CHAPTER 8

A History of Communications Security in New Zealand

By Eric Morgon

Early Days

"Admiralty to Britannia Wellington. Comence hostilities at once with Germany in accordance with War Standing Orders." This is an entry in the cipher log of HMS Philomel dated 5 August, 1914.

HMS Philomel was a cruiser of the Royal Navy and took part in the naval operations in the Dardanelles during the ill-fated Gallipoli campaign. Philomel's cipher logs covering the period 1914 to 1918 make interesting reading and show how codes and ciphers were used extensively by the Royal Navy during World War 1. New Zealand officers and ratings served on board Philomel and thus it can be claimed that the use of codes and ciphers by Philomel are part of the early history of communications security in New Zealand.

Immediately following the codes to Navy Office, the Senior Naval Officer New Zealand was advised that Cypher G and Cypher M had been compromised and that telegrams received by landline in these ciphers were to be recoded in Code C before transmission by Wireless Telegraphy (W/T) Apparently Cypher G was also used for cables between the Commonwealth Navy Board in Melbourne and he British Consul in Noumea. The Rear Admiral Commanding Her Majesty's Australian Fleet instructed that when signalling by WT every odd numbered code group was to be a dummy.

It is interesting to note that up until the outbreak of hostilities no provision had been made for the storage of code books or for precautions to prevent them from falling into enemy hands. In October, 1914, Admiralty gave instructions that a perforated metal box was to be prepared immediately in each ship for the stowage of confidential books and pamphlets in use in coding in the W/T office. The box was to be capable of being closed quickly and securely and code books were to be kept in the box except when actually in use. The instruction concluded with the sentence,"...The sinking power when full of books is to be tested on first opportunity." One wonders how literally this was interpreted by the ship"s signal staff!

While in the South Pacific, Philomel read messages concerning the operation of the German warships Gneisenau, Nurnberg, Leipzig and in particular the Emden which was causing havoc among merchant shipping in the Pacific. When finally the Emden was chased and trapped in the Cocos Islands by HMAS Sydney W/T played an important part in the action. The signal recorded in Philomel's cipher log on 9 November, 1914, reads, "Emden located in Cocos Islands this morning 9 November. Chased and engaged by Sydney and beached herself to avoid sinking. Sydney casualties 2 men killed, 13 wounded. Sydney standing by wreck of Emden after having chased and sunk Emden's collier. Great credit attached to wireless telegraph operator at Cocos Island who stuck to his post and gave warnings of Emden."

HMS Philomel reached Port Said on 2 February 1915 and shortly after was engaged in action off Alexandretta. On 16 February, as a result of a threat by the Turkish Military Commander of Alexandretta to murder British hostages, Philomel was instructed to issue a grave warning to the Commandant that if murder was committed his life and that of the Turkish Commander in Chief and all others concerned would "most assuredly be brief". Philomel was told to use Code C until further notice.

On 24 February, Allied Fleet Recognition Signals were brought into force and ships were advised that challenge and reply between ships of the Allied Squadron were always to be as laid down in the Allied Fleets Signal Book. On 23 March, the W/T Code (1914) and Cypher D were brought into force. During this period Philomel's cypher log also makes mention of the Playfair Code being used to Troop Transports, the MV (Merchant Vessels) Code

and the Economic Telegraph Code. The latter is presumed to be an unsecure code since HM ships were told not to use it unless the message had to repeated to a French ship.

In January, 11917, Philomel was overdue for a long and extensive refit and the Admiralty ordered her to return to New Zealand to pay off without recommissioning. Philomel left the Persian Gulf on 30 January 1917 and arrived in New Zealand on 16 March, 1917. Three weeks later on 7 April her cipher log records the receipt of a signal from Admiralty advising that a declaration of war between the United States and Germany had been signed by President Wilson. However, although Philomel was out of the war her log continued to record changes in the codes and ciphers used during the remaining months of the war. On 11 November, 1918, a message from Admiralty advised SNO NZ that the Armistice had been signed. On 13 June, 1919 a message from Admiralty warned that hostilities would be resumed if Germany did not sign the Treaty of Peace. Germany finally signed on 28 June 1919 and only then was World War 1 formally terminated.

As we have already read, the Playfair Code was used by the Royal Navy when communicating with troop transports. The first recorded use of Playfair in New Zealand Army documents is in a memorandum dated January 1917 from N.Z. Military Forces Headquarters in Wellington to Masters and Officers in charge of Troops on board transports en route to the war zone. The memorandum gives instructions that messages should be coded and despatched in Playfair code.

