FRACTURED HSTORY

IN THE BEGINNING

It is believed that the oldest known text to contain one of the essential components of cryptography, a modification of the text, occurred some 4000 years ago in the Egyptian town of MENET KHUFU where the hieroglyphic inscriptions on the tomb of the nobleman KHNUMHOTEP II were written with a number of unusual symbols to confuse or obscure the meaning of the inscriptions.

In 5BC the SPARTANS, a warrior society famed for their austere lifestyle, bravery, and skill in battle, developed a cryptographic device to send and receive secret messages. This device, a cylinder called a SCYTALE, was in the possession of both the sender and the recipient of the message. To prepare the message, a narrow strip of parchment or leather, much like a modern-day paper streamer, was wound around the SCYTALE and the message was written across it. Once unwound, for transport to the receiver, the tape displayed only a sequence of meaningless letters until it was re-wound onto a SCYTALE of exactly the same diameter. The code, produced by unwinding the tape, was a TRANSPOSITION cypher, that is, one where the letters remain the same but the order is changed. This is still the basis for many popular modern-day techniques.

The other major ingredient of these modern techniques is the ADDITIVE/SUBSTITUTION cypher. Although the Greek writer POLYIBUS described a substitution technique, its first recorded use was by JULIUS CAESAR. Messages were encoded by substituting the letter in the text by one that is three positions to the right. A became D, V became Y etc. The reason why a substitution of three letters, and not four, two or six, was chosen has never been explained.

In an essay written in 1466, an Italian LEON BATTISTA ALBERTI who is often called the ‘father of western cryptography’, described the construction of a cypher disk, founding the concept of POLY ALPHABETIC cyphers. Although he had made the most important advance in cryptography in at least five hundred years, he did not develop his concept. It was left for others, the best known being the French cryptographer BLAISE DE VIGENERE to devise a practical poly alphabetic system which bears his name, the VIGENERE SQUARE. At the time, and for a considerable time afterwards this technique was believed to be unbreakable (Le Chiffre Indechiffrable). There was however a weakness in this cypher waiting to be exploited because the cyphertext produced by this method was vulnerable to the yet undiscovered statistical attack.

Probably in 1854, CHARLES BABBAGE, developed the method of statistical analysis by which he successfully decrypted messages encrypted by the Vigenere square. Unfortunately, due to his habit of not completing ‘the paperwork’, or possibly to protect the fact that because of his work Britain could decrypt Vigenere messages sent in the Crimea, this fact was not discovered until the twentieth century. The honour of developing the statistical attack technique and cracking Vigenere was to go to the Prussian KASISKI in 1863, this technique having since been termed the KASISKI TEST.

WWI, THE WAR TO END ALL WARS

THE ZIMMERMANN TELEGRAM

On the first day of hostilities, the British cable ship TELCONIA located and cut Germany’s trans-Alantic cables, forcing them to send all their international traffic via Sweden or American-owned cables. Both means ran through the UK and soon all German traffic was routinely routed to ROOM 40, the Royal Navy’s cypher organisation.

On or about January 16, 1917 two Room 40 cryptanalists WILLIAM MONTGOMERY and NIGEL DE GRAY, were given a message encrypted in the German Foreign Office code, a BOOK CYPHER number 0075. By the next morning they had deduced enough of the message to be chilled by its content. Sent by the German Foreign Minister ZIMMERMANN to the Mexican President via the German Embassies in Washington and Mexico City, it advised the President of Mexico that Germany proposed to start unrestricted submarine warfare in February and that he should, with German help, attack the US and also convince the Japanese to do the same.

In short order the full text was recovered and presented to US President WILSON. On April 2, 1917 the then neutral US declared war on Germany and by 1918 Germany had been defeated.

To obscure the source of the original intercept, and to point to a security breach in Mexico, Room 40, using a British agent in Mexico, obtained a copy of the edited US/MEXICO version of the original Zimmermann cable. This of course differed from the original for procedural reasons associated with its re-transmission from Washington to Mexico City. The decrypt of this was the copy released to the US press its use obscuring the fact that the British had obtained their information not from espionage in Mexico but decryption of the original telegram in London. The Germans spotted the difference and took the bait. The deception was complete and the source was safe. The code breakers of room 40 were yet to benefit from the pen of Winston Churchill or their own historians!

