

# Codes and Ciphers in History

Derek J. Smith

Copyright Notice: This material was written and published in Wales by Derek J. Smith (Chartered Engineer). It forms part of a multfile e-learning resource, and subject only to acknowledging Derek J. Smith's rights under international copyright law to be identified as author may be freely downloaded and printed off in single complete copies solely for the purposes of private study and/or review. Commercial exploitation rights are reserved. The remote hyperlinks have been selected for the academic appropriacy of their contents; they were free of offensive and litigious content when selected, and will be periodically checked to have remained so. Copyright © 2003-2008, Derek J. Smith (Chartered Engineer).

First published 08:05 GMT 28th January 2003; this version [1.2 - correction] 08:30 BST 8th April 2008

## Codes and Ciphers in History, Part 1 - To 1852

Definitions: Singh (1999) explains that a code involves replacing sensitive words or phrases with different words, phrases, numbers, or symbols, whilst a cipher involves making letter-for-letter substitutions, according to a pre-set rule. Thus a spy might be given the codename "Intrepid", which could be ciphered as JOUSFQJE. Needless to say, it is possible (a) to decipher the cipher and still not be able to decode the code, and (b) to cipher the same codename an infinite number of different ways. "Cryptology" is the overarching science of codes and ciphers, "cryptography" is the specific science of encryption, that is to say, encoding and enciphering, and "cryptanalysis" is the specific science of hostile decryption, that is to say, unwanted decoding and deciphering.

### Early Codes and Ciphers

**"When you attack, your opponent should not know what to defend, for when he does not know what to defend, he must defend thinly, to your advantage; and when you defend, your opponent should not know what to attack."** (Loosely from Sun Tsu, "The Art of War".)

**"A quick peek is worth two finesses."** (Unwritten rule of (very) coarse contract bridge.)

The use of codes and ciphers to maintain personal, amatory, political, or military secrecy goes back to the beginnings of history, and the overriding lesson is that no written form of communication will ever be totally secure. Letters can be stolen from (or by) their carrier, or - and the practical implications of this are actually far worse - their contents scanned by a "black chamber", an interception point where mailings are systematically opened, copied, and resealed for onward transmission.

It was to prevent this sort of leakage of information that the Egyptians and the Greeks, etc., developed various forms of secret writing [for details of the Spartan scytale, [click here](#)], and the Romans experimented with both invisible ink and the "substitution cipher". This latter technique was made famous by none less than Julius Caesar himself. The "Caesar shift" is a ciphering method fit for little more than the school playground, and involves replacing each plaintext letter with the letter a known number of places further up the alphabet.

Now the problem with Caesar shift ciphers is that not all letters of the alphabet occur with equal frequency. The commonest letters in written English are E, T, and A, so if your ciphertext is suddenly full of Js, Ys, and Fs, you can start to make some easy guesses at the shift key used. One of the first steps in practical decryption is accordingly to build up a letter frequency profile of the ciphertext. To be a cryptanalyst, in other words, you need to be methodical, and the first "scientific" approaches to

# Codes and Ciphers in History

Derek J. Smith

cryptology emerged during the ninth century Muslim caliphates. Encryption and decryption techniques were common practice in the Middle Eastern civil services, and Singh (1999) credits a certain Abu Al Kindi as the first cryptanalyst worthy of the name.

The Arabian techniques eventually spread westwards into Europe, and monks such as Roger Bacon were soon using a whole variety of methods to protect the Church's internal deliberations. Modern international diplomacy was born in Venice in the thirteenth century (Deacon, 1980), but its communication techniques were never totally secure, and it only takes a few powerful people to have their favourite methods of cryptography broken, for the call to go out for better techniques and a more reliable class of messenger. One improved technique was devised by the Florentine architect Leon Alberti (1404-1472) in around 1466. This made use of two cipher alphabets simultaneously, so that high frequency cipherings from one balanced with low frequency cipherings from the other. Properly handled, the resulting ciphertxts were suddenly much less vulnerable to frequency analysis. As for the quality and reliability of the messengers themselves, the first military postal service in Britain was established as the "Royal Post" in 1482 (Cuerden and Fenwick, 2002 online), and their courier service gradually evolved into the civilian Post Office.

Alberti also invented the "cipher disk" [picture] as a way of semi-automating a rotary version of the Caesar shift. This is how Alberti described his invention:

"I make two circles out of copper plates. One, the larger, is called stationary, the smaller is called movable. The diameter of the stationary plate is one-ninth greater than that of the movable plate. I divide the circumference of each circle into 24 equal parts [called] cells. In the various cells of the larger circle I write the capital letters, one at a time in red, in the usual order of the letters [whilst those around the movable circle are] not in regular order like the stationary characters, but scattered at random. [I then] place the smaller circle upon the larger so that a needle driven through the centres of both may serve as the axis of both and the movable plate may be revolved around it." (Alberti, 1470, cited in Kahn, 1996, pp127-128.)

Kahn attaches great historical significance to what Alberti did next, because at a single stroke it overcame the Caesar shift's weakness. This is how Alberti explained himself:

"After writing three or four words, I shall change the position of the index in our formula by turning the circle, so that the index k may be, say, under D and all the other stationary letters will receive new meanings." (Alberti, 1470, cited in Kahn, 1996, pp128-129.)

This little trick turned the cipher disk into a "polyalphabetic substitution cipher", with as many separate alphabets at its disposal as there are radial positions on the disk. Another advantage of the cipher disk is that it was easy to operate, and therefore attractive to organisations such as diplomatic services, monastic orders, and the military, where the menial task of ciphering and deciphering tended even then to be left to secretaries and juniors rather than being done personally by principals. Alberti's cipher disk lived on to become the basis of the "cipher cylinder" (see Part 3 of this historical review). Cryptoworks from this general period include the monk Johannes Trithemius's "Steganographia" (ca. 1500).

## Tudor Cryptology

BACKGROUND: After the fall of the Roman Empire, a number of separate kingdoms - England, Scotland, Ireland, and Wales - emerged within the British Isles. These remained politically separate until England and Wales merged by Act of Union in 1536, to form the first "United Kingdom". Scotland joined the union in 1707, and Ireland in 1801. Strictly speaking, the modern Welsh have prior claim to the term "British" since they were the ethnic "Ancient Britons", and because the word derives from the

# Codes and Ciphers in History

Derek J. Smith

ancient Celtic name for the British Isles, namely "Prydain". Throughout this paper we use the terms "Britain" and "British" to refer to the members of the UK at the time in question.

The Tudor Age of British history began with the accession to the throne of Henry VII in 1485. The throne had already been bitterly fought over for political reasons during the Wars of the Roses (1455-1487), but these disputes reached new heights of intensity when the catholic-protestant religious schism came along as well. The Protestant Reformation, the gradual rejection of papal authority across north-western Europe, had its historical roots in the 14th century with churchmen such as John Wycliffe and Jan Hus, and began in earnest with Martin Luther in Saxony in 1517. The struggle was then taken up by the Calvinists in Switzerland, the Huguenots in France, John Knox's presbyterians in Scotland, and the Puritans in England (the movement which gave rise to the Pilgrim Fathers). As a result, relations between Britain and catholic Europe were often less than cordial, and written communication required some form of cryptological protection. Thus it was, for example, that Cardinal Wolsey (ca. 1471-1530), chaplain to Henry VII until his death in 1509 and thereafter long-time favourite of his son Henry VIII, used a form of shorthand cipher when at Venice in 1524.

Venice was a particular problem, in fact, because several centuries of remorseless mercantile and military adventurism had raised the status of the Venetian city-state within the Roman Catholic world to that of empire-in-miniature, and in controlling the trade routes Venice also controlled the world's mail services. The city was one big black chamber. Phau (1994/2003 Online) refers to the deliberate and cynical exercise of state power which brought the Venetians this success as "The Methodology of Evil". Here is how he describes "the Venetian method":

"Above all, the evil that was Venice was seen by her contemporaries in her manipulation of events and individuals through conspiracy and deceit: a kind of modern pioneer in religious warfare, espionage, and diplomatic warfare. The character of Iago in [Shakespeare's Othello] is perhaps the best case-study of the Venetian method. Intimate adviser, apparent friend, and comforter to Othello - a Moorish general retained to defend Venice - Iago [plays] upon the Moor's latent jealousies until Othello is driven to madness. It is an open question whether Shakespeare intended to evoke in the character of Othello the character of Henry VIII [but] whether he intended it or not, the resemblance between the [two] is there."

A major coalition of nations - the League of Cambrai - had rounded on Venice in 1508, and had done much to reduce her influence, but the Venetian Grand Council still ruled "with the help of an elaborate network of agents and informers" (Phau, op.cit.). Phau continues that there are a million and a half ambassadorial despatches in the Venetian state archives, "with many documents in cipher and probably in invisible ink, which Venice was first to patent", and a selection of Henry's correspondence from this period, both en clair and ciphered, is available in Tim Coates' "The Letters of Henry VIII, 1526-1529" (Coates, 2001).

The Venetian experience was excellent training for Wolsey's secretary, the lawyer Thomas Cromwell (1485-1540), standing him in good stead when he started to pursue his own career in Henry's court after Wolsey's death in 1530. He rose rapidly through the ranks of Henry's advisors, soon acquiring responsibility for the king's counterespionage service, and raising it to Venetian levels of ruthless efficiency: "No knavery," reported one of his agents in 1535, "can be hid from us" (Richard Layton, Archdeacon of Buckingham, cited in Deacon, 1980, p18). He was also continuing the Venetian tradition in 1536, when he masterminded the intrigues which led to the execution of Henry's second wife, Anne Boleyn, on hastily contrived charges of incest and witchcraft.

The Anne Boleyn affair earned Cromwell no little favour at court, because Henry's next wife, Jane Seymour (ca. 1504-1537), whom he married the day after Anne's execution, soon bore him his long-

# Codes and Ciphers in History

Derek J. Smith

sought-after legitimate male heir, Edward. Sadly, Jane died a few hours after giving birth, and it was when Cromwell set about finding Henry his fourth wife that he started to make mistakes. Cromwell decided that the protestant Anne of Cleves was the girl to go for, and after prolonged negotiations she arrived in Britain in December 1539. The standard story then has it that she was so "utterly destitute both of beauty and grace" (Hume, 1786, p11:190) that Henry could not stomach consummating the union. Cromwell did not get the blame straight away, and was elevated to the peerage in April 1540 as the Earl of Essex. His celebrating did not last long, however, for the rumour suddenly spread that he had deliberately concealed Anne's physical failings from the king during the royal courtship, whereupon Henry's temper snapped and Cromwell was immediately confined to the Tower of London, where he was beheaded 28th July 1540.

Henry died in 1547, and was succeeded by the boy-king Edward VI, still only nine years old, and as was standard practice in such circumstances a succession of "Protectors of the Realm" were appointed to exercise power on his behalf until he came of age. Unfortunately, Edward was a sickly child and when he died in 1553 the catholic Mary Tudor (1516-1558), Henry's daughter by his first wife, Catherine of Aragon, took his place. She, too, died young (but not before earning the nickname "Bloody Mary" for some anti-protestant excesses), but with her death came stability as her half-sister Elizabeth (1533-1603) began a reign that would span 45 years. Cryptoworks from this general period include Giambattista della Porta's "De Furtivis Literarum Notis" (1563).

Elizabeth's smooth accession to the throne was in certain key respects greatly assisted by the lawyer William Cecil (1520-1598), and his subsequent advancement under Elizabeth was accordingly rapid. He took over the queen's espionage service in 1558 when he was made Secretary of State, was elevated to the peerage as Lord Burleigh in 1571, and was one of the prime movers for the prosecution in the case of Mary, Queen of Scots. The central problem here was that the Roman Catholic church had traditionally refused to recognise divorce, and so regarded Henry VIII's first marriage (to Catherine of Aragon) as sacrosanct. Elizabeth, daughter from his second marriage (to Anne Boleyn) was therefore not truly legitimate, and the true monarch in catholic eyes was actually a slightly more distant relative, Mary Stuart (1542-1586), who had been Queen of Scotland since before her first birthday. Mary had spent her early life at the court of King Henry II of France, marrying his son Francis in 1558, and becoming Queen of France when the old man died in 1559. Yet in 1558, Mary was guilty of no more than considering her own claim to the vacant English throne, and in the end no challenge was made. Nevertheless, Elizabeth had been made sensitive to her rival's existence, and when Mary moved from France back to Scotland in 1561 she began to sense a more direct threat. She therefore arranged to have Mary routinely spied upon.