According to David Kahn in his book “Codebreakers”” the Playfair Code was first demonstrated in 1854. It was possibly used in the Boer War and was adopted by the British Army as a field system during World War 1. Twenty years later the Playfair code was still considered to be relatively secure and in February, 1941 the N.Z. War Cabinet approved the use of Playfair to secure commercial messages sent by wireless between N.Z. and the Pacific Islands. In September, 1945 the Playfair code was withdrawn and replaced by a one-time-pad system almost one hundred years after it was first demonstrated.

But to return to the period before World War 2, during these early pre-war das, secure book syphers were used by the military forces and government departments. Naval cipher logs covering the period 1927 to 1929 show that the Navy Office, Wellington held a General Cypher, the Interdepartmental Cypher, a Small Ships Cypher, Flag Officers Cypher used for messages to and from Admiralty, a Reporting Officers Cypher, a Peace Code and a Fleet Code. Recyphering tables on a regular basis were used with most cipher systems. In 1929 copies of the Colonial cypher were loaned by the British High Commission in Government House Wellington to the Department of External Affairs for confidential despatches between Wellington and Samoa. In 1934 Admiralty issued a new cipher “Admiralty Cypher No.1” and a new code “Administrative Code” to replace the General Cypher and Fleet Code Volume 2. The Administrative Code was not recoded for unclassified messages but was to be recoded with special tables for Secret or Confidential messages. By 1938, copies of the Interdepartmental cipher and the associated recyphering tables were held by the Governor General, the Prime Minister, Navy Office, Army and Air Force Headquarters, Wellington.

It was during these early years that the idea of national control of codes and ciphers originated. In 1920 an advisory committee on Defence was formed to report confidentially to the Minister of Defence on problems of defence and important policy questions. However, it was not until 1933 that the N.Z. Committee of Imperial Defence was set up to organise national activities so that all departments of state were in a position to deal immediately and effectively with duties which could develop on the threat of war or actual outbreak of hostilities.

In 1936 the NZCID was retitled the Organisation of National Security (ONS) to avoid confusion with the Committee of Imperial Defence in England. The co-ordination of defence activities was effected by the ONS by means of inter-departmental committees, one of which was the War Book Committee. It was at a meeting of this committee in February 1939 that it was decided to form a special sub committee to consider the question of the supply of ciphers. Only a few months previously, the ONS had expressed concern that the existing cipher staffs

of Government House and the Prime Minister's Department would be insufficient in an emergency. During September and October 1938 Navy Office conducted cipher training for 11 officers from the Posts and Telegraph Department, Air Department, Navy Office and the British Trade Commissioners Office. By this time an Administrative Code and Cypher had been introduced and on the same date, 11 February 1937, the Peace Code had been withdrawn.

Navy Office therefore provided instruction on the Government Telegraph Code, Administrative Code, Administrative Cypher, Reporting Officer's Code and Reporting Officer's cipher. In addition Naval Office staff were given instruction in Naval Cypher, Interservice Stencil Cypher and RAF Station Cypher. The last named cipher both low grade and high grade was used between Navy Office and RAF authorities concerning the Walrus aircraft which operated from HMS Achilles.

At the first meeting of the special sub committee on cipher in February, 1939, it was agreed that there should be a central cipher pool for handling of outward Government telegrams excepting those of the three fighting services. As practically all messages were required to emanate under the signature of the Prime Minister, it was considered that the cipher pool should be attached to the Prime Minister's Department. The cipher to be used would be either the the Dominions Office Cypher..."which is moderately secure"... or the Interdepartmental Cypher...which "is absolutely secure".. The Post and Telegraph Department agreed to release a further 8 officers to be trained in the use of various ciphers employed by the Navy Office and Government House. It was felt that those officers selected for cipher training should be ..."about twenty years of age with a good knowledge of English, smart at figuring and of a superior personality..." It is no wonder that ever since that time, cipher staffs have considered themselves to be "superior beings!

The War Book Committee continued to function throughout the war but there is no further record of the cipher sub committee. The move to form a national committee responsible for cipher security did not come until after the war but interestingly enough, the first Chairman of the committee was a member of the War Book Secretariat.