Towards the end of WWI the head of cryptographic research for the US Army MAJOR JOSEPH MAUBORGNE introduced the concept of a code based on truly RANDOM keys. This would take the form of two identical pads printed with lines of randomly generated letters. Using the Vigenere technique, each page is to be used to encrypt and decrypt ONE message and then destroyed. The weakness of the Vigenere square was the repetition of the key. This new technique injected the same randomness into the cyphertext as was contained in the key and there was therefore no usable pattern or structure within the message. Attacks seeking to exploit these weaknesses such as the Babbage and Kasiski tests, would fail.

A key length of as little as 21 letters meant that a KEY EXHAUSTION attack, the cryptographic equivalent of Custer's last stand, would require the testing of 500 x 10^{27} keys and even then multiple decrypts may all appear plausible.

This method is still in use today, called the ONE TIME LETTER PAD or OTLP, and is used for encrypting the most secret of communications. OTLP is still the only 'admitted' system to provide the 'holy grail' of cryptography – perfect secrecy.

THE NOT QUITE SO DISTANT PAST

There can be no doubt that times of conflict focus both national identity and national capability. This in turn leads to accelerated sociological and technological change. The first world war showed the importance of cryptography on the battlefield, and the danger of weak encryption, and spawned the development of the 'unbreakable' one time letter pad. The second world war became a defining moment in the history of cryptography and placed it squarely at the center of military and political strategy from that time to the present day.

Struggling under the weight of axis forces in the west and Japan in the east, the use of encryption by the allied nations and the interception and decryption of enemy cyphers became a game of life and death.

In the evening of 13.04.1943 the headquarters of the Japanese 8th fleet sent messages concerning the itinerary for a visit by the commander in chief (CIC) of the Japanese Fleet. To protect this vital information, the message was encrypted using Japanese Naval code 25 or JN-25. This message, like many others, was intercepted by a US intercept station in Hawaii and the Royal Australian Airforce #1 Wireless Unit in Townsville, North Queensland. Unknown to the Japanese or, as some suggest, suspected but ignored, the Americans had broken this code in late 1940 it having been a subset of a US army and navy code used in the Spanish-American war of 1898,. The allies ability to intercept and decrypt this message led directly to the shooting down of aircraft carrying ADMIRAL YAMAMOTO, over Bougainville, on the morning of 18.04.1943, by a United States P-38 Lightning piloted by CAPT THOMAS G. LAMPHIER. This resulted in the death of the most popular and, many say, capable officer in the Japanese navy robbing them of a brilliant and charismatic leader.

As an adjunct to this, on the occasion of the 50th anniversary of the Australian Defence Signals Directorate (DSD) their wartime allies, the United States of America, the United Kingdom, New Zealand and Canada made presentations. Underscoring under the importance of this war time codebreaking the US National Security Agency (NSA) presented DSD with a trophy containing one of the only 5 remaining rotors of a Japanese 'PURPLE' cypher machine.

For those with a penchant for conspiracy theories concerning other decryptions of JN-25 and associated radio traffic the book *Betrayal at Pearl Harbor* makes interesting reading. In this book the authors (one a respected WWII cryptographer - CAPT ERIC NAVE) argue that the British government intercepted all of the 'winds' messages, Japanese radio traffic which identified the time of the Pearl Harbour attack. They also suggest that the British failed to alert the Americans in the hope that this would drag them into the war, which of course it did. Michael Smith, author of *Station X* and *The Emperor's Codes* suggests that based on Nave's unpublished autobiography held at the Australian War Memorial that, despite the book, he did not subscribe to the conspiracy theory and his views were distorted by his co-author (*The Emperor's Codes 278).*

More widely known and reported today is the importance to the war effort of ULTRA, the British codeword for SIGINT derived from the decryption of Axis radio messages and, in particular, from the efforts and results of many hundreds of people dedicated to the decryption of German ENIGMA traffic.

The ENIGMA machine was developed by a German ARTHUR SCHERBIUS and was patented in 1919. Despite a lack of commercial success and after several improvements, the machine was adopted by the German Navy in 1926, the Army in 1928 and the Air Force in 1935. It was also introduced into service with other sections of the German government. Such an extensive use of Enigma being due almost entirely to revelations regarding British decryption of German wartime messages made by Winston Churchill in his book *World Crisis* published in 1926. This cryptographic door opened by Churchill was taken of its hinges in the same year by the official war history of the British Royal Navy and the exploits of Room 40. Scherbius's Enigma could not have received better publicity. The secrecy that surrounds western codes and code breaking today can be traced almost directly to the impact of these and several other publications. The watchword today is 'never give a sucker an even chance'. The jibe often directed at the NSA suggesting that their initials stand for 'never say anything' is, for them, not very far from the truth.