Mary's time in Scotland was eventful enough [fuller story] to force her in 1568 to seek refuge in northern England, but, fearful of her intentions, Elizabeth took this opportunity to have her placed under house arrest. And there she stayed, an embarrassment and irritation to the throne, until evidence of her involvement in a treasonous plot emerged in October 1586. Here is how Hume (1786, p11:486) described what happened next:

"Her two secretaries were immediately arrested; all her papers were seized, and sent up to the council; above sixty different keys to cyphers were discovered; there were also found many letters from persons beyond the sea, and several too from English noblemen, containing expressions of respect and attachment."

It soon transpired that Mary had been conducting a prolonged exchange of messages with a co-conspirator named Anthony Babington, ciphering them, and then hiding them in the hollowed out bungs of barrels going in and out of her kitchens. Now in 1573 Burleigh had passed the secret service job on to Sir Francis Walsingham (ca. 1530-1590), and the intervening years had been cryptologically

# Codes and Ciphers in History

Derek J. Smith

highly active. The Babington correspondence was discovered by a black chamber set up by Walsingham, and their substitution cipher [picture] broken by his clerk Thomas Philips (sometimes Phelippes) using the method of frequency analysis. Hume (1786, p11:467) describes Walsingham's intelligence techniques as follows:

"..... many arts, which had been blameable in a more peaceful government, were employed in detecting conspiracies, and even discovering the secret inclinations of men. Counterfeit letters were written in the name of the Queen of Scots, or of the English exiles, and privately conveyed to the houses of the catholics; spies were hired to observe the actions and discourse of suspected persons; informers were countenanced; [and] all the subjects, particularly the catholics, kept in the utmost anxiety and inquietude."

It was Walsingham again, who in 1587 obtained warnings that Philip II of Spain was preparing for an invasion of Britain. Using his contact network to subvert Philip's bankers, he managed to delay that invasion for a year, and then, in the opening months of 1588, he proceeded to neutralise the many Spanish spies in Britain, thus rendering Philip's approaching Armada effectively blind (McKee, 1963).

ASIDE: The next time a British intelligence blackout was as absolute was not until 1944, in the run-up to the D-Day landings. Nor was Britain alone in her paranoia, for the rest of Europe was equally jumpy. The catholic states lived in constant fear of the Venetian informers, or the Borgias' Inquisitors, or the Jesuits, whilst the first Tsar (Ivan "the Terrible") had just established Russia's first secret police force, the Oprichnina (Casey, 2002 online). The Oprichnina were not the first to combine intelligence gathering with a murderous hands-on enforcement policy, but they were perhaps the most stylish, sporting an all black livery and cryptic logo. Not surprisingly, it was an age in which the ancient secret societies (Cabbalists, Knights Templar, etc.) were reborn, and new ones (Freemasons, Rosicrucians, and the Italian Carbonari) spawned.

Mary Stuart was eventually executed in 1587, just fractionally too late to benefit from one of the most secure encryption systems yet, namely the Vigenère Square. This technique was developed in the mid-16th century by Blaise de Vigenère (1523-1596), a French diplomat, and published in "A Treatise on Ciphers" (1586). The method requires that a fully exhaustive vertical array of Caesar shift alphabets is drawn up, each line of which is one place further offset than the one above it [details]. Regardless of the particular national alphabet being considered, this table will always be as deep as it is wide, and the secret is to use only a key-controlled subset of it: you simply have to use different subsets of lines (those beginning K-I-N-G, say) on different occasions, according to prior agreement between sender and receiver, and each line encrypts a different subset of the plaintext (every fourth letter, say). So proud was Vigenère of his invention, that he confidently dubbed it "le chiffre indechiffirable"; believing that it could not (to use the modern technical term) be "broken back" (in the fullness of time, it was broken, of course - by the same Charles Babbage who first popularised the notion of automated computing). To play with your own Vigenère Square online, [click here](#).

## Early Stuart Cryptology

Elizabeth I remained childless, and so her death in 1603 brought an end to the Tudor lineage. This immediately reopened all the old squabbles, and the entire seventeenth century was a period of no little unhappiness for the British crown; a period of rebellions, civil war, and invasions. Not surprisingly, cryptological knowledge remained at a premium, and relevant works from this general period include Francis Bacon's "The Advancement of Learning" (1623) and John Wilkins's "Mercury: Or the Secret and Swift Messenger" (1641).

To start with, the crown passed to James I (I of England, VI of Scotland; 1566-1625), son of the unfortunate Mary Stuart .....

# Codes and Ciphers in History

Derek J. Smith

ASIDE: As already noted, Scotland did not join the United Kingdom until 1707. Note how this confuses the numbering of common monarchs.

..... and one of the most important figures in the ensuing generation was Sir Henry Wotton (1568-1639). Wotton had trained as secretary to Robert Devereux, Earl of Essex, and had to spend some years abroad in self-imposed disgrace after the latter had intrigued himself to the block in 1600. He took a job in Italy working for the Duke of Florence, and in 1602 his luck changed for the better when the Duke intercepted letters plotting against the life of James VI. Wotton was given the task of carrying a warning to Scotland [fuller story] and was thus an instant court favourite when James VI inherited the throne of England the following year. His reward was to be made British ambassador to Venice from 1603, and in that role he inherited a spying agency developed in the 1590s by the same Thomas Philips who had cracked the Babington cipher (Deacon, 1980) (he also coined the famous definition of an ambassador as being "an honest man sent to lie abroad for the good of his country"). Wotton received a special allowance to cover the bribes and inducements needed for effective secret service work (funding which he supplemented by selling on spare secrets to other governments). This is how Deacon (op. cit., p55) describes his work:

"He gave the Venetian Government intelligence about the Jesuits' activities at the same time that he passed it on to James I. He set up agents in Rome, Turin, and Milan as well as in Venice and robbed the posts and stole the Jesuits' correspondence. His organisation was superb, for he made a study of the seals used by the Jesuits on their mails [and] once he had intercepted the packets, read the contents and had them copied, he allowed the mails to go to the addresses intended."

However, on occasions he must have wondered why he was bothering, because the king seems to have been by nature an inveterate gossip, and freely shared his thoughts with the Spanish Ambassador in London (Deacon, op. cit.). Indeed, James was once described as "the wisest fool in Christendom, by reason of his strange blend of genuine far-sighted wisdom and naivete.

The early Stuarts were not a match for the French either, for France's Cardinal Richelieu (1585-1642) was running a much tighter ship, and it is to France that we have to turn for the next major cryptological milestone. Kahn (1996) begins this story at the Siege of Réalmont in 1628, where a force of Huguenot rebels had been besieged by an army led by Henry II of Bourbon. As supplies within the town began to run down, the defenders sent out a ciphered message for help. The courier was duly intercepted, but the cipher initially defied Henry's resident cryptanalysts. Henry then learned of a young local named Antoine Rossignol, with something of a reputation in this area. Rossignol was duly summoned, and broke the code at once, revealing that the defenders were far less well supplied than the ferocity of their initial defence had indicated. Henry simply returned their message to them, together with a copy of the decryption, and the town surrendered without further ado.

The Réalmont affair made Rossignol famous overnight, and over the next few years he was of repeated service to Richelieu against other Huguenot strongholds. He also improved the nomenclators used by the French court for their own despatches. His son Bonaventure was introduced to the profession by his father, and together they developed the Great Cipher (aka "Le Grand Chiffre de Louis XIV" or "le chiffre indechiffable") (see next section but one).

## English Civil War (1642-1651) Cryptology

The English Civil War began in 1642, following more than a decade of deteriorating relations between the monarchy, now in the person of King Charles I (1600-1649), and parliament. The forces loyal to Charles - the "Royalists" (colloquially, "Cavaliers") - attracted monarchists at heart, from backgrounds which were typically rural, upper class, catholic, Scottish, Irish, and Welsh. The armies loyal to parliament - the "Parliamentarians" (colloquially, "Roundheads") - attracted less flamboyant stock,

# Codes and Ciphers in History

Derek J. Smith

from backgrounds which were typically puritan protestant, urban, and English. The cryptology, however, did not take sides, and there was widespread use of ciphers and codes as the fighting ebbed and flowed across Britain. Oliver Cromwell's Parliamentarians chose well when they selected John Thurloe (1616-1668), an Essex lawyer, as their spymaster. Thurloe was made Postmaster General, and set up "the most effective espionage network since the days of Francis Walsingham" (source), making him by one report the second most powerful man in Britain. One branch of his strategy was for the Parliamentarians to create their own black chamber - called the "Secret Office" - within the Post Office, and another was to get the best available cryptanalyst on their side, in the person of John Wallis (1616-1703), the greatest English mathematician before Newton (Kahn, 1996, p166) (they approached Wallis rather than the rival cryptologist John Wilkins, Cromwell's own brother-in-law, because the latter harboured some Royalist sympathies). Wallis acted as chief cryptanalyst for Cromwell from 1643, and so good was he at the job, that when Charles II ascended the throne at the end of the interregnum, he kept him in it!

Royalist cryptography did at least secure the escape of Sir John Trevanion from a Roundhead death row in Colchester Castle, Essex. Despite being under constant guard, and with all his correspondence being carefully scrutinised, friends on the outside managed to get a message through to him. They sent him an apparently innocuous letter, which his jailers could find no immediate fault with, yet while at prayer that evening Sir John disappeared into thin air from inside the chapel. Only later was it discovered that the letter had in fact contained a message within a message. The visible message read as follows:

"Worthie Sir John, Hope, that is the beste comfort of the afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to [etcetera]" (Deacon, 1980, pp59-60.)

The secret was that the third character after each punctuation mark conveyed the following far more pressing message: "Panel at east end of chapel slides"! This is an instance of "steganography" (Greek = "hidden writing"), the science of invisible inks and general message concealment. Cryptoworks from this general period include John Wallis's "A Collection of Letters and Other Papers in Cipher" (1653).

## The Great Cipher of Louis XIV

Even as King Charles I's head was rolling from the executioner's block, the French King Louis ("L'état c'est moi") XIV (1638-1715) was coming of age. Louis XIII had died in 1643, when XIV was still only five years old, so his mother, Anne of Austria, acted as regent until he came of age in 1651. However, the "Sun King" only really came into his own with the death of his chief minister, Cardinal Mazarin, ten years later. There followed a period of the most intense international intrigue, even for those times, as the various European dynasties strove to settle issues such as Bourbon versus Habsburg, Rome versus Venice, and protestant versus catholic. Over the ensuing four decades, Louis fought four wars to further the glory of France. The first of these (1667-1668) was against Spain, the second (1672-1678) was against Holland, Spain, and Austria, the third (1688-1697) was against the "League of Augsburg" (Britain, Austria, Spain, Holland, and much of what is today Germany), and the fourth (1701-1714), the War of the Spanish Succession, was against just about everybody in Europe.

Cryptologically, the reign of Louis XIV is most famous for Antoine and Bonaventure Rossignol's development of the Great Cipher. Here is how Singh (1999, pp55-56) tells it:

"The Great Cipher was used to encrypt the king's most secret messages, protecting details of his plans, plots, and political schemings. [It] was invented by the father-and-son team of Antoine and

# Codes and Ciphers in History

Derek J. Smith

Bonaventure Rossignil [and] was so secure that it defied the efforts of [.....] generations of codebreakers."

It was so good, in fact, that when the Rossignols died, its secret died out with them, and nobody could re-crack it until Etienne Bazeris in the closing years of the nineteenth century.

Cave Beck in 1657 and Athanasius Kircher in 1663 had also broadened the horizons of cryptological theory with their respective "universal languages". These were numerically indexed all-encompassing dictionaries - "pasigraphies" - which in Kircher's case consisted of 1048 clusters of synonyms and near-synonyms, organised under 32 major headings (note these numbers). It was thus not dissimilar to the modern Roget's Thesaurus. Such systems both allow and encourage cryptological applications because they provide a ready-made, and by definition comprehensive, numerical code book. The diaries of Samuel Pepys (1659-1669) were also written in a shorthand cipher of this type, partly to save paper, and partly to keep them from prying eyes, not least (and with good reason) his wife's. They were not published until 1825, because nobody could work out the encryption system he had used.

Beck and Kircher may well have been on to something. In Smith (1997b), you will find a short section entitled Max Müller and the Search for Semantic Absolutes. In it, we described yet another pasigraphy, that of the nineteenth century linguistic philosopher, Max Müller. Here is the relevant background .....