On the 27th September, 1938, during the Czechoslovakian crisis a message was received in Flag Officers Cypher from the Admiralty giving advance warning of possible general mobilisation being ordered the following day as a precautionary measure against Germany. On the 28th, two further immediate telegrams were received from Admiralty in cipher. The first one gave the codeword SERVICE and the second STROKE MAST. The significance of the first telegram "Mobilise in accordance with instructions for war with a European Power." The second telegram meant "Mobilise Naval Reserves. Retain Time Expired mrn." The following day Navy Office signalled Commodore Commanding the N.Z. Squadron with the codeword SUSPEND which signified "The discharge of Imperial ratings in the NZ Squadron is suspended. NZ ratings permitted to take discharge until promulgation of a state of emergency when message PROCLAMATION will be sent signifying that the discharge of time expired NZ ratings is suspended." The same day Admiralty signalled Navy Office in Naval Cypher (which was handled only by officers) with the information that Lloyds had reported that all German shipping lines had recalled all their vessels on the high seas. German W/T stations broadcast the recall to merchant ships using the prefix BLIND which meant that the ship did not answer.

As we know, the British Prime Minister, Neville Chamberlain returned from a meeting with Hitler in Munich with the message "Peace with Honour". The Czechoslovakian crisis had been averted. On 5 October Admiralty signalled Wellington in Administrative Cypher that the international situation was generally stable but the mobilisation of the British Fleet would continue on account of the experience gained to all concerned. A further signal enciphered in Flag Officers Cypher advised CCNZS that he could retain any officers called up locally until they could be spared. The remainder could be released but should remain liable to recall should the necessity again arise. Finally, on 25 November the state of emergency was formally terminated and the order to mobilise was suspended.

Although the immediate threat of war had been averted, the Admiralty continued to make preparations to improve communications security in time of war. In April 1939 they advised the Governor General, Viscount Galway, that arrangements were being made to provide British merchant ships with secret W/T callsigns for use when rendering certain reports or when confidential official messages are addressed to particular merchant ships. It was considered preferable to issue these callsigns in time of peace to avoid the delays that would occur in issuing them on the outbreak of hostilities. Each individual callsign together with instructions for its use was to be placed in a double sealed envelope marked "Secret Envelope Z". The authority to open Secret Envelope Z and bring the secret callsign into force was broadcast by W/T as an Admiralty message "B" which contained Wireless Instructions Nos 1 & 2 and instructions to open the envelope. Secret callsigns were to be used for reporting enemy warships, enemy aircraft, or of a moored mine cut by a paravane. They were to be used for messages coded in Merchant Navy Code and for cancelling a false report of a submarine. Navy Office Wellington adopted this procedure and secret callsigns were used by merchant ships registered in New Zealand. Secret envelopes Z were issued by Navy Office to ships operating in New Zealand coastal waters and throughout the Pacific.

Codes & Cyphers in World War 2

When the war started New Zealand was still using book ciphers which had hardly changed since World War 1. Not only was the Playfair code in use in the Pacific Islands but in July 1940 the Ministry of Supply authorised New Zealand Trade Commissioners abroad to use Bentley's Second Phrase Code if it was considered indiscreet or expensive to despatch messages in clear. The Playfair code was to be reserved for secret messages. In March 1941 the War Cabinet issued an instruction that all commercial messages sent by Wireless Telegraphy (W/T) to or from the Chathams, Niue, Raratonga, and the Kermadec Islands should be encoded in the Playfair code. The use of commercial codes such as the Government Telegraph Code and Bentley's code was cancelled and smaller islands were instructed to use the native language when no codes were available. Considerable precautions were taken to preserve the security of the Playfair code and as many as 100 different key words were used and regularly changed. Navy Office continued to use the more secure interdepartmental Cypher for secret messages between New Zealand and certain authorities such as the Resident Naval Officer Suva and the High Commissioner Suva and to Army and Navy Offices in Melbourne.

The Playfair code was also used extensively by the coastwatching stations in the Pacific. In November 1942, Navy Office advised the N.Z. Naval Liaison Officer in Suva that it was certain that the Japanese were aware of the type of code in use for communications with British coastwatching stations in the Pacific as well as the W/T frequencies used. It was considered that even with frequent changes of keywords no message sent in Playfair code was secure for more than a few hours at the most. Therefore to deny the enemy of even the smallest amount of information, messages should not be transmitted to coastwatching stations except in exceptional circumstances, other than short innocuous words such as YES, NO, CONCUR etc.

