中央訓練團黨政訓練班講演錄

徐鴻濤先生講

密碼學概論

民國三十三年四月印

密碼學概論 綱目

（一）密碼重要性

1. 第一次世界大戰時之「甲慈堡」戰役與「齊茲門」事件
2. 此次戰爭各國密碼門爭概況及我國現時密碼洩漏之一般情形

（二）密碼內容概釋

1. 以數字或字母代表單字或成語而用作祕密通信之符號者謂之密碼
2. 密碼計可分爲二大系統

甲、密語系包括「密本」「密語表」

乙、密碼系包括「移位」「代碼」及「加減碼」各種密表及機器密碼皆屬之

3. 密碼之優劣條件在無「常性」及「循環」

（三）現代各國密碼趨勢

1. 由簡單「移位」進而繁複「移位」由「字母代字母」進而「數字代字母」
2. 由用本進而第二重變化及機器碼或第三重變化

（四）我國密碼現況：

1. 我們密碼脫胎於明碼本明碼本之缺點

密碼學概論

(一)密碼重要性

1.第一次世界大戰時之「坦能堡」戰役與「齊茂門」事件

密碼通訊係欲互相聯絡消息，使他人不得而知其祕密；倘使密碼編製不得其法或運用不能適宜，則通訊內容和盤托出，爲人盡知，洵屬萬分危險。且密碼通訊在軍事上爲發佈命令及傳達軍情之命脈，在外交上爲爭取壇坫及折衝樽俎之指揮，萬一洩漏，則影響於軍事外交之勝負得失者，至爲重大。其他如國防之計劃、飛彈之運輸、政治之活動、黨務之組織與宣傳甚而至於商業之競爭，幾無一不與密碼通訊息息相關。如有洩漏，亦均受他人之威脅，則密碼通訊方法之如何，實與國家民族之安危，有密切之關係也。

上次歐洲大戰時期，帝俄早已由專家籌備最機密、最新方式之密碼貯存於祕密保險櫃中，迨對德宣戰之日，由陸軍最高統帥基林斯基將新密碼取出啓用，同時下令燒燬舊密本。俄軍當時先以兩個軍團向東普魯士突進，第一軍團由蘭南哥夫將軍統率，預定向東方推進，第二軍團由山疎諾夫將軍統率，向南方推進。但兩軍出發前進時爲四十里寬廣之馬蘇利安湖區所分隔。該地帶係一片荒野，既無鐵道，又無公路，兩軍聯絡消息，全賴無綫電通訊。此兩軍團均爲沙皇之精銳部隊，裝備與訓練俱屬優良，基林斯基早已

將密碼交與兩軍使用，但第二軍團山疎諾夫忽視密碼之重要性，不僅不遵奉命令將舊密本燒燬，且貪圖便利如常使用舊密本，不斷與兩軍通電，甚至有時雙方均使用明碼譯發之。一九一四年八月二十日之夜兩軍致山軍一電說明前鋒必須停止前進三天，以待後續輜重部隊。是時德將興登堡及魯登道夫接任統軍主帥任務，其時德軍兵力雖超越於蘭氏之一軍，但其戰鬥方面於蘭山兩軍兵力之總和。魯登道夫不斷截收俄軍之密碼，同時一一譯出之，初不幸俄軍竟公開洩露其軍事行動之機密，如宿營地點、警戒部署及糧彈配備等各項報告，經派騎兵聯隊偵察蘭軍行動，證明確實。一面調派德軍精銳各師循鐵道運抵波蘭，於八月二十六日以優勢兵力包圍其兩翼，並全力向正面撲擊，鏖戰三日，山氏軍隊被殲者近十萬人，三週後蘭軍亦被擊潰，此為軍事上著名之「坦能堡戰役」。是帝俄軍事之失敗，由於密碼之洩漏，可為前車之鑒。

當同盟國與協約國兩軍正在酣戰之時，在英方面運用種種外交手腕欲使美國參戰；在德方面則又用種種手段以牽制之。而美國總統尚在猶豫，仍欲始終保持中立，迨一九一七年德國派駐南美洲祕密活動之外交代表齊茂門氏曾發一重要密電致德外長伊卡脫，報告與墨西哥談判之條件，並締結德墨同盟及煽亂美洲牽制美國參加歐戰之計劃，密電中並涉及與日本合作，將來以美國西南部的領土讓與日本。該項密碼電文被英國海軍情報部之「四十號室」將其全文譯出，立即將原文送交美總統威爾遜氏，此一份密碼可以

證是直接促成美國加速參戰。自此密電披露之後，一時美國輿論大譁，美總統立即決定對德作戰，命潘興將軍統率大軍開赴西歐與協約國速參戰，此爲外交史上著名之「齊茂門」事件。是英國外交之勝利，由於密碼之成功，德國外交之失敗，由於密碼之洩漏，於此足資佐證。

