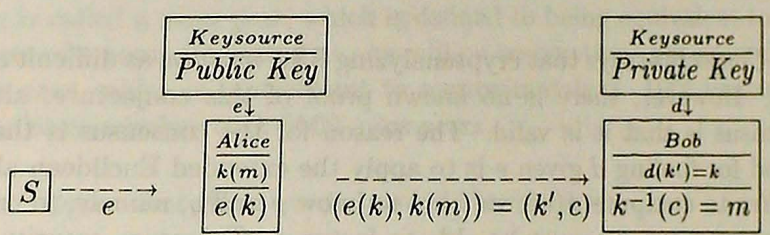
The idea behind modern cryptographic usage is to employ public-key cryptography to obtain keys, which are then used in a symmetric-key cryptosystem. Such cryptosystems are called *hybrid cryptosystems* or *digital envelopes*, which have the advantages of both types of cryptosystems. Here is how they work in practice.

Alice and Bob have access to a symmetric-key cryptosystem, which we will call S. Also, Bob has a public-private key pair (e, d). Alice wishes to send a message m to Bob. Alice first generates a symmetric key, called a *session key* or *data encryption key*, k to be used only once. She enciphers m using k and S obtaining $c = k(m)$, the ciphertext. Then Alice obtains Bob's public key e and uses it to encrypt k.

yielding $e(k) = k'$. Both of these encryptions are fast since S is efficient in the first enciphering, and the session key is small in the second enciphering. Then Alice sends c and $e(k)$ to **Bob**. Bob deciphers k with his private key d, via $d(e(k)) = k$ from which he easily deduces the symmetric deciphering key k^{-1}. Then he deciphers: $k^{-1}(c) = k^{-1}(k(m)) = m$.

Hence, the public-key cryptosystem is used only for the sending of the session key, which provides a digital envelope that is both secure and efficient — an elegant solution to the above problems.

Diagram 1 (Digital Envelope — Hybrid Cryptosystem)



Example 5 *Suppose that the symmetric-key cryptosystem, S, that Alice and Bob agree to use is a permutation cipher with $r = 6$, $\mathcal{M} = \mathcal{C} = \mathbb{Z}/26\mathbb{Z}$, and key $k = (5,2,3,1,6,4)$ from which one easily deduces the deciphering key $k^{-1} = (4,2,3,6,1,5)$. Further suppose that Alice wants to send $m =$* **quiver** *to Bob, who has set up his RSA keys as follows. He chooses $n = pq = 1759 \cdot 5023 = 8835457$, with public key $e = 11$, and private key $d = 802607$ determined from $11d + \phi(n)x = 11d + 8828676x = 1$ with $x = -1$. Since $10^6 < n < 10^7$, then $\ell = 6$. So Alice proceeds as follows.*

She converts m to numerical equivalents via Table 5 to get $m = (16,20,8,21,4,17)$ to which she applies k to get

$$c = k(m) = (4,20,8,16,17,21).$$

She then proceeds to encipher k using Bob's public key as follows.

Since $\ell = 6$, then we may encipher the key k as a 6-digit, base 10 integer:

$$k = 5 \cdot 10^5 + 2 \cdot 10^4 + 3 \cdot 10^3 + 1 \cdot 10^2 + 6 \cdot 10 + 4 = 523164. \tag{1}$$

She then enciphers k as

$$k' = k^e = 523164^{11} \equiv 6013077 \pmod{8835457},$$

and sends the pair $(k', c) = (k^e, k(m))$ to Bob. Bob receives the pair and makes the following calculations.

He computes $(k')^d = (k^e)^d = k^{ed} \equiv k \equiv 523164 \pmod{n}$. He then converts this back to its original format via (1), and is able to easily deduce k^{-1} which he applies to c to get

$$k^{-1}(k(m)) = m = (16,20,8,21,4,17) = \textbf{quiver}.$$

For the sake of brevity, we have not included some of the modern-day notions that are of importance such as *public-key infrastructure* (PKI) which embodies a foundation of protocols and standards that support and enable the secure and transparent use of public-key cryptography, particularly in applications requiring the use of public-key cryptography. For an entire book dealing with PKI see [2], and for a brief overview, see [11]. Moreover, there are numerous applications involving the use of public-key cryptography and hybrid cryptosystems that we do not have the opportunity to tackle here such as *nuclear test ban treaty compliance* (see [11, Chapter 9]), secure transmission of electronic data (including e-mail), wireless security, smart cards, and biometrics, to mention a few.

As we begin a new millennium, the effects of cryptography on our everyday lives will only increase since we are in the midst of a revolution in information processing and telecommunications. To ever increasing depths, our lives are impacted on a daily basis by interactions that require our sending of digital messages through cyberspace. This may involve the electronic transfer of digital dollars, the sending of personal "e-mail" messages, or the sending of military secrets. What is common to all these types of message-sending is the need to keep these messages secret, and ensure that nobody tampers with the message. Hence, the importance of cryptography to our information-based society will only deepen in the new millennium. It is essential that we are equipped with the knowledge to understand and deal more effectively with the new reality.

Acknowledgments: The author's research is supported by NSERC, Canada grant # A8484.

References

[1] F. L. Bauer, **Decrypted Secrets**, Springer, Berlin (1997).

[2] C. Adams and S. Lloyd, **Understanding Public-Key Infrastructure**, New Riders Publishing, Indianapolis, Indiana (1999).

[3] D. Atkins, M. Graff, A.K. Lenstra, and P.C. Leyland, **The magic words are SQUEAMISH OSSIFRAGE** in **Advances in Cryptology**, ASIACRYPT '94, Springer-Verlag, Berlin, LNCS **917**, (1995), 263–277.

[4] C.C. Cocks, **A note on "non-secret" encryption**, GCHQ/CESG publication, November 20 (1973), 1 page.

[5] W. Diffie and S. Landau, **Privacy on the Line — The Politics of Wiretapping and Encryption**, MIT Press, Cambridge (1998).

[6] J.H. Ellis, **The possibility of secure non-secret digital encryption**, GCHQ CESG publication, January (1970), 7 pages.

[7] J.H. Ellis, **The history of non-secret encryption**, GCHQ-CESG publication (1987), 4 pages.

[8] D. Kahn, **The Codebreakers**, Macmillan, New York (1967).

[9] A.K. Lenstra and M.S. Manasse, *Factoring by electronic mail*, in **Advances in Cryptology**, EUROCRYPT '89, Springer-Verlag, Berlin, LNCS **434** (1990), 355–371.

[10] R.A. Mollin, **An Introduction to Cryptography**, Chapman and Hall/CRC Press, Boca Raton, New York, London, Tokyo (2001).

[11] R.A. Mollin, **RSA and Public-Key Cryptography**, Chapman and Hall/CRC Press, Boca Raton, New York, London, Tokyo (2002).

[12] B. Schneier, **Applied Cryptography**, Wiley, New York, Toronto (1994).

[13] S. Singh, **The Code Book**, Doubleday, New York, London, Toronto (1999).

[14] C. Suetonius Tranquillus, **The Lives of the Twelve Caesars**, Corner House, Williamstown, Mass. (1978).

[15] Unknown author, **Final report on project C43**, Bell Telephone Laboratory, October (1944), p. 23.

[16] M.J. Williamson, **Non-secret encryption using a finite field**, GCHQ-CESG publication, January 21 (1974), 2 pages.

[17] M.J. Williamson, **Thoughts on cheaper non-secret encryption**, GCHQ-CESG publication, August 10 (1976), 3 pages.