In June, 1945 the Joint Communications Board came to the conclusion which was confirmed by the Chiefs of Staff that it would be impracticable to discontinue the use of codes altogether at that stage of the war. The Board decided that in view of the limited security value of the Playfair code it should be replaced by a more secure code and that a one-time letter code should be made available. The Navy view was that the transmitters in use at Wellington, Chathams, Niue, Rarotonga, Apia and the Kermadecs were of sufficient power for their transmissions to be picked up in Japan but that the transmitters of the outstations centering on Apia and Rarotonga were not. It was therefore decided to withdraw Playfair code from all islands and provide the islands which used high-powered transmitters with both IN and OUT pads of one-time letter code. The minor stations were to be provided with IN pads only for the receipt of traffic. The use of codes for commercial traffic was considered no longer necessary.

More secure ciphers were used by the fighting services. As mentioned in Chapter 1, secure book cipher systems were in use by Navy Office and Commodore Commanding the New Zealand Squadron before the war. In April, 1940, General Freyberg, Commander of the New Zealand Expeditionary Forces in Egypt was supplied with the Interdepartmental Cypher to allow direct secret communications with the New Zealand Government in Wellington without the the necessity of despatching messages through Army headquarters. The 1936 edition of the Interdepartmental cipher was at this time held by the Governor General, Viscount Galway who received two copies from the Dominions Office in London.

In May 1940 the Commodore Commanding the N.Z. Naval Squadron was receiving copies of the Naval Cypher, the Administrative Code, Auxiliary Code and the Merchant Navy Code. By the end of 1940 "one-time" pad subtractor recyphering tables were in use with figure ciphers. Subtractor tables consisting of numbered IN tables and correspondingly numbered OUT tables were intended for single line communications either for vulnerable posts or for any special purpose for which added security was considered essential. In December 1940 when Naval staff was considering distributing these tables to Pacific Islands, one staff officer commented, "...our coding and ciphering systems seem to be coming more complicated every day."

While the book ciphers and subtractor tables employed by the services and government departments were certainly more secure than Playfair code or Bentley's Second Phrase Code, nevertheless they were time-consuming in use and prone to arithmetical error. In addition, the system suffered from a primary disadvantage in that if any one set of code books was captured or compromised new sets had to be issued to all users, and in wartime tha could be a very lengthy procedure.

With the benefit of hindsight we know that most of these codes nd ciphers were already compromised before they were received New Zealand. The Administrative Code had been used before the war both with and without the subtractor tables and this had enabled the German naval B-Dienst to break the code and its tables. By the outbreak of war the Germans were reading traffic in this system extensively. Success with the Administrative Code enabled B-Dienst to break the Naval Cypher ad by April 1940 they were reading 30 to 50 percent of intercepted traffic. On 20 August 1940 Naval Cypher nO.2 replaced Naval Cypher No.1 and on the same date Naval Code No.1 replaced the Administrative Code. Because of improvements to the security of the long subtractor system, B-Dienst success against Naval Cypher No.2 was comparatively limited but in September 1941 an indicator procedure as abandoned for a much weaker one. From then until January 1942 when Cypher No.4 replaced No.2, B-Dienst again succeeded in reading a good deal of traffic in generally held tables. Fortunately by October 1942 Naval Cypher No.4 had been reconstructed to an extent that the enemy was unable to achieve results comparable to its success against the previous No.1 and No.2 cyphers.

While it is not part of the New Zealand story, it is worth noting that Naval Cypher No.3 was employed by the British, US and Canadian Navies in the Atlantic. To begin with it was used without the improvements the long subtractor tables which had been applied to Cyphers No.2 and No.4. As a result the enemy was sometimes obtaining decrypts about convoy movements between 10 and 20 hours in advance and was able to decrypt the daily signal in which the Admiralty issued its estimate of U-boat dispositions. From November 1943 the Naval Cypher was being progressively replaced for British/Canadian/US communications in the Atlantic with the Combined Cypher Machine (CCM) against which the enemy made no progress.

The Merchant Navy Code which was also held by the Commodore Commanding the New Zealand Naval Squadron was a simple recoding system. By March1940, B-Dienst was having some success in decrypting this system and it was greatly helped by the capture of copies of the Merchant Navy Code at Bergen in May 1940 after which it was able to read the bulk of the traffic with little delay. Reading the Merchant Navy Code was of substantial assistance to B-Dienst's work on Naval Cypher No.3 since it contained intelligence about convoys and stragglers..