2. 此次大戰各國密碼鬥爭概況及我國現時密碼洩漏之一般情形

（口述從略）

（二）密碼內容概釋

1. 密碼之定義

無論阿拉伯數字或外國文字之字母，用以代表一個單字或一句成語，避免他人所知而將秘密通訊之符號者，此種數字及字母，均謂之密碼；其能公開而任人知者，謂之明碼。

2. 密碼之系統

密碼計可分爲二大系統：（甲）密語系 Code System 包括「密本」「密語表」，（乙）密碼系 Cipher system 包括「易位碼」，「代碼」及「加減碼」各種密表及機器碼均屬之。

「密本」我國譯電碼以密本爲主，有簡單編法，亦有繁複編法。其簡單者順部首之

次序直而編之，其繁複者則分節橫編及編來去本並增加常用單字編入各種成語。然編法無論如何繁複，在一本密本之內，因受頁數之限制，可能增加之常用單字爲數有限，編入各種成語亦無法可以滿合乎應用之要求。譯電之時，不免發現常性，一有常性發現，即易爲人揣測，是以單純使用密本譯電，殊難保持機密。

「密語表」此種方式係以一種表編入若干應用術語，以爲應付最短期間之用，其編法與密本徵有不同。密本之編法多屬使用於普通的，密語表之編法僅係適應小部份之需要，惟編碼之時，必須使其隨時變化活動，方足保持機密。現時我國使用此項密語表者尙少。

「易位碼」(Transposition cipher)易位法計可分爲兩種：(1)電文易位，即將電文顚倒錯亂其位置，使人難以得知電文中文字之意義；(2)電碼易位，即將電文之組碼各個分別拆散，而顚倒錯亂其位置，使人難以得知原來組碼之眞相爲如何。然易位必須使用軍電紙格式及運用「密鑰」key 與「指標」Indicator 以指示使用何種表示及如何譯法，否則無法譯電。惟密鑰指標必須設法隱藏善爲掩護方可。

「代碼」(Substitution cipher)以甲碼代替乙碼，謂之代碼。例如以P代A或以9代5之類，有單式代碼及複式代碼之編法，我國以前使用明碼本編爲密本，即係使用代碼法之最簡單者，是以萬分危險，一攻即破。故必須絕對禁止使用之，如單純使用代碼，

則必須組成表式甚多，且要善於運用及謹愼隱藏指標，否則危險性甚大。

還「加減碼」（加碼與減碼之理相同故以下祇言加碼），所謂加碼者，係在一組原來碼之下加上另一組碼，使其成爲一種新的密碼之意。例如（以四碼言之）有一組原來碼4567加上另一組碼2691兩數相加其和爲8258（加碼逢十不進位），此8258即係變成另一種新的密碼，與原來碼4567完全不同。故加碼即可以減少電文中之常性，增強密碼之機密性能不少。

各種密碼及機器密碼　所謂各種密碼者，即運用密碼之各種表式，如易位碼表，加碼表，代碼表之類。機器密碼指用機器發出之密碼而言。

3.密碼之機密條件在減「常性」（freauency）及「循環」（Periodic）

所謂常性者，即有一個組碼如1234此1234之組碼在電文中常常發現之謂也。因常性發現而生出文字狀態，由文字狀態而得其文字之意義；所謂由點而延伸至線，由線推而至於全面，即可窺其全豹。故必須將其常性減量減少或竟完全消滅之，方可保持機密。所謂循環者，即週而復始所生出之循環性也，例如使用加碼法，每加若干組碼，則加至若干個字之後，即有一次循環。假使加十組碼週而復始，則第十一個字即開始發現循環，加一百組碼則第一百零一個字即開始發現循環。使用代碼法亦然，假使將一個字用一張代碼表代之，而使用十張或一百張代碼表，週而復始，則第十一個字或第一百零一個

字即開始發現循環，並無差異。一有循環，即易爲人所算。故必須將其循環盡量減少或竟澈底打破之，否則不足以言機密。要而言之，加碼愈多，即密碼之機密性能保持愈大也。

（三）現代各國密碼趨勢

（1.）由簡「易位」進而繁複「易位」由「字母代字母」進而「數字代字母」

上次歐洲大戰以後，美國著名研究各國密碼之黑室（創立於一九一三年在一九二九年即已停止工作），將其已往成績公開宣佈，謂在此十六年之內，曾譯出英、德、俄、法、中國（請注意中國二字）、日本、巴西、智利、阿根廷、祕魯、墨西哥等各國之密電，不下四萬五千份之多。於是舉世震驚，幾無不知密碼洩漏之原因及其利害之關係，而競相研究或致力於偵研他人之密碼，以期有所得，或竭心於保持自己密碼之機密，以免有所失。攻守兼施，各極機巧，而研究密碼之術亦即風起雲湧，對於改革自己之密碼尤爲注意，由簡單易位進而繁複易位，由字母代字母，進而數字代字母。所謂簡單易位者，例如有一個組碼爲1234，此1234之組碼其1字係在四碼中之第一位，2在第二位，3在第三位，4在第四位，今將其位置移動使2字移爲第一位，4字移爲第二位，1字移爲第三位，3字移爲第四位，則1234之組碼業已移動其位置（亦即更易其位置），而變成2413新的組碼矣。此種易位方式係屬於最簡單者，設使有數十個或百數以上之組碼，