"[Max Müller] was one of the first to recognize that word meanings are constantly evolving, and spent a lifetime studying the etymologies of words in a variety of languages with a view to tracking down their derivations (Müller, 1887). Working in this way, he reduced all languages to much smaller pools of word roots and fundamental concepts. To give but one example, the Greek words for lift, compare, tribute, spread, delay, bury, madness, endure, recover, reproach, help, and excel (to name but a few) all derive in various ways from  $\square \square \square$ , 'to bear'. Müller's central argument goes as follows: 'Give us about 800 roots, and we can explain the largest dictionary; give us about 121 concepts, and we can account for the 800 roots. Even these 121 concepts might be reduced to a much smaller number, if we cared to do so.' (op. cit., p551.) [and] Saban (1993) chooses 31 basic 'semantic fields'." (Smith 1997b, p204.)

In other words, different pasigraphies have no trouble working to core dictionaries of wildly different sizes. However, we then suggested that the various numbers might not be so different after all .....

"..... to be precise, they might just represent three points on the powers of two dimension. That is to say, we need five bits of information to specify a single one of Saban's 31 semantic fields, seven bits of information to specify a single one of Müller's 121 original concepts, and ten bits of information to specify a single one of Roget's 1000 related ideas." (Smith 1997b, p204.)

And to explain this possible pattern, we suggested that human conceptual memory might somehow operate according to a "binary chop" principle [technical details], so that the natural size of a given pasigraphy would always be a power of two (that is to say, 16, 32, 64, 128, 256, 512, 1024, 2048, and so on), or roughly so.

## The Golden Age of Conspiracy, I - The Wars of Succession

Back across the English Channel, Britain remained in the grip of religious confrontation. When Charles II died in 1685, he left no legitimate heirs, and was accordingly replaced by his brother, the catholic James II/VII, much to the chagrin of his own illegitimate son, the protestant James Scott, Duke of Monmouth. A number of armed coups were attempted, and, after a lot of bloodshed, James II was replaced by the protestant William of Orange [fuller story]. The cryptological history here is that

# Codes and Ciphers in History

Derek J. Smith

William, too, was a keen user of coded correspondence, having conspired in cipher with Admiral Edward Russell (later Earl of Orford) in 1688, prior to making his successful bid for the throne. However, no sooner had James been deposed, than his supporters across Europe began a 60-year campaign to have him (or, after his death in 1701, a suitable descendent of his) reinstated. A number of anti-protestant uprisings then took place, known collectively as the "Jacobite Rebellions" (1689-1748) (James = Jacques/Jacob in French). There were two main "Pretenders" to the throne, respectively, James III/VIII and Charles Edward Stuart ("Bonnie Prince Charlie"). One of the most active conspirators in the early years was William Standish, of Standish Hall, Lancashire. He was a Jacobite sympathiser, and used a cipher in 1694 which was so cryptic that it was not broken until the 1920s (Johnson, 2002 online).

William died on 8th March 1702, having been thrown from his horse when it stumbled into a mole hole ("Hurrah for the mole", cheered the catholic opposition), and his sister-in-law, Anne, the last of the Stuarts, took over. When she died heirless in 1714, the nearest acceptable protestant was George, Prince of Hanover, and he was crowned George I of Britain on 20th October 1714. His great-grandson, George III (see under American Revolution below) was therefore also a Hanover, as was Queen Victoria in her turn until she became a Saxe-Coburg-Gotha (since anglicised as Wind-sor) upon her marriage to Prince Albert in 1840. This reassertion of protestantism naturally infuriated the Jacobite opposition, and there were major uprisings in 1715, 1719, and 1745. The full cryptohistory of this period is told in Hugh Douglas's "Jacobite Spy Wars" (1999), although there is online coverage of Thomas Southcott's correspondence as the principal Jacobite fundraiser in England, in which he used codenames for both proper names and nouns (Scott, 2002 online).

## **The Golden Age of Conspiracy, II - The Wars of Secession**

The next cryptologist of note (not to say downright notoriety) was Sir Francis Dashwood (1708-1781; from 1763, Lord le Despencer), a larger than life character, who managed to combine his spying and cryptology with diversions such as gambling, devil worship, and debauchery (by virtue of which, Knowles, 2002 online, dubs him "the rogue of his day"). It so happened that mid-eighteenth century Britain was an age of "clubmanship", a period in which the nobility indulged their darker passions behind the closed doors of each other's mansions. Such clubs went by the generic name "hell-fire clubs", and Dashwood's was a hell-fire club extraordinaire. Its members called themselves the "Friars of St Francis of Wycombe", and they celebrated either in some underground workings at West Wycombe House, Buckinghamshire [picture], Dashwood's family seat, or at Medmenham Abbey a few miles away (where the motto over the entrance was an alluring "Do As You Will"). Their interests were "sex, drink, food, dressing up, politics, blasphemy, and the occult" (Knowles, op. cit.), not to mention applied cryptology, the key to not getting caught doing any of the others. And spying. Only 13 men formed the "inner order", namely "the Abbot" - Despencer himself - and 12 "Apostles", who included, over the years, such personages as the Prince of Wales, the Duke of Queensbury, the Earl of Bute (later Prime Minister), Sir John Montague (1718-1792) (Fourth Earl of Sandwich, who according to legend invented the snack named after him to save having to waste time away from Dashwood's card table), John Wilkes (the reformer), and William Hogarth (the painter). A baboon was dressed up as a chaplain during selected revelries, and the estate boasted a well-stocked library of pornography, including one of the earliest translations of the Kama Sutra (Knowles, op. cit.). [The bare bones of this story have been written into a number of (usually pretty poor) movie plots, including the 1960 Peter Cushing offering, "The Hell Fire Club".]

As to the cryptology, Dashwood has been reported as both Crown and Jacobite agent in the 1740s, but was in truth probably a double agent for the Crown (Deacon, 1980). Certainly, by catering to the lusts of powerful people he made powerful friends, serving as Chancellor of the Exchequer for a few months in 1762, and as Postmaster General - de facto controller of the British black chambers,

## Codes and Ciphers in History

Derek J. Smith

remember - from 1766 to 1781, and it was in this latter role that he was visited in 1773 by the American Deputy Postmaster General, Benjamin Franklin (1706-1790).

Which brings us to the American Revolution (1775-1783). We begin this story back in 1748, when the same Benjamin Franklin published a book on codes and ciphers by one George Fisher. Thereafter, he both applied the known techniques within his circle of acquaintances, and further developed the science by inventing the "homophonic substitution cipher" [details] in 1781. But Franklin's acquaintances, of course, included many prominent colonial dissidents, and as a major public figure needing to communicate privately with correspondents over long distances, Franklin was a regular user of encryption methods. Indeed, it has since become a point of modern US law that "cryptographic systems [aided Franklin's] correspondence and that of fellow patriots" (Bernstein, 1997).

So why was Franklin so interested in Dashwood? Here is Deacon (1980):

"Four members of [Dashwood's Hell-Fire Club] were undoubtedly mixed up in espionage and gained much of their intelligence through belonging to it. Almost certainly several of the other members were at one time or another working for British Intelligence. The four were John Wilkes, the Chevalier D'Eon de Beaumont, a French diplomat, Sir Francis Dashwood himself, and, surprisingly enough, Benjamin Franklin, the statesman and philosopher." (Deacon, 1980, p100.)

"Franklin was a regular visitor at Dashwood's home, West Wycombe House, where he stayed in the summers of 1773 and 1774. In the papers of one John Norris, of Hughendon Manor, Buckinghamshire, there is the enigmatic comment: '3 June 1778. Did this day heliograph intelligence from Dr Franklin in Paris to Wycombe'. Norris had built a 100-ft tower on a hill at Camberley, Surrey, from the top of which he used to signal and place bets by heliograph with Lord le Descencer at West Wycombe. // Franklin refers to a sixteen-day visit at Dashwood's home, West Wycombe House, in July 1772 which is significant in that it was in the months of June and July that the Chapters of the Brotherhood were held." (Deacon, 1980, pp112-113.)

The Montague Millennium website has made available some material from Cecil B. Currey's "Road to Revolution: Benjamin Franklin in England, 1765-1775" (Currey 1969), which give general background to Dashwood's creation of the Medmenham Monks, of their debaucheries, and of Franklin's part in it [read this extract]. Readers wishing to stand where Franklin once stood will be pleased to hear that tours of Dashwood's Hell-Fire Caves (complete with a waxwork Abbot in the act of toasting the devil) can be arranged.

Other major crypto-players from the period were:

Thomas Jefferson (1743-1826): Thomas Jefferson, a Virginia gentleman farmer and lawyer, drafted the American Declaration of Independence in 1776, and commonly used codes and ciphers for both Pepsian and patriotic purposes. In fact, he is often credited with inventing the "cipher cylinder". Kahn (1996) concludes that said apparatus was indeed invented by Jefferson, some time between 1790 and 1800, and describes it as being "so far ahead of its time, and so much in the spirit of the later inventions, that it deserves front rank among them" (p192). The mechanism consisted of a number of separate Alberti disks, each carrying a randomised alphabet stamped around its circumference, and drilled through at the centre. These wheels were then threaded in a predetermined order along a central spindle, and rotated so that a string of characters from the plaintext can be seen along one axial line. Any of the other 25 lines of letters can then be used as the ciphertext, and the recipient of the message can only decipher it if s/he knows both the disk sequence and the rotational positions. The process was then repeated for the next chunk of plaintext, and so on until the entire message has been processed. Gaddy (1993 online; Figure 3) provides a picture of an unidentified cipher cylinder

## Codes and Ciphers in History

Derek J. Smith

from this general period, and we meet the equipment again when we get to the late nineteenth century. Jefferson was subsequently President of the USA from 1801 to 1809.

Arthur Lee (1740-1792): Arthur Lee was born in Stratford, VA, but educated in Britain. He qualified initially as a physician, then as a lawyer. During this period, he was closely associated with one of Despencer's twelve "apostles", John Wilkes, and came to see himself as a "crusading patriot" (Rhatican, 2002 online), a political writer in support of American independence. He thus did much to turn colonial disaffection into active rebellion, referring to the British House of Commons as "the most tremendous tyranny that ever existed " (ibid.). During the revolution itself, he helped found the Committee of Secret Correspondence on 3rd June 1776, and arranged a dictionary-based cipher system to help keep that correspondence secret.

George Washington (1732-1799): George Washington was born in Wakefield, VA, and trained as a surveyor in the 1740s. He joined the Freemasons in 1752, and then had a successful military career in the French and Indian War (1754-1763), making Lieutenant-Colonel in the colonial militia at the age of only 22, and full colonel a year later. It was this combination of overt and covert standing which got him the post of Commander-in-Chief of the first Continental Army in July 1775, and it was his qualities of icy determination and attention to detail which helped the colonists prevail. After the war, he was the obvious choice to become the first president of the USA.

The revolution proper did not begin formally until July 1776, but was preceded by significant formative events such as the Boston "tea party" of 1773, the Hutchinson Affair of 1774, and the skirmishes at Lexington and Concord in 1775. When the revolution finally became a shooting war, the British spymaster was William Eden (1744-1814), later First Baron Auckland, one of George III's principal advisors. One of Eden's agents was the London/Guyana plantation owner, Paul Wentworth (1749-1793), who, having been born in New Hampshire, retained many contacts in the Americas. Eden therefore had Wentworth organise a small spy ring there, in order to monitor both political and military developments. However, the Americans gave as good as they got (and often a whole lot better). Ryan and Ryan tell the story of how Dr Benjamin Church, a Boston physician, was arrested in late-1775 for spying for the then British commander, General Thomas Gage. Church's intelligence had been material to Gage's decision to confiscate an accumulation of military contraband, an action which provoked the first major engagements of the revolution, at Lexington and Concord, on 19th April 1775. His encryption method was a monoalphabetic substitution cipher, and it was duly broken on 3rd October 1775.