The Inter-Departmental Cypher issued to General Freyberg in April 1940 was also compromised. A basic book with subtractor tables it was held by the British Foreign Service, the Colonial Dominions and India Offices and the British services. The Germans captured the basic book at Bergen in the summer of 1940 and soon broke the system. Until June 1943 when the Germans stopped work on it, it provided valuable political intelligence and information about merchant shipping. It is not known whether the Germans ever intercepted General Freyberg's messages but certainly if they had, the information they contained would have been compromised.

The story of Enigma and the introduction of machine cipher systems is well documented in other histories concerning codes and ciphers but its connection with the Typex system used by the New Zealand Government is worth recording here. Enigma was adopted by the German Navy in 1926, by the German Army in 1928 and by the Luftwaffe in 1934. The British were also considering the replacement of book systems by cipher machines and in 1928 two commercial Enigma machines were purchased at Admiralty initiative. It was not until 1935 however, that it was decided that Air Ministry should arrange for the construction of three sets of cipher machines of an improved Enigma type. Air Ministry commissioned Creed & Company, a commercial teleprinter manufacturer to produce copies of the commercial Enigma. By March 1936 Creeds had made two copies which became known as the RAF Enigma with Type X attachments and subsequently as "Typex". The Air Ministry adopted Typex before the outbreak of war and by September 1939 it was in use at all RAF HQs. It proved to be completely secure for more important RAF ground-to-ground communications throughout the war. British War Office adopted Typex before the war and by September 1939 this system which remained secure throughout the war, was in use between the war office and commands, at home and overseas and within commands down to division level.

Typex was not used at sea by the Royal Navy during the war but the Combined Cypher Machine (CCM) was used from November, 1943 and it was eventually held by all HM ships. CCM was based on the US Electrical Cypher Machine (ECM) and the British Typex machine which had been made available to the US on their entry into the war. By an agreement in June 1942 the US undertook to modify the ECM to work with Typex and develop an adaptor for the latter. The modified ECM and Typex machines became different marks of the CCM. Like Typex, CCM proved to be totally secure and the Germans made no serious attempt to solve either system..

By April 1941 Typex had been adopted by service departments in Canada and the Union of South Africa and was being considered by Australia. Ten Typex machines were supplied by the British government for use by N.Z. government authorities nominally without charge but in the event the N.Z. Government insisted on payment and the cost of 145 pounds [$290] for each machine was finally paid in 1947. In June 1941 the Navy Department with the concurrence of Admiralty, made one machine available on loan to the Prime Minister's Department. In December of that year, Air Department assumed responsibility for the inspection and maintenance of all Typex machines used by service departments, the Prime Minister's Department and the U.K. High Commissioner's Office. In May 1942 Dominion drums and settings were held by the Prime Minister's Departments in New Zealand and Australia, the Department of External Affairs in Canada and the Union of South Africa, the Governors of Newfoundland and of Southern Rhodesia and United Kingdom High Commissioners in Australia, New Zealand, Canada, and the Union of South Africa.

Typex machines remained in service in New Zealand after the war until they were replaced by modern machine systems. The RNZAF destroyed Typex in 1963 but the last machines in use by the Ministry of Foreign Affairs were dumped at sea some ten years later. An ignominious end after 30 years of loyal service! Fortunately, one was salvaged and is held in GCSB archives for future display in a museum of cryptology.

Chapter 3

The Post War Years 1945-1960 .

The end of hostilities in Europe and the Pacific found the New Zealand services and government departments using a mixture of machine and book cypher systems. The Navy and Army were using the Combined Cypher Machine (CM) which was a Typex Mark machine adapted for and held with special adaptors tenable the New Zealand forces to operate with American services. The Air Force and the Department of External Affairs were both using Typex. On 1 January 1950 Typex Mark 2 and Mark 3 were superseded by the Mark 22 and 23 [BI/08/2 & BID/08/3] the latter being a Mark 22 modified for use with the CCM adaptor. Both these models were fitted with the crossover device which provided additional security. The crossover consisted of a base plate fastened to he right hand side of the Typex containing a plugboard with 26 leads lettered A to Z which could be plugged into a lettered hole in accordance with a settings key which was changed at set intervals.

The need to reorganise the signals staffs of the military forces in keeping with a peacetime establishment now became necessary. In 1942 the cipher staff in Army Headquarters Wellington, consisted of two officers and eleven female civilians who were enlisted in the WAAC the following year. In September 1944 the staff numbered twenty but by November 1946 it had been reduced to three.