將其全盤位置完全拆散，隨便錯亂而移動之，使其變成組組不同之新碼，如此則謂之繁複易位。所謂字母代字母者，例如以P代A、以M代B之類；所謂數字代字母者，例如以1234代A、以1286代AND之類，然此尤屬不足保持機密。於是

2由用本進而第二重變化及機器碼或第三重變化

所謂用本者，即使用密本之謂也，第二重變化即使用密本譯電之外再加一重變化，如再加碼或再代碼或再易位而成二重密碼，使其有所保障也。現時我國規定使用密本譯電之外，必須加碼，即同此理。第三重變化則使用密本譯電之外再加碼，加碼之後再復易位，或使用密本譯電之外再易位，易位之後再復加碼，務使密碼有多重之變化，以求機密之堅強。所謂機器碼者即使用一種機器發出隨時變化之密碼，此種機器結構精巧，其內配以數字排成方式，一按其關鍵，即可使各個數字千變萬化也。

（四）我國密碼現況

1.我國密碼脫胎於明碼本明碼本之缺點甚多

2.黨政軍高級機關雖纂密本頗多進步惟距全體使用二重密碼之途尚遠

3.各部份自纂密本而未送審者甚多其洩漏可能性最大

4.根據電台無線電底審查研究不合標準者達百分之四十以上

綜上以觀，可知我國人尚多未明瞭密碼機密之重要及密碼洩漏之危機，故使用密碼

尚未達到合乎標準，足以保持機密之程度。蘇黨政軍高級機關編製密本已多進步，催電純使用密本譯電，殊難保持機密，是以多年以前，本會即已大聲疾呼拍發密電必須加碼，且復明定規章，俾資遵守。奈時經數載，各機關部隊之譯電人員其能切實奉行遵章加碼者，人數寥寥；其弁髦法令經不加碼者，尚居多數。除單純使用密本譯電絕不加碼外，更將括弧符號暴露，甚至將番號如[illegible]等字樣不以密碼譯出而明明白白譯之於電文之上，貪圖個人之便利，而不知機密洩漏之危險，且又不願將編之密本送會審查，因而上級機關無法予以指示改進，遂使機密洩漏於無形之中而不自知，言之不寒而慄，須知我國密碼原由明碼本脫胎而來，其結編法本甚簡單，儘將明碼本編配角碼及橫直小碼，遂即作爲密碼通訊之用，無惑乎美國黑室祭其一攻即破，而完全譯出我之密碼電文也。而明碼本之編制又僅根據康熙字典之二百一十四個部首，擇其普遍所用之字約七千七百餘個而編成之，故其缺點甚多。列舉如次：

明碼本之缺點：

A公開的印版本本同樣。

B每一個字限於一個組碼如「工」字祇有0081一個組碼之類。

C字與部首之位置均固定毫無變化。

D角碼之編法採順其數字之次序。

E 小碼之位置頁頁相同。

F 可能常用之字不過三千，其最常用者且不及三千。

G 常用之字集中於第一頁即（〇二頁）者時多。

H 常用之字聚於一行之內者不少。

I 字與部首之排列係按筆畫多寡約有一定次序。

J 第一頁之字有特殊狀態。

雖我國編纂密本之方法，由簡單而漸複日有進步，然而單純使用編本譯電尚有危險，必須使用二重密碼方足保持機密，若僅以明碼本編配角碼及橫直小碼即作爲密碼通訊之用，欲不洩漏機密，寧可得乎，此所以本會三令五申絕對禁止使用明碼本編爲密本者也。

（五）如何鞏固我國密碼陣容

1 編纂及使用密本表示以「機密」「迅速」「確實」三原則爲標準

編纂及使用密碼之原則，第一最重要者厥爲機密。故舉凡密本體裁之如何釐訂、頁數多寡之如何決定、單字組何增加及如何佈置、成語如何選擇及如何配用、角碼小碼之如何編配，與夫各種密表如易位碼表、代碼表、加碼表等之如何編法，其使用法是否靈敏活動、且有變化，有無常性，發現情況如何及其循環性如何，在在均與機密性有密切