George Washington's own account of the Church affair is available online in a letter to Congress dated 5th October 1775, and includes the following:

"I have now a painful tho' a necessary duty to perform respecting Doctor Church, Director General of the Hospital. About a week ago Mr Secretary of Providence [presumably Henry Ward, Secretary of State for Rhode Island] sent up to me one Wainwood [Godfrey Wainwood, a Newport baker], with a letter directed to Maj'r Cane [one of Gage's aides; Kahn identifies him as Maurice Cane; possibly 6th Regiment of Foot] in Boston, in Characters [note this quaint term], which he said had been left with Wainwood some time ago by a woman who was kept by Doctor Church; she had before prep'd Wainwood to take her to Captain Wallace [of the frigate HMS Rose, on blockade duties off Newport], Mr. Dudley the collector or George Home, which he declined; she then gave him the letter with a strict charge to deliver it to either of those gentlemen. He suspecting some improper correspondence kept the letter and after some time open'd it, but not being able to read it laid it up, where it remained until he received an obscure letter from the woman, expressing an anxiety after the original letter, he then communicated the whole matter to Mr Ward who sent him up with the papers to me; I immediately secured the woman, but for a long time she was proof against every threat & persuasion to discover

## Codes and Ciphers in History

Derek J. Smith

the author, however at length she was brought to a confession and named Doctor Church. I then immediately secured him and all his papers. Upon his first examination he readily acknowledged the letter, said it was designed for his brother Fleming [John Fleming, his brother-in-law, a Boston printer, and therefore on the British side of the lines] and when decyphered would be found to contain nothing criminal. He acknowledged his never having communicated the correspondence to any person here but the girl, and made many protestations of the purity of his intentions. Having found a person capable of decyphering the letter, I in the meantime had all his papers searched but found nothing criminal amongst them, but it appeared upon enquiry that a confidant had been among the papers before my messenger arrived. I then called the General Officers together for their advice, the result of which you will find in the inclosure No. 1. The decyphered letter is in the inclosure No. 2." (From the George Washington Papers at the Library of Congress, 1741-1799; Series 3a, sheets 53-54.)

Rafalko (2003 online) takes up the story:

"An amateur cryptanalyst stepped forward in the person of Reverend Samuel West, who happened to have been a Harvard classmate of Church. A second person, Elbridge Gerry, a member of the Massachusetts Provincial Congress and the Committee of Safety, who would later be the fifth vice-president of the United States, teamed with Colonel Elisha Porter, a colonel in the Massachusetts militia to conduct a separate cryptanalytic attack on the cipher. Church had used a type of cipher known as a monoalphabetic substitution, one of the easiest to solve. Both West and the Gerry-Porter team provided Washington with identical translations ....."

The full transcript of Church's letter is online at the Massachusetts archives [[click here](#)], and the following extract is indicative enough .....

"..... I counted 280 pieces of cannon ..... I saw 2200 men ..... Twenty tons of powder lately arrived at Philadelphia, Connecticut, and Providence ..... An army will be raised in the middle provinces to take possession of Canada ..... Make use of every precaution or I perish."

Church was duly convicted, served some months in prison at Norwich, CT, and was then lost at sea en route for a new life in the West Indies.

Eden was similarly unsuccessful in trying to thwart American attempts to secure European allies against the British. When it became known that the Americans were sending a senior delegation (Benjamin Franklin, Arthur Lee, and Silas Deane) to the French Court to begin negotiations, Wentworth quickly recruited the delegation's secretary, Edward Bancroft, (or at least he thought he had recruited him, for he was possibly a double-agent whom the Americans willingly allowed to be placed in the party specifically to spy on the British - Davidson and Lytle, 1992/2002 online).

The Franco-American negotiations began in May 1776, and the French were initially somewhat cautious: true, the British had few friends in France, where memories of the Seven Years War (1756-1763) were still fresh and raw, but equally the French could not risk siding openly with the Americans until their victory was assured. Eden was kept fully informed of the delicate negotiations by Bancroft's secret correspondence. Davidson and Lytle (1992/2002 online) explain how it was done .....

"Eventually Bancroft discovered that he could pass his information directly to the British ambassador at the French court. To do so, he wrote innocent letters on the subject of "gallantry" and signed them 'B. Edwards'. On the same paper would go another note written in invisible ink, to appear only when the letter was dipped in a special developer held by Lord Stormont, the British ambassador. Bancroft left his letters every Tuesday morning in a sealed bottle in a hole near the trunk of a tree on the south

## Codes and Ciphers in History

Derek J. Smith

terrace of the Tuileries, the royal palace. Lord Stormont's secretary would put any return information near another tree on the same terrace."

Among the matters which thereby came to light were the efforts of the French playwright-spy Pierre de Beaumarchais (with the full, but covert, blessing of the French government) to organise a fleet of some 40 vessels to traffick "no supplies whatsoever" from France to America via the Caribbean. The existence of such secret aid prior to the formal declaration of war was, of course, officially denied (CIA website), but this gun-running was material to the pivotal American victory at Saratoga in 1777. It was the third man in the delegation, Silas Deane, who did the organising in this respect, he having been included in the party at the behest of the Continental Congress's Committees (a) of Secrecy, and (b) of Correspondence (Connecticut Historical Society, 2002 online). He used at least one alias ("Timothy Jones") and used a heat-developing invisible ink made from cobalt chloride and glycerine for his reports back to America (CIA website).

ASIDE: These two committees were the colonials' de facto Foreign Office, and "..... employed secret agents abroad, conducted covert operations, devised codes and ciphers, funded propaganda activities, authorised the opening of private mail, acquired foreign publications for use in analysis, established a courier system, and developed a maritime capability apart from that of the navy. It met secretly in December 1775 with a French intelligence agent who visited Philadelphia under cover as a Flemish merchant, and engaged in regular communications with Britons and Scots who sympathised with the Patriots' cause." (CIA website.)

In the end, the well-honed conspiratorial skills of Franklin, Lee, and Deane proved the decisive factor. The British were out-thought and out-plotted, and the Franco-American Treaty was duly signed 6th February 1778, making France one of the first countries to recognise the new United States of America. For the remainder of the war French ships sailed openly (now) alongside those flying the Stars and Stripes.

ASIDE: Deacon (1980) suggests a different scenario. Benjamin Franklin, he argues, was a British agent (codename "Agent 72") from around 1772, and successfully betrayed many of Beaumarchais' blockade runners. In his analysis, the British intelligence operation in Paris was never so successful than when Franklin happened to be in town. Deane fell into disgrace in 1781 for suggesting treasonously that the US would do well to rejoin Britain, and died near London of a sudden "oppression at his stomach" on 22nd September 1789. Davidson and Lytle (1992/2002 online) suggest that Bancroft, now living reasonably comfortably in London on his spy's pension from the British government, poisoned him to prevent his own double life being revealed. The British do seem to have seen through at least one cover story, that of the soldier-turned-artist, John Trumbull (1756-1843). Trumbull was the son of Jonathan Trumbull, a friend of George Washington, and the only pre-revolutionary Governor (of Connecticut) to declare immediately for the revolution. John's brother, Jonathan Jr., was "confidential secretary to General Washington" and his brother-in-law William Williams was one of the 56 signatories to the Declaration of Independence (Office of the Curator's website, US Capitol, 1997/2002 online). John served with distinction in Washington's Continental Army, rapidly reaching the rank of Colonel, until on 22nd February 1777 - with the war still raging - he suddenly decided to give it all up to become an artist (although, fortunately for his former comrades, this new calling was not so debilitating as to prevent him assisting General Sullivan's campaign against the heavy British fortifications around Newport, RI, in high summer 1778). Two years later, he made his way to France, carrying at least one letter from Benjamin Franklin, master cryptologist. On balance of probabilities, therefore, we see little injustice in the fact that when he took his easel to Britain a few weeks after that Trumbull the artist was promptly arrested as Trumbull the spy.

# Codes and Ciphers in History

Derek J. Smith

Washington, meanwhile, had been busy winning the real war. After the incident with Church, he had assumed personal responsibility for his Continental Army's intelligence service, through his spymaster Major Benjamin Tallmadge, codename "John Bolton". Their operative in (British) New York City was Robert Townsend, codename "Samuel Culper, Jr", an apparently loyal merchant. The network was put together in 1778 to help Washington in his stand-off with the latest British commander, Sir Henry Clinton. Townsend sent out regular reports on troop movements and morale, writing in code, cipher, and invisible ink, as well as sending messages via a makeshift flaghoist involving the raising of petticoats on washing lines (CIA website).

The Culper ring used a "nomenclator", a hybrid cipher-cum-code. The cipher encrypts the bulk of the message, but critical content words are given code words beforehand. Nomenclators were developed by Gabrieli di Lavinde in the late 14th century (Kahn, 1996), and in this particular one (devised by Tallmadge) 38 meant "attack", 192 meant "fort", 660 meant "vigilant", 703 meant "wagon", 711 was George Washington, 723 was Townsend, 727 was New York, and 728 Long Island. When the ring needed something special, it also had access to one of the cryptoanalytic geniuses of the day, James Lovell, of the Continental Congress's Committee of Secret Correspondence, whom Kahn (op. cit., p181) describes as "the father of American cryptanalysis" for his part in deciphering despatches from Lord Cornwallis shortly before the Yorktown campaign in 1781.

At the beginning of this final and ultimately decisive campaign, the British had two major strongholds on the American eastern seaboard, Clinton in and around New York City and Lord Charles Cornwallis in and around Yorktown, a touch over 300 miles further to the south. In an eighteenth century act of bluffery not dissimilar to Operation Fortitude during the Second World War [details], Washington secretly moved about 80% of his forces away from the New York City siege lines and sent them south towards Cornwallis. The remaining 20% did their best to conceal their sudden weakness by making five times the normal noise and dust, and the double agent James Rivington used Clinton's trust in his intelligence to persuade him that Washington's main force remained the other side of his defences. This was awesome "total generalship" on Washington's part, because the strategy, the tactics, and the intelligence support all dovetailed together perfectly, and the ruse worked spectacularly well. Clinton duly abandoned any ideas he had of reinforcing either the naval or the shore defences around Yorktown, and Cornwallis, caught off balance both on land and at sea, surrendered his forces on 19th October 1781. The War of Independence was then over bar the shouting. Not for nothing had Washington allocated more than ten percent of his military budget to intelligence operations (Deacon, 1980). [For more on the gunpowder war, see Allen (2001 online), and for more on Dr Edward Bancroft, see Rafalko, 2002; Chap3 online. See also Fraser (1997/2002 online, Part III (entire).]

The American Revolution ended formally with the three-way "Peace of Paris" in 1783, but this was not an end to American political intriguing. Jefferson corresponded with James Madison in cipher while framing the US Bill of Rights in the late 1780s (Bernstein, 1997; but see also Hobson and Rutland, 1978 and Smith, 1995), and there was also correspondence in a curious mixture of plaintext and ciphertext between Madison and other officials negotiating the Louisiana Purchase with Napoleonic France in the period 1803-1804 [specimen]. Fraser (1997/2002 online) lists many other instances of secret communication during this period, and summarises the role of cryptology in the American struggle for independence this way:

"From the beginnings of the American Revolution in 1775 until the adoption of the United States Constitution, Americans used codes, ciphers, and other secret writings to foment, support, and carry to completion a rebellion against the British government. In the words of one author, 'America was born of revolutionary conspiracy'."

# Codes and Ciphers in History

Derek J. Smith

## Encryption in the Age of the Optical Telegraph

"The secret of war is to make oneself master of communications." [Napoleon, "Maxims of War".]

Scarcely was the American Revolution over, than the French Revolution began. The period 1789-1815 is then marked by three historically distinct but technologically similar phases. The first of these, the French Revolution proper, started with the storming of the Bastille in July 1789, ended with the execution of Louis XVI in January 1793, and was part bloody civil war and regicide, and part war with Austria and Prussia. The second phase started with the extension of the war to include Britain, Spain, and Holland in 1793, and ended in 1799 when Napoleon became First Consul. The third phase - the "Napoleonic Wars" - began in 1800 with First Consul Napoleon reopening the fight against the Austrians with campaigns at Marengo and Hohenlinden, became more intense after he was made Emperor of France in 1804, and ended at the Battle of Waterloo in 1815. During this latter phase, France was actively at war with Britain all of the time, and on and off with various coalitions of Austria, Russia, Prussia, Spain, and Portugal, as particular circumstances dictated.

The Napoleonic Wars were another cryptologically active period. Napoleon's chief of police more or less without break after 1799 was Joseph Fouché (1759-1820), a cold and calculating revolutionary extremist, and a skilled political survivor. Fouché, once described as "the father of modern espionage", achieved his reputation in the mid-1790s thanks to his ruthless dealings with the aristocracy, counter-revolutionaries, the church, and anybody else unlucky enough to get in his way, and it was his habit to send Bonaparte daily secret reports of gossip, public opinion, rumour, and intercepted correspondence. If sedition was spoken one day, he boasted, he would know about it the next day (and the emperor, presumably, the day after). Another less well told cryptostory from this period seems to be that of a Dr Joseph Head Marshall, but our researches here are incomplete.

The Napoleonic age is also technologically significant as the birthplace of the optical telegraph (as described in Part 1), and the cryptological impact of this invention is that because it "broadcasts" rather than "beams" its signal it actually increased the need for encryption systems and services rather than decreasing it. A commander no longer had to capture one of his opponent's message bearers, in other words, because anyone with a decent telescope and a convenient hiding place could see every move of the enemy semaphore's arms. The champion of the French optical telegraph, Claude Chappe, therefore provided a detailed codebook to go with his hardware. Kahn (1996) gives details, if interested.