The post war years saw the replacement of many cypher systems that had been used continuously throughout the war and either the systems themselves had become less secure or the machines had become worn out and parts were hard to replace. In 1948 the Admiralty decided that the Stencil Subtractor System could not remain secure if it were to be exposed to a r d rise in traffic in an emergency a until a replacement system could be found double subtraction appeared to be the only acceptable solution. Luckily, the Stencil Frame system was purely a stand-by system and its use was fairly limited. A more fortunate change as the decision to withdraw the CCM machine which in the early fifties was the N.A.T.O. off-line machine cipher system. The replacement was an American-built machine, the KL-7, which was released to NATO and Australia and New Zealand.

The K-7 was a small lightweight (20lb) electromechanical keyboard operated cipher machine which enciphered and deciphered at a rate of approximately 60 words per minute. The encrypted message was printed out on gummed paper tape in five letter groups and the decrypted message was printed out in clear text. This gummed tape was then affixed to a message form for transmission or delivery to the recipient as appropriate. The cryptographic principle used with the KL-7 was the ADONI system which was brought into force with Commonwealth navies on 1 July 1956. In typical Navy fashion the signal from Admiralty quoted biblical verse "**TYPEX 2 Timothy Chapter 4 verses 6-7. ADONIS John Chapter 14 Verse 15.** Translated the verses are appropriate to the demise of Typex and the introduction of KL-7. Hus 2 Timothy. "For I am already being offered and the time of my departure is come. I've fought the good fight, I have finished the course. I have kept the faith" John 14 reads "If you love me you will keep my commandment."

On the same date a number of other changes were made by Admiralty. The Stencil Subtractor System was abolished as was the Admiralty and Naval Stations One Time Pads. A Commonwealth Naval Edition of the Britax system (the British version of Natex) was introduced for use between the RN and Commonwealth navies and a single basic book, the Inter-Departmental Basic Book, was adopted for all purposes.

Although the us of one-time pad systems was discontinued in the New Zealand Navy, they were maintained by the Air Force and by the Department of External Affairs. Also, a number of Typex Mk 23 machines were transferred from the RNZN to the RNZAF and the Department of External Affairs. RNZAF holdings of codes and crypto systems in 1958 included Typex Mk 23. One-time-pad, Stencil Subtractor, Britex and Natex systems, the Colonial Defence Code as well as the KL-7. At the end of the fifties the N.Z. Army had no cipher system in use in the field. An equipment called 5UCO was installed in Army Headquarters and provided on-line encryption on the teleprinter channel between Wellington and Canberra. The RNZN also had three 5 UCO machines installed in Navy Office Wellington for operation with HMAS Harman in Australia but this circuit did not come into effect until later in 1960.

Chapter 4

The Growth of Communications Security in Government

The first move towards the formation of a national body charged with responsibility for communications security in N.Z. came during the war years when in August 1943 he Secretary of State for Dominion Affairs in London wrote to the Minister of External Affairs in Wellington. In his letter the Secretary advised the Minister of the existence and responsibilities of the U.K. Cypher Security Committee. The N.Z. response was that as all ciphers used by N.Z. were received from British sources and as the accompanying security instructions were strictly observed it was considered unnecessary to set up a local N.Z. cypher security committee. In May 1946 the British Government tried again to awaken the Government of N.Z. to an awareness of communications security.

In may 1946 the British Government tried again to awaken the Government of N.Z. to an awareness of communications security. This may have prompted a meeting that was held in the Prime Minister's Department on the 31 July 1946 where it was the general consensus that a Cypher Security Committee should be established with functions comparable with those of the UK Committee plus the responsibility to co-ordinate security and other arrangements for the use of cyphers in N.Z. and the Pacific Islands. These recommendations were forwarded to the Prime Minister in September 1946. However, in September, 1949, replying to a query from the Joint Intelligence Committee noted that no actual approval from the Prime Minister to the recommendation had three years earlier could be found but that the Cypher Security Committee was established and operating although it had never met!

Following this discovery a more positive approach was taken and the first meeting of the N.Z. Cypher Security Committee was held on 3 May 1950. In December 1950 Air staff agreed to provide the secretariat for the Committee. In July 1966 the committee was retitled the New Zealand Communications Security Committee and the Defence Secretariat transferred from the Prime Minister's Department to the Defence Office on the Formation of the Ministry of Defence. The Committee did not meet again until September 1974 when as a result of concern expressed by both the UK and Australian cipher committees a meeting was arranged. In 1977 a nqtional communications security authority, the Government Communications Security Bureau (GCSB) whose director Mr C M Hanson became Chairman of the newly formed Government Communications Security Committee which replaced the NZCSC..