Unfortunately for the WWI allies their decryption of almost all German cypher traffic had ceased by early 1930 because of the introduction of the Enigma.

The Enigma is referred to as an OFF LINE cypher system which was designed to provide high-grade cyphertext from the input of plaintext and the reverse. Enigma was a manual system whereby each plaintext letter was typed on the KEYBOARD (*TASTATUR*) and the resultant cyphertext letter appeared illuminated on the LAMP BOARD (*GLUHLAMPENFELD*). This letter was transcribed on a message pad and the procedure repeated until the message was complete. This cyphertext message was then transmitted by radio using Morse code. Decryption followed the same procedure with the cyphertext letter typed in and the plaintext equivalent displayed on the lamp board.

Although much has been written about British efforts against Enigma, they were not the first. The first crack in the ENIGMA armour came not from brilliant cryptanalysis but as the result of good old fashioned espionage (HUMINT). In late 1931 a disgruntled German public servant allowed, for a fee, a French secret service agent to photograph two ENIGMA instruction manuals which, while non-technical, contained sufficient information to deduce the internal wiring of the machine. The French, despite their previous brilliant wartime cryptanalysis, failed to capitalise on this windfall. Luckily for the British, copies of the manuals were given to Poland under an intelligence-sharing agreement. A brilliant young mathematician MARIAN REJEWSKI began work on this seemingly 'impossible' task. Within 18 months the Poles, without revealing their success, were able, by manual means, to recover a 'day key' and read Enigma traffic. When the Germans changed the transmission technique, a mechanical device, comprising six separate machines in total, was developed to extract the key. This was the first of many *BOMBE's* which were to become synonymous with British code breaking at BLETCHLEY PARK. This success continued until 1938 when two new scrambler wheels (4&5) and 4 more plug board (*STEKERBRETT*) connections were added. With war imminent and without resources to build larger bombes the Poles considered the common good. On July 24th 1939 British and French cryptnalysts arrived at the Polish BOURO SZYFROW to be told of Rejewski's success, almost a decade of successful Enigma decryption, and not only to be shown a bombe but to be given one each with the accompanying blue prints. There is no doubt that without this exceptional work done by the Poles prior to the start of WW2 the immensity and complexity of the British wartime decryption task may have defeated them.

The Poles had proven that, despite the apparent strength of the Enigma, there were weak points, and these, along with others discovered by the British, were used to great effect. The Enigma was, in terms of its internal architecture, a swapping machine and, as such, two machines set the same would give the same result. Key X to get C or Key C to get X. This meant that once the 'setting' or 'day key' was found, all messages using that setting could be decrypted. There was no internal dynamic update of the key based on the message traffic or any other variable. In addition keying X would not give X. This latter weakness was used to great effect when applying 'cribs', 'ordered or known text that provide clues to breaking a cypher' such as Dear Sir, or Heil Hitler!

Decrypts of Enigma traffic produced many results for the allies. Despite being warned of the German airborne landing on Crete, the allied forces were defeated because they were forbidden to pre-empt the attack in case the source of their information was deduced. Despite a recent (2000) American movie which attempted to rewrite history, British work on the decryption of the German naval Enigma which had more rotors than a 'normal' machine, and associated military operations designed to capture code books, led directly to the defeat of the U-boat offensive in the Atlantic and the saving of countless lives on both sides.

A LEGACY OF WAR

OPERATION VENONA (OR NEVER THROW ANYTHING AWAY)

The British began successful SIGINT activities against Russia in 1904. This success continued until British politicians, and the media, made public detailed transcripts of intercepted and decrypted Soviet traffic first in AUGUST 1920 then May 1923 and finally May 1927. Although the roubel didn't quite drop on the first two occasions, on the third occasion, the Soviets finally got the message and replaced the compromised codes on all their OGPU (KGB) and diplomatic networks with OTLP. This resulted in a complete loss to Britain of Soviet intercept traffic from 1927 to the early 1940s. This, coupled with the literary indiscretions of Churchill and the Royal Navy historians are blunders which are almost impossible to believe, but sadly, which occurred. After ceasing all work in the early 1930's because of the perceived impossibility of the task, the British began intercepting Russian traffic again in 1940. By 1941 the intercepts were being shared with the US. This intercept work and its associated sharing agreement continued during and after the war, culminating in 1947,1948 in the UKUSA agreement (which also included Australia, New Zealand, and Canada).