The French also used a range of ciphers in the Iberian Campaign ("The Peninsular War") in 1811. To start with, there were a number of petits chiffres for low priority messages. These would substitute 50 or so key nouns but would only protect the content for a matter of hours. For more strategic communications, his generals introduced a special grand chiffre, a 1400-character codebook along the lines of Louis XIV's chiffre indechiffable. There was also the "Army of Portugal" cipher, the "Great Paris cipher", and the common cipher, but eventually these were all broken by one of Wellington's Staff Officers, Captain George Scovell. Henceforward, Wellington routinely gathered such intelligence using a small but highly mobile force of Scovell's - some experienced men, plus "Portuguese smugglers, Spanish ne'er-do-wells, and Irish soldiers of fortune" (Urban, 2001, p57). His term for information gathered in this way was "seeing over the hill", and it therefore contrasts appropriately with optical telegraphy, which merely sees from hilltop to hilltop.

The last three years of the Napoleonic Wars saw two major European campaigns and another American war. The European campaigns were (a) Napoleon's abortive Russian campaign of 1812 (see next section), and (b) the "hundred days" campaign of 1815, which culminated in the finally decisive Battle of Waterloo. The American campaign was the Anglo-American War of 1812-1814 (the "White House" War), which took place during the presidency of James Madison. It is best known for

# Codes and Ciphers in History

Derek J. Smith

two key events, (a) the tit-for-tat burning of government buildings, and (b) the Battle of New Orleans. Cryptologically, the war is notable only for the fact that the American intelligence system had slumped badly from the heights of efficiency to which George Washington had raised it (Fishel, 1996), this despite the fact that President Madison had been an active user of cryptography for some 40 years. The Battle of New Orleans is notable not just as a case study in flawed military decision making (on the British part), but also for the fact that it took place on 8th January 1815, two weeks after peace had been declared, the news having yet to reach Louisiana - a reminder of how deficient long distance communications really were at that time.

## The Great Game, 1815-1852

The irony of Napoleon's abortive invasion of Russia in 1812 was that it allowed and encouraged the Romanovs to emerge as major new players on the international scene [for an introduction to Russian royal history between 1613 and the bloodbath of 1917, [click here](#)]. The Russia of Catherine the Great (1729-1796) had been significantly pro-British, thanks to tireless work back in the 1770s and 1780s (a) by the British ambassador there, Sir Charles Hanbury-Williams, and (b) by our old friend Sir Francis Dashwood (so significantly pro-British, in fact, that the latter even managed to bed the Tsarina (Deacon, op. cit.). Catherine's successor, Paul I (reigned 1796-1801) tended to side with Bonaparte but did not live long, and his son Alexander I (reigned 1801-1825) quickly realigned Russia with Britain for the remainder of the Napoleonic Wars.

ASIDE: In other words, while the Americans had been courting the French in their struggle against the British, the British had been courting the Russians against the French, and Sir William Eden lived just long enough to take solace, no doubt, from every disastrous frozen mile of Bonaparte's 1812 retreat from Moscow.

After Alexander I's death in 1825, everything changed. Alexander was succeeded by his brother Nicholas I (reigned 1825-1855), who grew increasingly tyrannical as the years unfolded, and became increasingly obsessed with territorial expansion. This led to two new trouble spots along Russia's southern borders, one as they tried to take the Crimea back from the Turkish Empire, and the other as they tried to destabilise the British in India. This latter adventure became known to the British as "the Great Game" after one of those who fought in it, Lieutenant Arthur Conolly, used the term in his 1834 memoirs (see Buxton, 2002 online), whilst to the Russians it became the "Tournament of Shadows". A period of small regional uprisings and wars followed, culminating in the First Afghan War (1839-1842). The "North West Frontier" (the land between Afghanistan and modern Pakistan where the Taliban and Al Qaeda hid so successfully in winter 2001) remained a running sore on the eastern flank of the British Empire for the next century, and the Great Game began an age of Central Asian high-sierra intrigue which is worthy of note for no more compelling reason than that it has not yet run its length and could go nuclear, chemical, or biological at any moment (see Rainwater, 2002 online). The story is told in greater detail in Hopkirk (1994) and Meyer and Brysac (2001).

## Codes and Ciphers in History, Part 2 - 1853 to 1917

### Cryptology and the Electric Telegraph (1853-1865)

"Without communications, I command nothing but my desk." (General Thomas Power, USAF, cited in Woods, 1974.)

The story of the development of the electric telegraph was told in detail in Part 1 of the main paper, and the "Great Game/Tournament of Shadows" was introduced towards the end of Part 1 of this historical review. These apparently unconnected threads of history came together in the Crimean War (1853/4-1856). The immediate cause of this war was the Russian annexation of the Crimean

## Codes and Ciphers in History

Derek J. Smith

Peninsular from the Turkish Empire. They did this as an attacking move in the Tournament of Shadows, calculating that it would give them a greater Black Sea presence, and thus greater influence throughout the Mediterranean and the Middle East. To help counter this, Britain (under Queen Victoria) and France (under Napoleon III) suddenly had cause to forget old differences and become allies. The Russian-Turkish war began in October 1853, when Tsar Nicholas I seized upon a (possibly engineered) atrocity in Bethlehem to seize Turkish possessions on the Lower Danube. Britain and France then declared on the Turkish side on 28th March 1854, although little actually happened until September that year, because that was how long it took for a joint British-French expeditionary force to arrive in the Crimea. The expeditionary force established a bridgehead at the port of Balaklava, and the campaigns which followed became the first major war to be fought in the age of the electric telegraph, and gave the new technology a thorough baptism of fire.

The Crimean telegraph had two distinct aspects, namely (a) an eight-station theatre telegraph system around Balaklava, and (b) a submarine cable link to Varna, 340 miles away across the Black Sea (on the coast of what is today Bulgaria). The theatre system was laid by a cable-laying party under Lieutenant Stopford of the Royal Engineers, and was ready for service after only a few weeks [one of the two cable wagons used, and other equipment from this period, is on display in the Royal Signals Museum, Blandford, Dorset]. The submarine cable followed in April 1855, and, for the first time in the history of warfare, put field commanders in direct and nearly immediate touch with their respective war departments. However, not everybody responded equally to the new technology. For the French, Napoleon III kept personal close contact with the commander of the French forces, but for the British the new technology became - it seems - an avenue for petty bureaucrats to raise minor administrative problems. Perhaps not surprisingly, therefore, another textbook example of poor military communication - the Charge of the Light Brigade - comes from this very war.

For their part, the Russians took out a spur from their Siemens and Halske telegraph system in Odessa, and ran it all the way to Sevastopol (where according to Woods, 1974, they got it operational just in time to inform Moscow that the city was about to surrender). The Vigenère polyalphabetic cipher was one of the main codes used by the Russians, and it has been suggested that this is why such an unearthly silence greeted the British computing pioneer, Charles Babbage, when he managed to crack it in 1854.

ASIDE: Both Singh (1999) and Swade (2000) tell the story that in 1854 a Bristol dentist named John Thwaites published claims to have invented a new cipher system. Babbage responded that the man had actually re-invented the as-yet-uncracked Vigenère cipher. Disappointed, the man challenged Babbage to crack it anyway, and he did, by analysing the ciphertext for patterns of a higher order than simple letter frequencies (Singh explains that the principle of counting letter groupings rather than the letters individually will result in repeats of common words - eg. BUK for "the" - if coincidentally they are a multiple of the key length apart in the plaintext). What Babbage could not do, however, was publicly proclaim his breakthrough, for then the Russians would immediately stop using the Vigenère. There would be plenty of opportunity for Babbage's decryption method to be tested, but only as long as he kept his discovery to himself. The 1854 break did not become public knowledge, therefore, and the credit is nowadays given to the Prussian Friedrich Kasiski, who arrived at the same method in 1863. Singh gives a detailed worked example, if interested.

Three thousand miles to the east, the local rebellions continued in British India. The telegraph here had to cope with distances on a truly continental scale. A telegraph line opened between Agra and Calcutta (800 miles) on 24th March 1854, and by 1856 had been extended to Bombay, Peshawa, and Madras. The engineer in charge was William (later Sir William) O'Shaughnessy, of the East India Company, who had successfully demonstrated an experimental 13-mile of telegraph near Calcutta as early as 1839 (John H. Lienhard, 2002 online, on the excellent "Engines of our Ingenuity" website,

## Codes and Ciphers in History

Derek J. Smith

University of Houston). Telegraph development was then forcefully promoted by Lord Dalhousie, after he became Governor General of India in 1847, and O'Shaughnessy's system was fully operational in 1851. Amin (1999/2002 online) explains how the introduction of western postal and telegraph services in the sub-continent gave the Indians a new sense of their own political identity, thereby elevating humble cable and keys to being one of the causes of the Indian Mutiny (1857-1859). The rebellious Sepoys certainly fully appreciated the telegraph's tactical significance, and regularly targeted telegraph offices and the lines themselves. This in turn prompted acts of bravery such as that of the 18-year old Delhi telegraph operator George Brendish, who, with his officer killed, remained at his equipment keying warnings until the last possible moment [picture; example]. Woods (1974) dates the first Indian field telegraph (that is to say, the deployment of equipment mobile enough to stay close to the action and deliver real time tactical support) to 1858, when a wiring party accompanied the British relief column on its way up to Lucknow.

The 1850s were also a formative period for American military signalling. The leading figure here seems to be Major Albert James Myer (1829-1880), who turned his early experience as a physician teaching sign language to the deaf to military purposes, introducing a hand-held semaphore signalling system (colloquially, a "wig-wag" system) into the US Army in 1856. Myer's system was so well received, that in June 1860 he was transferred from the medical corps to the newly established US Army Signals Corps, and his system was then put to the acid test by the American Civil War (1861-1865).

The American Civil War was fought over territory which already had a large pre-existing telegraph network. Both sides therefore arranged for their field telegraph systems to bridge into that existing network, and the northern states - the Union - even set up the War Department Telegraph Office to coordinate the fixed and the battlefield networks. In August 1861, Myer proposed attaching a telegraph signal unit to every army on the march, and thanks to the foresight of Colonel Thomas A. Scott, Assistant Secretary of War, this was duly authorised (Woods, 1974). It was then necessary to keep all the additional telegraph traffic secret, and Anson Stager, of the Western Union Company, was recommended for the job. Stager duly set about designing and administering the ciphers to be used, and did the job so assiduously that the southern states - the Confederacy - never managed to crack them (Kelley, 1999 online). President Lincoln is reported to have spent considerable time in Stager's cipher office in Washington, deeply intrigued by what went on in nineteenth century cyberspace (Greely, 2002 online). The telegraph service made no military decisions on its own, of course; it merely fed information up into a sometimes inconsistent military intelligence superstructure (Finnegan, 1994/2002 online). The Union also made use of the pre-war detective agency run by the Scottish emigré (and one-time workers' rights activist), Allan Pinkerton, although Finnegan dismisses Pinkerton's contribution as "mostly misinformation" (op. cit.).

As a basically rural economy, the Confederacy had less access to state-of-the-art hardware than did their enemy. However, they compounded this shortcoming with another; that of failing to create a central co-ordinating department like Stager's. Instead, they were content to leave individual commanders to select their own encryption methods. The Vigenère polyalphabetic system was frequently used, and reasonably secure, but the schoolboy Caesar shift was not unknown, as was no protection at all. On balance, therefore, Ryan and Ryan conclude that Union commanders enjoyed significant access to what the Confederates hoped and believed were secret communications: "The South's failure to protect critical information," they argue, "undoubtedly contributed to many Yankee victories".

The Ryans point especially to the Battle of Antietam on 16th-18th September 1862 as the "most catastrophic" (and in the end pivotal) example of Confederate cryptological negligence. This was a supremely violent battle in which the Union General George B. McClellan had to blunt a multi-column

## Codes and Ciphers in History

Derek J. Smith

advance by Confederate General Robert E. Lee, and by the time it was all over there had been twice as many casualties as in the 1812, Mexican, and Spanish-American Wars put together, and four times as many as were suffered during the D-Day landings 82 years later. The intercept on this occasion was very low tech - nothing more complex than the loss from an unknown Confederate staff officer's pocket of an en clair copy of General Lee's special order #191 for the invasion of Maryland.

ASIDE: The Confederates were in fact thrice negligent at Antietam, (a) for not enciphering the order in the first place, (b) for simply losing it, and (c) for not monitoring their enemy's newspapers (specifically, for failing to abort their attack after the New York Herald had stupidly reported the intercept on 15th September); in fact, Robert E. Lee subsequently claimed that he only learned of the loss early the following year (Fishel, 1996).