之關係。如繕纂得其法則可具機密之效能，反之則密碼有易於洩漏之弊。其次則爲迅速，夫軍情瞬息萬變，使用電報通訊其目的不外爲達到迅速之要求，倘使密本內容之結構過於凌亂複雜，各種碼表之編法運用迫於須臾，則譯電之時勢必多費時間，影響於迅速。故應在不失機密原則下，力求迅速之效能。再次則爲確實，假使繕纂密本之時在同一行內而有兩個或兩個以上之數目字，則應使其各個分散，不免錯碼之時無法決定，且亦難於追索，例如與碼本第一頁第一行內有「一」「七」「三」幾個數目字，如有錯碼則此個組碼究竟是一是七抑或是三殊難決定，諸如此類，所謂差之毫釐謬以千里，不可不愼。故應在最高機密範圍內力求迅速，尋求確實，方免貽誤。

2密本表之保管與寄遞須特別嚴密謹愼

密碼運用適宜，實爲保持機密之重要條件，而密本密表之需要嚴密保管，亦屬切要之圖。假設甲方面已將密本密表同時遺失落於敵人之手，而乙方面一時尚未知之，仍復用此密本密表通報，則所發電文直與敵人通報無異，其危險又如何耶？即使遺失之後立刻通電作廢，而敵人亦可以利用此密本密表將已往偵收所得我方之電報逐一譯出，則我之軍事命令、軍事計劃、軍隊行動、部署位置以及如何配備等項洩漏無遺，影響於軍情者至爲重大。是以各國有將密本密表鎖於保險箱者，其箱內配以電火機，指派專人負責看管，遇有危急，一鈕其機即發出電火將密本密表完全燬燼，務使片紙隻字不落於敵人

之手。保管人員對密本密表爲第二之生命，坐臥不離，盡其職責，此種精神足資取法。惟我國物資缺乏，據此設備，故祇有指派專人負責將密本密表分開保管，以免同時遺失，遇有危急立即以火焚之。至於需備本之所以必須主管長官親自保管者，良以主管長官所處之地比較安全，而電情瞬息萬變，設使不幸各級密本完全遺失，無法可以通訊時，亦已有所準備，隨時啓用此種密本，以免軍訊停滯，影響軍心。其餘應如何保管之法在「拍發軍電須知」內言之甚詳，毋庸多贅。關於寄遞在發出者必須使用堅韌之封套，其內加入印製之清單列以類別、件數、號數、名稱等項，俾資查考，嚴密封固然後寄遞；在收件者必須詳細驗明封套，有無毀壞，內封各件是否與清單所列者一一相符，如有所疑應立即查究，視損壞情形或將本表作廢，或將密本更改名稱，改編其角碼及橫直小碼，並改換密表，以期嚴密而免洩漏。

8 電稿避免公文常套透露公佈或轉電須顧及是否影響密本

中級機關接奉上級機關命令而轉達於下級機關，或下級機關有所陳請或報告，則中級機關據此轉報，或請示於上級機關者，此種電報時所常有，若擬稿者不加注意而視爲例行文件，遂將電文全部照述，則其弊病甚大。因各級機關所用之密本密表，其機密性能之強弱各有不同，萬一有一機關其所用之密本密表編法較爲簡單已爲偵研密碼者所攻破，則與相通訊之機關其密本密表縱使編法堅強，亦必易於疏漏，或竟受其牽累。故宜

將原文之字數酌予增減，使其數目相差較大，以免爲人所算。其他如通報、報告、情報等之電稿，均應隨時變動字句，切不可有固定之格式，撰擬電文亦須字句靈動，極力避免公文常套，庶免影響於密本也。

4.不可任用毫無訓練之人員充任譯電員因而洩漏國家機密

現在世界科學昌明，他人研究密碼究竟逈步至如何程度，殊難揣摹，而偵譯我國密碼者，環伺於傍，目光灼灼，絲微不入，使用密碼，稍一不慎，洩漏無遺。若仍以爲隨便派一參謀或派一祕書甚至派一書記、司書或文書上士即可以譯電，誠屬萬分錯誤。因現時代之譯電絕非如從前翻譯明碼本編成之密本謹檢其角碼及橫直小碼即便了事。蓋我之譯電手續簡單，則他人之攻我密碼者必甚容易，倘我之譯電手續繁複，則他人之攻我密碼者，亦必困難，此理至爲明顯。故必須在機密、迅速、確實三原則下運用種種方式以應付，足以保持機密之要求，在在均與技術有密切之關係，是以必須曾受訓練及訓練之後尙須體察努力研究，對密碼能有深刻之認識及有相當技術之能力，方克負譯電艱鉅之責任，倘以未經訓練及毫無技術之人，而貿然負担譯電之責，不獨斷難勝任，抑亦未有不僨事者矣。

5.結論

（口述從略）