While OTLP offers complete security in theory, this is not true if the pads are reused, or, if either the original plain text, or the used pages or current code books fall into the interceptors hands. During the war years, for a variety of reasons, all these events occurred.

In the view of the western allies, the Soviets were not the 'good guys' despite their alliance against Germany and Japan.

The US VENONA project began at ARLINGTON HALL Virginia in February 1943 and by 1947 had broken into a considerable amount of traffic including 1945 KGB traffic between Moscow and Canberra. Supplemented by a similar UK effort, they were able, by the early 1950's, to identify Soviet agents in their respective intelligence and government services and the existence and makeup of a major Soviet spy ring in Australia.

Despite preventing access for almost 20 years the Soviets had, at a most critical time, compromised the security of their global spy network by their failure to follow simple security rules.

THE BEGINNING OF THE FUTURE

The 1980's and '90's have evolved into a digital world. The advent of the microprocessor and the personal computer (PC) and their acceptance into every-day life has meant that although our primary means of communication is the spoken word the 'lingua franka' of our working lives, and increasingly our private lives, is digital. This digital dialect has spawned vast communications networks (INTERNET, DIGITAL (GSM) MOBILE PHONES, AUTOMATIC TELLER MACHINES (ATM)) offering instant 'secure' communication. These networks increasingly carry the most mundane, private and sensitive messages of ordinary citizens, business, government, and all manner of criminals and terrorists. The future of ELECTRONIC COMMERCE (E-COMMERCE) and, in fact, the electronic world, rests on secure digital communication. Unfortunately, so does the success of drug rings, people smugglers, child porn, organised crime, spy rings, and 'cyber crime'.

Legitimate governments and law enforcement bodies want 'transparent' or KEY ESCROW encryption (CLIPPER) to fight crime and ensure national security. This technique, although now all but discredited as a US government 'Trojan horse', was designed to allow government/law enforcement to obtain one's secret key if they established that one was involved in illegal activities. Other governments ban digital security to harass political opposition and quell dissent. Lobby groups, conspiracy theorists, oppressed minorities, distrustful and disgruntled citizens all want triple military-grade encryption fitted to their 'fly-by' cards.

The arguments for and against are many. Do you have anything to hide? Do you trust your government? Do you trust the French government since the Rainbow Warrior? Do you trust the US government since the Bay of Pigs or the 'Contra' affair? Do you trust your lover, business partner, bank, or the florist? Are you or others at risk because of your political, religious or ethnic heritage? The applications of modern digital encryption are endless and should be applied in direct proportion to your level of paranoia or to the threat to your life and liberty.

DES – DATA ENCRYPTION STANDARD

In 1972 the US NATIONAL BUREAU OF STANDARDS began the search for an encryption algorithm that could be tested and certified. After several false starts in 1974 IBM offered the US government an algorithm which was based on the early 1970's LUFICER algorithm. The offer was accepted and the algorithm was tested and 'adjusted' by the NSA and eventually released as a federal standard in 1976.

DES is a SYMMETRIC BLOCK cypher based on a 64 bit block. The user feeds in a 64 block of plain text and is returned 64 bits of cyphertext. The same algorithm and key are used for the encrypt and decrypt operations.

Since its release in 1976 the key has remained fixed at 56 bits (reduced from a 128 bit key as part of the NSA 'adjustment') although it was possible to 'build' DES with a 128 bit key, exporting it from the US was banned. Recently however this key length restriction was removed by the US Government.

Much has been written about the security of DES and the hand of the NSA in its design. Constant analysis over the last 20 years has nor really compromised its basic security. Some high profile decrypts have come as the result of reduced 'rounds' and other 'manufactured' situations. Is it good enough for personal or commercial use? - probably. Should the big guy in Baghdad send his travel plans using it? – we don't think so.

PGP – PRETTY GOOD PRIVACY

This software package is designed to provide an encryption capability for e-mail and was originally developed by PHILIP ZIMMERMANN who began working on the algorithm in the late 1980's. The development of this system was as much about Zimmermann's distrust of the US Federal Government and its ability to intercept electronic communication as the development of a commercial cryptographic product. The history of this system has two interesting facets. Initially, an unlicensed implementation of RSA was used to provide key management while the IDEA algorithm was used to provide the actual data encryption layer. Because of Zimmermann's distrust of the US government, the complete package was downloaded onto the Internet so that it could be distributed as free ware. This, of course, created maximum heart-burn for the US government and led to their ill considered use of pressure on him which in turn reinforced his position.