Nor was Antietam the Confederacy's only error. Their agent Rose Greenhow made the elementary mistakes (a) of keeping copies of her reports, and (b) of keeping at least one set of matching plaintext and ciphertext. When she was arrested by the Pinkerton agency on 23rd August 1861, the forensic cryptanalysis was simplicity itself (Horan, 1970). The lesson here (yet again) is that it takes more than an encryption system to make a successful encryption service: Mrs Greenhow was an enthusiastic amateur who broke commonsense procedural rules, and we will shortly be seeing how similar gross procedural errors would compromise the German encryption systems in World War Two (see Part 3).

Civil War telegraph technology also had tactical implications. The inventor George W. Beardslee patented a battery-free telegraph system in 1857 to capitalise on the need for a lighter, and therefore field-portable, telegraph station. These units were first adopted in May 1862, and 30 of them were in use by 1863 (Woods, 1974). The following extract will give a flavour of what was possible once it was no longer necessary to drag a heavy battery wagon along with you:

"The army signal-telegraph has been so far perfected that in a few hours quite a large force can be in constant connection with headquarters. This while the battle is progressing, is a great convenience. The wire used is a copper one, insulated, raised on light poles made expressly for the purpose, on convenient tree, or trailed along fences. The wire and the instrument can be easily carried in a cart, which as it proceeds unwinds the wire, and, when a connection is made, becomes the telegraph office. Where the cart cannot go, the men carry the drum of wire by hand. The machine is a simple one, worked by a handle, which is passed around a dial-plate marked with numerals and the alphabet. By stopping at the necessary letters, a message is easily spelled out upon the instrument at the other end of the line, which repeats by a pointer every move on the dial-plate. (Harper's Weekly, 24th January 1863; from the website of the Ohio Valley Civil War Association.)

Thus whereas Stopford had ploughed his wires two feet down into the Crimea in 1855, less than ten years later we have the signallers in much closer tactical support to the front line. Needless to say, these field telegraph systems immediately became prime targets in themselves, and when you were not wiretapping, you were wire cutting [see, for example, Abruscato and Hara, 1999-2001 online]. Both sides took to sending out small groups of telegraph technicians accompanied by skilled backwoodsmen, to cut into the enemy's wires in some secluded spot. One of the most striking examples of this was C.A. Gaston, General Robert E. Lee's personal telegraph operator, who tapped General Grant's network during the siege of Richmond, VA, for no less than six weeks (Greely, 2002 online). [For the fuller story, see W.R. Plum's "History of the Military Telegraph in the Civil War" (1882/2000 available in facsimile). Fishel (1996, p4) plays down the importance of tapings, reporting "only one brief tap" (presumably Gaston's).]

# Codes and Ciphers in History

Derek J. Smith

## Spies on the Line (1866-1902)

The "Confederation of the Rhine" was established in 1806 as Napoleon's way of making some sense of the ruins of the Holy Roman Empire, whilst keeping Germany divided and weak, and France strong. However, from the German point of view not enough of these provisions were reversed in the 1815 Treaty of Vienna. This was because Habsburg Austria still held too many of the cards. The most influential Austrian at the treaty negotiations was Prince Klemens von Metternich (1773-1859), and the resulting German constitution left the German-speaking people as a collection of 39 separate states, with the Austrians having the most votes. This led during the 1820s and 1830s to social unrest in many of these states, and, before long, to a reaction against the overbearing Austrian-ness of Metternich's Vienna.

The German unification movement flourished in the 1840s, championed by the largest of Austria's rivals, Prussia, which saw itself as the ideological and ethnic heartland of a larger German empire, and in May 1848 the "Frankfurt Assembly" was convened with a brief to draft a suitable constitution for a unified northern Germany and to appoint its first emperor. Somewhat optimistically, given the extent of the opposition from the Habsburg establishment and Tsarist Russia, the assembly invited King Friedrich Wilhelm IV of Prussia to become the first imperial Kaiser, but he did not feel sufficiently certain of himself to accept. It took another twenty years for the German nationalists to recover from this setback, but recover they did, and the central figure in the renewed manoeuvring was by now Otto von Bismarck (1815-1898). Bismarck became Prussia's Minister-President in 1862, and immediately embarked on a national muscle-building programme, during which the Prussian army was progressively developed. They were tested in 1864 when the lands of Schleswig and Holstein were taken from Denmark after a pretty one-sided six month campaign.

Now we mention all this, because in 1866 Prussian eyes turned to the Habsburg territories of Silesia and Bohemia, and to help it in this deliberately engineered confrontation a counterintelligence organisation named the Abwehr was established. Abwehr agents were placed in key positions throughout the capitals of Europe, and those in Vienna were combat tested almost immediately in the Austro-Prussian War (1866) (the "Seven Weeks War"). This time it was the Habsburg's turn to be humiliated, for the Prussians ripped apart the Austrian army at the Battle of Königgrätz on 3rd July 1866, and by the Treaty of Prague on 23rd August the German states were reconstituted as the Prussian-led "North German Federation".

ASIDE: Though not much spoken about nowadays, Königgrätz was at the time the largest battle ever fought in Europe, involving more than half a million men. It is historically significant not just for heralding the end for the Habsburg dynasty, but also for proving the success of the latest German military tactics.

With Germany unified and Austria sidelined, Bismarck's gaze now turned to Alsace-Lorraine, on the west bank of the Rhine. This automatically placed them at odds with France, but they were lucky because the French were in an over-confident and slightly decadent national mood, lulled by the success of their 1867 Great Exhibition (Horne, 1965, sees a larger truth in the fact that the French exhibited "the beautiful and the frivolous", whilst the Prussians were showcasing the latest Krupp armaments).

So successfully had the Abwehr done its job in 1866, that it was recommitted in strengthened form in the Franco-Prussian War (1870-1871), after Napoleon III had been goaded into declaring war on Germany. One of its most thoroughly documented agents was August Schluga. Schluga - codenamed "Agent 17" - was active from the very beginning of the service and reported on the situation in Paris in 1870 to the German military attaché there, Lieutenant-Colonel (later Field Marshall) Alfred von Waldersee. He remained in business until forced by ill health into retirement in 1917 (Pöhlmann,

# Codes and Ciphers in History

Derek J. Smith

1999/2002 online), but one of his ciphertxts is on the web, if you fancy the challenge [view]. Brückner (1998/2002 online) remains unimpressed with Schluga's overall contribution, describing it as merely "interesting". Wilhelm 1 was proclaimed Kaiser on 18th January 1871, and Bismarck promoted to Reichskanzler of the German Empire - the "Second Reich" (the "First Reich" was deemed to have been the Holy Roman Empire) - a position he held until retiring in 1890.

One analysis of the turbulent 1860s and 1870s has since become a classic of cryptanalytical theory, Auguste Kerckhoffs' "La Cryptographie Militaire" (1883). Kahn discusses Kerckhoffs' work in some detail (Chapter 8), and draws particular attention to his insight that different rules applied to the occasional communications of ambassadors and gentlemen than did to heavily used battlefield communication systems. In fact, there were two fundamental requirements for a successful field cipher system, namely (a) that it could cope with the volume of traffic likely to be thrown at it, and (b) that its inventors/manufacturers were not necessarily the best people to appraise their systems' weaknesses - thieves needed to be set to catch thieves.

The last quarter of the nineteenth century saw a lot more imperial wars, and the Great Game in particular was far from over. Rainwater describes how a new "forward policy" was brought into British imperial strategy when Benjamin Disraeli became Prime Minister in 1874. By now, the Russians were making major inroads into the Turkish Empire, and had established their influence across Central Asia, Britain needed to defend the northern borders of the Indian subcontinent. This resulted in the Second Afghan War (1878-1881), during which they were tormented by a force of agents provocateur reporting to Moscow.

ASIDE: When Alexander II was killed by an anarchist bomb in 1881, his son, Nicholas II, actually supplemented his international intelligence service by forming the Special Department, the Okhrana, who served him much as the Gestapo would later serve Adolf Hitler, and who were, for a time probably the most effective SIGINT organisation in the world.

The nineteenth century closed with two further telegraph-assisted wars. The Spanish-American War (1898) saw the Americans deliberately targeting their intelligence operatives on the Western Union telegraph office in Havana, so as to monitor communications between local commanders and their commanders-in-chief in Madrid, and the Anglo-Boer War of 1899-1902 saw the British relying on the established Wheatstone Automatic telegraph. Some 18,000 miles of cable were laid during this war (Royal Signals Museum website), and despite constantly having to cope with cut wires successfully delivered 13,500,000 messages. Not that all of these arrived intacta at their destination: Philip Pienaar, one Boer telegraphist, once got "the entire plan of campaign for the next four weeks" by tapping General Hamilton's telegraph line (Pienaar, 1902, cited in Lee, 1985). The archives at King's College London include two volumes of cipher telegrams between the Secretary of State for War and General Sir Horatio Herbert Kitchener, Commander-in-Chief, South Africa. The British also experimented with sending their messages in arcane languages such as Hindustani (Deacon, 1980), a ploy repeated by the Navajo "windtalkers" in World War Two, and popularised by the 2002 movie of the same name.

## Spies on the Air (1897-1917)

Note: Although the words "wireless" and "radio" both mean much the same thing nowadays, they derive from different inventors. For the sake of convenience, we shall use the former as short for "wireless telegraphy", that is to say, station-to-station aerial telecommunication using Morse or other non-voice codes, and the latter as short either (a) for "radio telephony", station-to-station aerial telecommunication of the spoken voice, or (b) "radio broadcasting", the undirected transmission of the spoken voice to a large and individually anonymous audience.

# Codes and Ciphers in History

Derek J. Smith

Following only three years of basic experimentation, Marconi's Wireless Telegraph and Signal Company (see Part 1) started successfully demonstrating its wares in August 1897. Orders were immediately forthcoming from the world's navies, merchant marines, and news agencies (all those, in fact, who had been most restricted by the hard-wired world of telegraphy). Things then moved very quickly indeed. For example, the Prince of Wales was able to dictate a message from on board the Royal Yacht on 10th August 1898, and a year later messages from the wireless room aboard HMS Defiant managed to control a fleet of three ships at sea. The first theatre trialling of wireless telegraphy was by the British in 1899, during the Boer War [picture], although no substantive content was carried. A Boer order for six wireless sets from Marconi's German rivals Siemens and Halske, was impounded as contraband upon arrival at Capetown (IEEE website). The experiment was repeated in Somaliland in 1903 by Lieutenant Arthur E. Silvertop, RN, but poor earthing and adverse atmospheric conditions restricted the effective range to only 33 miles (Trappes-Lomax, 1955), and over the ensuing decade, much important research was carried out by Henry J. Round (1881-1966), of the Marconi Company. Maurice Wright, a Marconi technician, worked with Round on a high-power wireless receiver, and was intercepting German wireless traffic from the company's Chelmsford laboratories two days before the outbreak of the war.

The new technology immediately prompted renewed interest in the science of encryption, for whenever you sat down at your transmitter you were deliberately risking your secrets "on the air" - anybody who could get their hands on a suitably tuned receiving set could listen in, and that included your enemies. Indeed, one of the very first messages to pass from England to France, on 29th March 1899, was sent in a simple cipher, not because it was secret but because its originators wished to ensure thereby that the equipment was not an elaborate hoax of some sort (McClure's Magazine, June 1899). Cryptology was accordingly a major aspect of First World War military intelligence, and the French, building on the traditions of Vigenère, Rossignol, and Kerckhoffs, were again reputedly the best at it (Kahn, 1996). They broke the German double transposition system in October 1914, and one of their best cryptanalysts, George Painvin, was single-handedly responsible for blunting a major German offensive in 1918. For their part, the Germans annihilated an entire Russian army at the Battle of Tannenberg in August 1914, because the Russians, having botched the distribution of their codebooks, resorted to using unencrypted radio transmissions (Finnegan, 1994).

The British efforts were concentrated in Room 40 at the Admiralty, a department which was founded by Sir Henry Oliver in 1914 and headed by Captain (later Admiral) William Reginald ("Blinker") Hall (1870-1943). Their operations were helped by the capture in 1914 of codebooks from two sunken German vessels, and in 1915 of a copy of the diplomatic codes. They were also impressed by Round's August 1914 eavesdropping success, and directed Marconi to release both Round and Wright for special duties developing a network of wireless tracking stations around Britain (Wright, 1987). These were codenamed the "Procedure 'Y' Stations". Wright even ran an illicit listening station in neutral Oslo for six months in 1915, escaping capture only by a whisker.