The Beginnings of Cryptography

It is believed that the oldest text known 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 Khufi 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 inscription.

In an essay written in 1466, an Italian Leon Alberti, who is often called the "father of western cryptography" described the construction of a cipher disk but did not develop the concept. A French cryptographer, Vigenere devised 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. 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 around 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.

Perhaps the true frailty of book ciphers was highlighted by the ease with which the Royal Navy's fledgling code-breakers in the celebrated Room 40 were able to decrypt the celebrated Zimmermann telegram from its German Foreign Office Code. Less than three months after the full text had been delivered to U.S. President WILSON, the then neutral. United States declared war on Germany.

Vigenere Technique

Towards the end of World War 1 the U.S. introduced the concept of a code based on truly random keys which took the form of two identical pads printed with lists of randomly generated letters. Using the VIgenere technique each page is used to encrypt and decrypt ONE message and then destroyed. The weakness of the VIgenere had been the repetition of the key but this new techjnique injected the same randomness into the cyphertext as was contained in the key and there was therefore no usable patterns or structure within the message. This meant that attacks seeking to exploit these weaknesses such as the Babbage test would fail because 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 to the 27^{th} power keys and even then multiple decrypts could all appear plausible. The basis of this method is still in use today, called the One Time Letter Pad, or OTLP and it is still the only "admitted" system to provide the "holy grail" of cryptography – perfect security.

If the first world war showed the importance of cryptography on the battlefield and spawned the development of the "unbreakable one time letter pad" the second World War placed cryptography squarely at the centre of military and political strategy.

One of the fundamental weaknesses of all these earlier versions of cryptography was that their application was time consuming. This did not matter unduly when the encrypted message was being delivered by foot, by horseback or by sailing ship but became critical when the information was received in time to affect the conduct or even outcome of a battle. The increased speed of encryption and indeed of decryption coupled with electronic methods of transmission and reception were significant features in the Japanese loss of Admiral Yamamoto and the earlier British interception and decryption of all the "winds" Japanese radio traffic which identified the time of the Pearl Harbour attack.

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

An Enigma.

The Enigma machine was designed by a German and patented in 1919. The machine was adopted by the German Navy in 1926 and later by the other services as well as other

sections of the government. It has been reliably stated that the widespread adoption of Enigma was almost entirely due to Winston Churchill's revelations in his book "World Crisis" published in 1926. This cryptographic door opened by Churchill was taken off its hinges in the same year by the official war history of the Royal Navy describing in some detail the exploits of Room 40.

Unfortunately, the Royal Navy's decryptions of German cipher traffic had ceased by early 1930 because of the introduction of the Enigma. Although much has been written about British efforts against Enigma they were not the first. The first crack in the Enigma armour came from HUMINT, not SIGINT. This ultimately led to the brilliant work of the Polish cryptographers who in July, 1939, handed a working Enigma machine and a full set of working blueprints to each of the British and French cryptographers. There is now no doubt that without this exceptional work done by the Poles before the start of World War 2 the immensity and complexity of the British wartime decryption task may have defeated them.

What the Poles did prove was that, despite the apparent strength of Enigma it did have weak points and these, along with others discovered by the British were used to great effect. In terms of its internal architecture Enigma is simply 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. One other weakness exploited by Bletchley Park was the discovery that keying X would not give X, a fact that was applied to great effect when applying "cribs", 'ordered or known text that provide clues to breaking a cipher' such as Dear Sir, or Heil Hitler.

While OTLP offered 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 interceptor's hands. During the war years, for a variety of reasons, these things happened. What has become apparent is that the most successful attacks on any cryptographic systems came initially from HUMINT but this method of attack was supplanted by ELINT and SIGINT as electronic techniques became more prevalent and more successful. Evidence has now revealed that at the beginning of WW2 only two British encryption systems were unable to be broken by determined attack. One of these, the Basic Book, a list of the most commonly used words and phrases expressed as four-figure groups was known to be in the possession of the Germans. The four-figure groups were the basis of two of the Royal Navy's most widely used systems, the Stencil Subtractor Frames and the One-Time-Pads. The integrity of the Stencil Subtractor Frame. System was later bolstered by being doubled-up but the integrity of the One Time Pads remained unchallenged, even though individual versions or pads were known to have been compromised or broken, a fact that was used to advantage in the successful Man That Never Was operation.