DIFFE-HELLMAN-MERKEL KEY EXCHANGE

WHITFIELD DIFFE was already considering the problems of e-commerce when the US defence department's ARPA Net, the forerunner of the Internet, was still in its infancy. In 1974 he teamed with MARTIN HELLMAN and later RALPH MERKLE to begin research into the problem of key exchange.

By 1976, using one-way functions and modular arithmetic, Hellman had developed a strategy to solve the key exchange problem. In June 1976 at the US National Computer Conference, they demonstrated that Bob no longer had to meet Alice to exchange a secret key. While this was a fundamental breakthrough in conceptual terms, it did not offer a 'real world' solution to the problem of key exchange. While working on the key exchange problem with Hellman and Merkel, Diffe had continued to ponder a solution for the obvious problems of the key exchange technique. In 1975 he developed the concept of the ASYMMETRIC KEY which opened the possibility of operating a crypto system with a PUBLIC (published) and PRIVATE (secret) key. He also published a paper on his work in the same year while continuing to look for the one way function that would make his theory a reality. He never made that connection and the first (then) known developers of an asymmetric key system would be the inventors of RSA

RSA

This algorithm, based on the original work of Diffe, was named after the three inventors Ron Rivest, Adi Shamir and Leonard Adleman. This is an ASYMMETRIC cypher and as such is able to be used for PUBLIC KEY CRYPTOGRAPHY. In simple terms you can send Bob a message encrypted with his PUBLIC/PUBLISHED key and when he has received it he can decrypt it with his SECRET/PRIVATE key (from which his public key was derived). The security of this system is based on the difficulty in FACTORING large numbers. The private and public keys can be functions of large (300-400 digit) prime numbers. While the process is known, recovering the plain text from the public key is considered to be the equivalent to factoring the product of the two prime numbers. With large numbers this is considered a **MAJOR** computational task, even by to-days standards, and is **believed** to be, in terms of time, beyond the capability of any existing technique/computer combination.

As a footnote to this, and to explain the reason that we used 'believed' in the previous paragraph, it was revealed in December 1997 in a talk given by Clifford Cocks that he, along with James Ellis, and Malcolm Williamson, all employees of the British GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ) had, as the result of classified research, discovered all the fundamental techniques of public key cryptography by 1975, some three years before the Diffe-Hellerman key exchange or RSA technique were developed. Because of who they were and where they worked it took another 25 years before they put their hands up.

PLEASE NOTE

This is not intended to be a scholarly work nor to be an exhaustive treatment of either the methods or history of cryptology. The fact and fiction of this discipline is endless. Our intention in presenting this material is to provide interested persons, often school students, with basic information and links to resources that might assist them. We welcome suggestions, corrections, additions.

WORKS CONSULTED

'THE CODEBREAKERS' David Kahn, Sphere Books 1977

'CODE BREAKERS' edited by F.H. Hinsley and Alan Stripp, Oxford University Press 1994

'THE EAVESDROPPERS' Jack Bleakley, AGPS 1991

'BREAKING THE CODES' Desmond Ball & David Horner, Allen and Unwin 1998

'THE CODE BOOK' Simon Singh, The Fourth Estate 1999

'APPLIED CRYPTOGRAPHY' 2nd Edition Bruce Schneier, John Wiley & Sons 1996

'COURSE IN CRYPTOGRAPHY' General Marcel Givierge, Aegean Park Press 1978

'INTRODUCTION TO CRYPTOLOGY & PC SECURITY' Brian Beckett, McGraw Hill 1997

‘THE PUZZLE PALACE’ James Bamford, Penguin Books 1983

‘BETRAYAL AT PEARL HARBOR’ James Rusbridge & Eric Nave, Summit Books 1991

‘STATION X THE CODEBREAKERS OF BLETCHLEY PARK’ Michael Smith, Ch 4 Books 1998

‘THE US INTELLIGENCE COMMUNITY’ 4th Edition Jeffery T Richelson, Westview Press 1999

‘THE EMPEROR’S CODES’ Michael Smith, Bantam Press 2000

Today, most books can be purchased on the internet, and that many do just that. We still buy books for our library the old fashioned way, from a book store. We normally purchase titles from the TECHNICAL BOOK AND MAGAZINE COMPANY in Melbourne Victoria. The books in this list were purchased from them. This company has provided us with good service for more than twenty years and they are always happy to chase down the most obscure titles.