ASIDE: ASIDE: The Y-Stations were used extensively in both world wars, and provided the Bletchley Park codebreakers (see Part 3) with much of their raw material. Maurice's son, Peter, himself had an eventful career in British counterintelligence, claiming to have identified the "fifth man" in the Burgess-Maclean-Philby-Blunt spy scandal of the 1950s-1970s, and publishing the best-selling "Spycatcher" in the late 1980s (Wright, 1987).

The war at sea was also a learning experience for all involved. The naval battles of Coronel (1st November 1914; two British warships sunk by a five-unit German cruiser squadron under Admiral von Spee) and the Falkland Islands (8th December 1914; Royal Navy revenge) highlighted the need for new tactics and strategies. Wireless intercepts from ports along the eastern and western coasts of South America guided the opposing fleets (often by tracking their supply ships to their secret

## Codes and Ciphers in History

Derek J. Smith

rendezvous). Only the Dresden escaped the Royal Navy at the Falkland Islands, and the next three months were spent playing hide and seek from Valparaiso to Cape Horn. She was finally located by radio intercept in early March 1915, which, when deciphered by the Room 40 people, gave the position of a planned rendezvous 300 miles out into the Pacific from the Chilean mainland. A final wireless-aided chase ensued, resulting in the Dresden being run to earth at nearby Mas a Fuera, where she was scuttled after a short fire-fight. The Germans got their own back a year later, when on 26th May 1916 the Abwehr's marine section managed to decipher an out-of-the-ordinary mine-clearance report. This intercept enabled them to re-seed the cleared channel within hours, and the next ship out through it was HMS Hampshire, carrying the British Commander-in-Chief, Lord Kitchener, on a visit to Russia. It struck one of the newly laid mines, and was lost with nigh on all hands.

ASIDE: One of Dresden's officers, a young Lieutenant named Wilhelm Canaris, managed to escape Chilean internment, and made his way back to Germany. By 1932, he had risen to the rank of Captain, and at Christmas 1934 was put in charge of the Abwehr. Remembering the Dresden and the Hampshire, he never forgot the strengths and weaknesses of wireless. Indeed, he even authorised his own Enigma network, which the British Bletchley Park codebreakers (see Part 3) had to form a separate team to monitor.

The Americans, too, were learning new skills the hard way. In 1914, Ralph van Demen created a Military Intelligence Cipher Bureau under Herbert O. Yardley (1889-1958), poker player turned cryptanalyst. The new service saw action between March 1916 and February 1917, when General John J. Pershing mounted a punitive expedition against Mexico's Pancho Villa for armed incursions into New Mexico [details]. Not only was this the first opportunity for the Americans to use aircraft and motor vehicles in action, but it also allowed them to make full use of the latest telecommunications technology. Unfortunately, Pershing was searching for a force of Mexican irregulars in a land which largely adored them. The Villistas were therefore able to appear and disappear at will, and when they fought at all it was as guerrillas. Pershing countered this by appointing Major James A. Ryan as his intelligence officer, and the latter set about organising a network of telegraph and telephone listening stations (Rafalko, 2002; Chap3 online). The Signal Corps also provided the "radio tractors" which did the monitoring (Finnegan, 1994), although it must be presumed that these heard more from the legitimate Mexican government than from Pancho Villa's ill-equipped irregulars. Many of the intercepted messages were passed in the first instance to Captain Parker Hitt of the Signal School at Fort Leavenworth, KS. Captain Hitt was the US Army's resident expert on cryptological techniques, and had already put together the service book on the subject in 1915. Pershing's official report included the following:

"It was early observed that the Mexican authorities had no code in general use but that each commander had his own local code. This department took up the study of code messages and soon was able to decipher any code used in Northern Mexico. Thereafter, by tapping the various telegraph and telephone wires and picking up wireless messages we were able to get practically all the information passing between the various leaders in Mexico." (Pershing's "Report of the Punitive Expedition", quoted in Finlay, 1993.)

The Pershing expedition was finally recalled in January 1917, by which time relations with Mexico's official government were at a new low (a fact which - as we are about to see - was far from lost on the Germans). Much had been learned, however, and the experiences of a young Lieutenant named George S. Patton would prove particularly valuable a quarter of a century later when, as one of Eisenhower's Generals, he combined duties preparing the (real) US Third Army for the Autumn 1944 drive across France with inventing the radio traffic for a totally fictitious First Army Group (Tavares, 2001). Other members of either the expeditionary or the border defence forces who later became

# Codes and Ciphers in History

Derek J. Smith

famous were Omar N. Bradley, Matthew B. Ridgway, and George C. Marshall, the only professional soldier ever to have been awarded the Nobel Peace Prize (in 1953) (Finlay, 1993).

Room 40's highest profile success was to ensure the entry of the US into the war in the spring of 1917. This story begins with a telegram transmitted on 16th January 1917 from the German Foreign Minister, Arthur Zimmermann, to Count Johann von Bernstorff, his Ambassador in Washington, warning them that the Kaiser's Supreme Command had just decided as a point of grand strategy to intensify the U-Boat campaign in the Western Atlantic. This broke previous German undertakings to the US, and risked bringing the US into the war on the side of France, Britain, and Russia. Von Bernstorff was accordingly instructed to try to persuade the Mexicans to attack the US from the south. What Zimmermann did not know was that the trans-Atlantic telegraph cable was being routinely tapped by a British black chamber [yes, they were still around; and yes, they still are], and so the "Zimmermann intercept" was soon in Room 40. The problem then was that its high diplomatic priority meant that it was in a relatively new cryptographic system known as 0075, which Room 40 had yet to master, despite six months of trying. Nevertheless, enough words could be made out to give some hint as to the message's importance, so it received priority attention.

Now Hall knew that the second leg of the transmission, from Washington onwards to the German Legation in Mexico City, would probably travel by an older encryption system known as 13040, which Room 40 could decipher. He therefore placed an operative, codename "T" (Kahn, 1996), in the telegraph office in Mexico City, and a few days later Room 40 knew the German plan in full.

The British were immediately faced with the classic codebreaker's dilemma, namely whether to respond to a decryption, and thus reveal the true extent of their cryptanalytical competence, or keep quiet and suffer the consequences.

ASIDE: Having broken a code, it becomes important not to reveal that fact too directly. Specifically, you cannot afford to be "right too often", or your enemy will smell a rat, improve his systems, and you will be back where you started. There are two ways around this difficulty. One is to rely on (sometimes very elaborate) subterfuges, in which totally fictitious spies are praised for having obtained the information in question through more conventional espionage methods (Bury, online). The other is just to play dumb; to pretend you have not received this or that warning, sit back, and just let things happen. Needless to say, this means that the people in the hot seats end up having to play God with the lives of the people on the receiving end of whatever happens to be afoot. Military intelligence is accordingly a world of harsh realities and seamy secrets, when enemy intentions are known, but no action is taken to respond to them. Nor do things get any better: one very compelling (but entirely speculative) explanation of the failure to prevent the Omagh terrorist bomb in Northern Ireland in August 1998 is that after a string of successful "busts" the security forces had determined to let a bomb go through "undetected" to preserve the integrity of their informant. They therefore responded deliberately slowly to telephoned warnings, and 29 innocent bystanders were killed.

Hall decided to do nothing hasty for a day or two, but when the torpedoing did start again, it soon became apparent that President Wilson was still vacillating. In mid-February, therefore, with British shipping losses starting to mount, Hall finally took matters into his own hands, and revealed his decrypt to his superiors, and together they hatched a scheme to have the Americans learn "for themselves" of the German grand strategy. Using diplomatic contacts at the US Embassy in London, they passed the Americans the transcript of the Mexico City version of the telegram, which, since it matched a ciphertext the Americans themselves already had on record, could then be treated as both discovered and decoded on American soil. President Wilson duly made the matter public, and the story hit the streets in the morning papers on 1st March 1916, causing such a violent swing of public opinion against the Kaiser that the US declared war on Germany just over a month later.

# Codes and Ciphers in History

Derek J. Smith

Here are the first few lines of the Zimmermann telegram, as intercepted, to give some feeling for a large numeric codebook. For the full ciphertext, [click here](#), and for the decrypts, [click here](#) and [here](#).

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	

## Codes and Ciphers in History, Part 3 - 1918 to 1945

### The Automation of Secrecy, 1 - Simple Mechanical Systems

This story begins in 1891, when a French military cryptologist named Etienne Bazeries (1846-1924?) decided to resurrect, and if possible improve, Jefferson's cipher cylinder (see Part 1 of this historical review). He took around 30 separate disks and inscribed a different random cipher alphabet on each of their circumferences. He then stacked them in random order along a central spindle, giving what is nowadays called the "Bazeries Cylinder". The French army were not sufficiently impressed to develop this into a fully operational system, but a quarter of a century later the idea was resurrected by Captain Parker Hitt, fresh from his successes supporting Pershing's Mexican expedition (see Part 2 of this historical review). After further development by Major Joseph O. Mauborgne, the Jefferson-Bazeries cipher cylinder, was introduced in 1921 into the US Army Signal Corps under the equipment code M-94 (Gaddy, 1993 online), and remained in operational use until 1942. The M-94 consisted of 25 simple aluminium rotors, slotted onto a central spindle, and secured with a locknut [picture: note that disk #17 includes the plaintext ARMYOFTHEUS, a phrase which coincidentally (and necessarily) includes no one letter more than once.]. The US Navy CSP-488 [picture] was a close variant, and a flat slide version became the M-138-A (CSP-845 naval) "strip cipher" system [pictures]. Instead of 25 disks with circumferential lettering, each randomised alphabet was now printed vertically on a narrow lath. A stock box of 100 different laths was provided, from which a controlled subset of 30 was selected on any one occasion. The US Navy purchased this system in 1931, but only for high level communications. [To play with a simulated M-94, courtesy/copyright Wilhelm Plotz, [click here](#).]

### The Automation of Secrecy, 2 - The Hebern Wheels

As we have already seen, the late nineteenth century was the age of the technical entrepreneur. Inspired by the telegraph, the calculator, the typewriter, the cash register, etc [see Part 1], inventors in a number of countries started to develop automated cipher machines, and one historically important development appeared in four countries almost simultaneously. The first past the post was Edward Hugh Hebern (1869-1952), an American. In 1917, Hebern filed for a patent in a wired rotor cipher machine. The main functional component was a modern-day Alberti disk: it returned a cipher character for every input plain character, and it did this by means of covert internal wiring. The patent was awarded 30th September 1924, and, because Hebern was the first to deliver a working system, such rotors are sometimes referred to as "Hebern wheels" (eg. by Good, 1979). A German variation on the same basic principle was designed by Arthur Scherbius (1878-1929), and a patent applied for in 1918 [for sight of Scherbius' patent, [click here](#)], but Scherbius was robbed of a military marketplace

# Codes and Ciphers in History

Derek J. Smith

by the 1918 Armistice. He therefore targeted the security needs of banks and finance houses instead, exhibiting a prototype cipher machine named "Enigma" at the World Postal Congress in Stockholm in 1924. He then set up Chiffriermaschinen AG in Berlin, and his chief engineer Willi Korn took charge of developments after Scherbius died in 1929, accumulating further patents in his own name. The third rival system was devised by the Dutchman Hugo Alexander Koch, and the fourth by the Swedish engineer Arvid Damm. Both filed for patents in their respective countries in October 1919.

ASIDE - SWEDISH CRYPTOLOGY: This is a major story in its own right, but it strays too far from our central argument to be covered in detail. We cannot move on, however, without mentioning two central figures. Firstly, there is Boris Hagelin (1892-1983), a Russian-born Swede, who developed Damm's ideas during the 1920s and made a fortune selling the B-211 series of cipher machines to the French and Russian armies. He then took his know-how to New York in April 1940 and made another fortune selling the M209/CSP1500 to the US Army/Navy, and, as if that were not enough, his company Crypto AG made yet another fortune after the war selling cipher machines worldwide during the early decades of the Cold War. Then there is Arne Beurling (1905-1986), one time head of Sweden's cryptological service, and subject of a recent best-selling analysis by Bengt Beckman (Beckman, 2003 in Britain). It was Beurling who in 1941 first broke into the German Geheimschreiber system (see Part 3), and after the war his reputation was such that when he took up a post at Princeton University's Institute of Advanced Studies in 1965, he was allocated to Room #115, where Albert Einstein had once worked. Beurling died leaving no published explanation of how he broke the Geheimschreiber: "A magician," he insisted, "does not reveal his secrets".