Time Consuming

The Basic Book system had one elementary fault in that the encrypting or decrypting process was laborious and therefore time-consuming making it totally unsuitable for tactical or quickly changing operations This fault was not peculiar to the British Navies. The German U-boats had One-Time-Pad systems involving four-figure basic books and necessary recyphering tables but because of the time required to process the text into encyphered groups these were only used when their Enigma system was damaged or defective.

The most common and most compromised Royal Naval tactical operations cipher was known as the Playfair Code, offering a simple substitution table where three-letter groups were substituted for common words or descriptors. While Playfair Code was quick, its security classification was at best Restricted and at worst non existent. Having said that, Playfair Code's one advantage appears to have been its brevity rather than it's security.

Another relative substitution code was used for callsign encryption but because of advances in transmitter identification was inevitably compromised as soon as it was introduced,

Machine Systems

Typex/CCM

As long ago as 1936, Lord Louis Mountbatten, then Fleet Wireless Officer with the Mediterranean Fleet, had recommended that the Royal Navy adopt a machine cryptograph for enciphering all its radio traffic as the German Navy had been doing since 1926 with the Enigma. The two Enigmas that the British had bought in 1928 had lain idle while a committee had spent two years debating how best to use machine cryptography. But at the end of six years they had been unable to come to any decision.

By 1934 the R.A.F. borrowed one of the machines and, using parts from commercial teletypes then in service with the RAF, produced a cumbersome machine they called the RAF Enigma, which weighed over 55 kilos and, unlike the Enigma's battery system, needed a 230 volt supply. Fortunately, the committee declined the proposal. Undeterred, the RAF handed their prototype to the fledgling Creed company who produced 29 machines which they called Type-X Mk1. Creed then made a number of improvements and by May 1937 produced Typex MkII. This was shown to the Cypher Committee on 14 June and they immediately approved an order for 350 Mk II machines at a cost of $53.90 each. A later attachment enabled Typex MkII to produce punched tape using the standard five-unit Baudot code but the MkII could not work on-line with other Typex machines.

Typex Mk II used five active rotors plus one static rotor and was plainly a copy of Enigma and infringed their patents, a dispute that was still going on when the war began. If properly used, the Enigma was unbreakable and indeed several keys were never penetrated by Bletchley Park throughout World War 2.

Stories have grown up that the Royal Navy rejected Typex but these are incorrect and the sole reason the Admiralty didn't put Typex aboard ships was due to slow production, a fact that is confirmed by official records that show that Admiralty had ordered 630 Typex machines by October 1939 with a further 500 ordered by July 1941. While the British showed Typex to the Americans, the Americans never permitted the British to see their MkII E.C.M. which was of a more advanced design. Instead, attachments were built for both that allowed them to read messages enciphered on the other's machine. Typex was used by all British armed forces and was also used throughout the Commonwealth and, with the CCM adaptor, figured prominently during the Korean War, remaining in service until the late 1960s

TSEC/KL7

The KL7 was an off-line cipher machine, developed in the late 1940s and went into production in 1952. Code named Adonis it was similar to but more advanced than the German Enigma. KL-7 was used for the protection of off-line traffic. The unit had the approximate dimensions of a medium sized portable typewriter and was housed in a moulded fibreglass carrying case which was painted in an olive drab khaki colour. On the front of the KL7 there was a character counter to help keep track of the number of characters in a message and a small lamp to illuminate the keyboard. The KL-7 had eight rotors but the rotor in position #4 was stationary. As a result there are seven windows on the rotor basket, one to view each rotor that moves. Perhaps it was another example of HUMINT that hastened the demise of the KL-7 when the Walker family spy ring was exposed in the mid-1980s and it was found that they had supplied the Soviet Union with a complete working KL-7 together with all keying materials. Immediately all U.S.and Canadian based machines were withdrawn from service and returned to the COMSEC depot at Fort Mead, Maryland U.S.A.

The Beginning of the Future

The dawning of the twentieth century have cemented the emergence of the digital age. The microprocessor and the personal computer and their acceptance into everyday world has meant that although our primary means of communication is the spoken word the 'lingua franca' of our working lives and increasingly our private lives, is digital. The digital dialect has spawned vast communications networks – Internet, Digital GSM, Mobile Phones, Automatic Teller Machines offering instant 'secure' communications. 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 and, in fact, the electronic world, rests on secure digital communications. Unfortunately, so does the success of drug rings, people smugglers, child pornography, organised crime, spy rings and 'cyber crime'. This is one war that is not likely to be won or lost any time in the near future

.