## The Scherbius-Korn System in Greater Detail

The basic commercial Enigma system relied on scrambling keyboard input through an in-built electrical maze. Only the 26 letters of the alphabet were catered for; numbers were either written out in full, or otherwise coded. Pathways through the maze were controlled by three randomising rotors and a randomising "reflector". To put this another way, the maze was built up in parts, each part further scrambling what the preceding part had already scrambled. Each rotor was at first sight not unlike one of Alberti's cipher disks, and was removable to allow the left-right sequence - the Walzenlage - to be varied. Given three rotors and three slots, there are six different left-to-right rotor sequences, namely (I, II, III), (I, III, II), (II, I, III), (II, III, I), (III, I, II), and (III, II, I). Around the circumference of each rotor's outer ring were either the numbers 1 to 26, or the 26 letters of the alphabet, and pressed into the body of the inner ring was the scrambling circuitry. It was, however, possible to vary the relationship between the scrambling circuitry and the alphabet by rotating the inner ring within the outer ring prior to use. The ring position for any one encryption session was known as the Ringstellung. The built-in scrambling circuitry cross-strapped 26 fixed stud contacts (Walzenkontakte) on one face of the inner ring to another 26 sprung stud contacts on the reverse face [for close up pictures of rotors, both in and out of their mounting slots, click [here](#), or [here](#), and for a schematic wiring diagram, click [here](#)], and when the prepared rotors were fitted into slots at the top of the equipment, they left enough of their circumference protruding for the operator to adjust their angular setting. They were then rotated to a controlled start position known as the Grundstellung. Given three 26-letter rotors, there are 17,576 (ie. 26 cubed) different start settings for each of the six different rotor sequences (AAA, AAB, AAC, and so on to ZZZ), making the odds of randomly chancing upon the correct Ringstellung (26 cubed permutations), and the correct Walzenlage (six permutations), and the correct Grundstellung (26 cubed permutations) around two billion to one against.

After the initial set-up, current was switched into the right hand end of the maze by depressing individual alphabetical keys. The current then passed through the rotors one by one, entering by one of the right-facing contacts, passing through the hidden wiring, and exiting by whichever left-facing contact it arrived at; and so on until it reached the reflector on the left. This had 26 stud contacts on its right face (only), again wired together covertly in pairs, so that it could reverse the current back the

# Codes and Ciphers in History

Derek J. Smith

way it had arrived. The current then passed back through the three rotors a second time. Finally, the current was used to light a specific alphabetical lamp on the lamp board. This was the selected cipher for the alphabetic key which had been pressed. No letter was allowed to encipher as itself. At the same time as a key was depressed, the right hand rotor was mechanically advanced by one letter (so, in fact, the very first letter was actually encrypted on the rotor setting <Grund plus one>). Moreover, if at any stage a rotor advanced to its factory pre-set "turnover position", it would step the rotor to its left as well, using basically the same internal gearing as the "tens carry" mechanism in a calculating machine (see Part 1).

When the Scherbius system went to market in about 1925, commercial sales were poor (not least because the equipment was actually quite expensive), and the military were unimpressed. Scherbius therefore added a scrambling plugboard on the military versions, so that the output from the rotors could be enciphered an eighth time before being displayed, but this time under operator control. This letter-swapping plugboard was known as the Steckbrett panel. If R was "steckered" with L, say, on the plugboard, then L would light up as the encrypt, even though the last rotor had powered R. This massively increased the odds against trial-and-error decryption. The system therefore obeyed Kerckhoffs' principle that there should be a relatively basic general system, plus a foolproof specific key - a combination of the ring settings, the rotor sequence, the rotor start positions, and the steckerings. The key, in short, was everything, and theoretically (at least) could neither be guessed (Stripp, 1993, estimates the odds against an enemy cryptanalyst guessing the correct rotor and steckerboard settings at around one in 159 million million million) nor broken back (there was no pattern to the ciphertext to guide the cryptanalyst). Moreover, different networks with different keys and different operating procedures served different branches of the services and/or different geographical zones, and every day the settings were changed!

When the military tested this version of the equipment, they finally reached for their cheque books, and in 1926 the Enigma system entered service in the reborn German navy, the Reichsmarine (later Kriegsmarine). Systems for the army followed in 1928, and for the Luftwaffe in 1935. Enigma was also used by Canaris's Abwehr, the railways, and certain government departments. Volume production was eventually contracted out to a number of specialist engineering firms, including Atlas, Olympia (the typewriter people), Konski and Krüger, and Heimsoeth and Rinke, and by 1945 perhaps as many as 200,000 machines had been produced (Deutsches Museum). The steps in BLACK below show how the commercial hardware worked, and the step in RED shows the additional protection offered by the early military versions:

If you keyed the letter A, it might be converted to J by the first rotor,  
the J would then be converted to W, say, by the second rotor,  
the W would then be converted to B, say, by the third rotor,  
the B would then be converted to P, say, by the reflector, and the direction of travel reversed.  
the P would then be converted to X, say, by the third rotor,  
the X would then be converted to D, say, by the second rotor,  
the D would then be converted to R, say, by the first rotor,  
[military versions] the R would then be converted to whatever letter it happened to have been manually steckered with (or left unchanged if self-steckered).

The letter R (or whatever it had been steckered to) would then light up on the lamp display panel as the encrypt for the original A.

Of course, the right hand rotor (the "fast" rotor) advances one position with every key depression on the keyboard, so if a second A was now keyed, the right-hand rotor would be offering 26 different

# Codes and Ciphers in History

Derek J. Smith

stud-to-stud connections. The current to the lamp board would therefore follow a different encryption pathway, and generate a different cipher character .....

EXAMPLE: If you typed in the phrase ATTACKTOMORROWATNINE, the machine might cipher it as BXGUVJNCQQBIYJAWMPP. Note that the three Ts encrypt differently on each occurrence because the system is position-sensitive, that the double Q encrypt does not indicate a double letter in the plaintext, that there are no spaces between the words, and that the numerical "nine" has been spelled out in full because there were no separate numeric keys.

It remains to mention one of Willi Korn's most important innovations, that of selecting the rotors to be used in any one operational session from a larger stock. From December 1938, the rotors were selected from a stock box of at least five, later more [to see a seven-rotor machine, [click here](#)]. Given that there are ten different ways of picking three rotors out of five, and 35 different ways of picking three out of seven, this simple improvement greatly multiplied the unpredictability of the system.

Typical Enigma operating procedures for early 1940 were as follows (distilled from a number of sources, including Welchman, 1982, Stripp, 1993, and Singh, 1999) [we have deliberately excluded the complexities of station identification codes and dealing with multi-part messages, which are addressed in detail in Mommsen (1996-2002 online), if interested]:

## AT THE SENDING STATION

The message to be sent was stripped of spaces, numbers were written out in full, and X used to denote full stops.

The date was checked against the master code book, and .....

The specified day's rotors were taken from the stock box and laid out in the sequence specified (rotors III, IV, and I, say). The loading positions were known as the Walzenlage.

The inner ring on each rotor was then rotated within the outer ring until its alignment marker was level with the letter specified. The instruction 06-20-24, for example, would mean aligning the left rotor to F, the middle to T, and the right hand one to X (Stripp, 1993). The ring positions were known as the Ringstellung.

The steckerboard links [Steckerverbindungen] were plugged between the letter pairs stated in the code book. To start with, six steckerings were specified, leaving 14 letters "self-steckered", but this was later extended to ten steckerings, with six left over.

The rotors were then inserted into their slots, taking care not to disturb the ring settings nor damage the spring-loaded stud contacts, and rotated to the specified start position. This was the Grundstellung. The sending operator then decided upon a random three letter code, and keyed it in twice, noting the six encrypted characters. This gave him the message header, that is to say, the first six characters of the ciphertext. [With effect from 1st May 1940, the procedures changed, and it was only necessary to encipher the local code once.]

WORKED EXAMPLE: With the sending machine set to rotors III-IV-I and Grundstellung EJC, say, the sending operator devises a local key of GUS, say, and ciphers it twice to give LAJRCH, say. CONTINUED BELOW .....

# Codes and Ciphers in History

Derek J. Smith

The sending operator then reset the Grundstellung to his random code, and proceeded to encrypt the remainder of the message text, one character at a time, carefully noting down which lamp came on each time.

The full ciphertext was then sent in Morse Code.

## AT THE REMOTE STATION

The receiving operator decoded and wrote down each Morse character as it arrived. Providing reception was clear and the transcription was accurate, this produced a perfect remote copy of the ciphertext.

The remote Enigma was set to the day's official rotor and steckerboard settings (as above). The first six characters of the ciphertext - the message header - were keyed in, and this would decipher as the sending operator's Grundstellung, occurring twice.

WORKED EXAMPLE: CONTINUED FROM ABOVE ..... The receiving operator receives LAJRCH. He then sets his machine to III-IV-I/EJC (because he is working to the same codebook as the sending operator), so that when he keys in the LAJRCH message header, it will decipher as GUSGUS.

The rotors were reset to this value, and the remainder of the message decrypted.

WORKED EXAMPLE: CONTINUED FROM ABOVE ..... The receiving operator then resets his machine to a Grundstellung of GUS and decodes the remainder of the message. In this way, any one encryption is a theoretically safe function (a) of the machine's internal wiring, (b) of the daily codebook settings, (c) of the network operating procedures, and (d) of operator whimsey.

Finally, numbers were restored if required, and spaces and punctuation inserted as appropriate. Readers may find it useful to spend some time on one of the several Internet Enigma simulators. We found the Johns Hopkins University Internet Enigma simulator (Schwager, 1998-2002) [[click here](#)] user friendly and informative: note (from top to bottom) the rotor settings, the alphabetic lamp array for output, the keyboard for input, and the stecker panel, or plugboard.

## The Automation of Secrecy, 3 - Telephone Systems

### The Automation of Secrecy, 4 - Teletypewriter Systems

The First World War also prompted the creative use of teletypewriter technology [see Part 1] within cryptology. The pivotal figure here is Gilbert Sandford Vernam (1890-1960), a telegraph engineer with AT&T. When America entered the war in 1917, AT&T put Vernam to work on methods of guaranteeing the security of the then recently introduced teletypewriter systems. He did this by inventing a scrambler-unscrambler which would offer meaningless noise to any enemy agent who happened to be electronically eavesdropping. This is what he decided to do:

Key Development - Vernam's "Modulo 2" Bit Flipping: The modern definition of a cipher key is that it is "a large integer that tailors the behaviour of the standard algorithm and makes it generate a cipher that is specific to that number. All other things being equal, the longer the key, the more secure the mechanism." (Murray, 1994/2002 online.) Noting that every teletypewriter character was coded by five parallel bits across a paper tape [for details of the International Telegraph Alphabets, [click here](#)], Vernam suggested intervening electrically to change some or all of the bits according to a preset cipher key. This could be done by reading two tapes simultaneously, one containing the ITA2 plaintext and the other the cipher key on a repeating loop. All the equipment had to do - for each of the five bits

## Codes and Ciphers in History

Derek J. Smith

- was to carry out a "modulo-2" addition (binary, but without carrying) of plaintext bit with keytext bit. Each plaintext bit was therefore reset to a ciphertext bit as follows:

plaintext ZERO plus key ZERO gives ciphertext ZERO  
plaintext ZERO plus key ONE gives ciphertext ONE  
plaintext ONE plus key ZERO gives ciphertext ONE  
plaintext ONE plus key ONE gives ciphertext ZERO

In modern parlance, a modulo 2 addition is known as an "exclusive or" operation, or XOR for short. As in other ciphering systems, the key turns plaintext into noise which can only be unscrambled by someone else (a) with the same basic system, and (b) with the same key. As Christensen puts it: "Plaintext went in and plaintext came out, while anyone intercepting the message [would see only] a meaningless sequence of marks and spaces". A selection of Vernam's papers from the period in question are in the George C. Marshall Foundation archives, Lexington, VA.

The secret of the effectiveness of the Vernam technique is the key tape, which must be genuinely random, and as long as practicable. This requirement exposed a significant weakness in the system, because teletypewriter tapes were actually quite delicate, even in comparatively short lengths. A colleague of Vernam's, Lyman Morehouse, went a long way towards solving this problem by introducing a second key tape, and by setting the lengths of the two tapes to 1000 and 999 characters. This gave him two eight-foot loops of tape, but by a clever stepping arrangement, the 1000-character tape cycled once for every character on the 999-character tape, giving a "virtual" tape length of 999,000 characters, and saving about a mile and a half of tape in the process (Murray, 1994/2002 online).

The Vernam-Morehouse system subsequently formed the basis of a number of important World War Two cipher systems, including the German Lorenz SZ40/42, whose cryptanalysis we are now going to deal with in detail in Part 3 .....