Guerre électronique et chiffrement

Par Daniel TANT

De tous temps les hommes ont éprouvé le besoin de communiquer. Le Romains pratiquaient les signaux nocturnes par le feu sur une hauteur, ce qui a donné au nom de l'implantation le suffixe « igny », d'où Murigny = le feu sur le mur, Montigny = le feu sur le mont, etc… D'autres pays ont communiqué par pigeon voyageur ou par messagers.

SERVICE DE LA TÉLÉGRAPHIE MILITAIRE. — TÉLÉGRAPHIE OPTIQUE. — Ce n'est pas un temps de demoiselles qu'il faut à messieurs les *télèphes* : ils demandent du soleil.

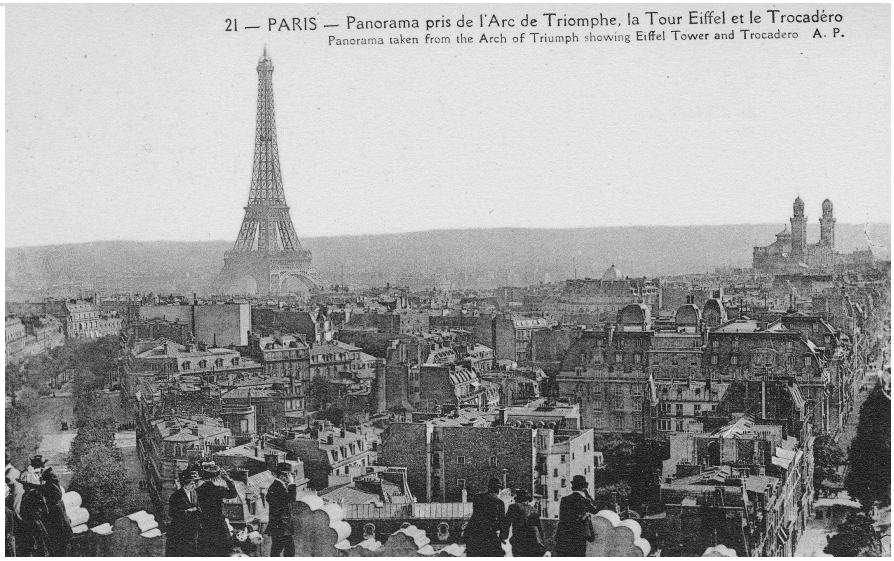
Parallèlement sont apparus les procédés de chiffrement pour rendre le message inintelligible en cas de capture par l'ennemi. Pendant la Renaissance ont fleuri toutes sortes de procédés de chiffrement. Evidemment les grands cryptologues comme Jean Trithème sont accusés de magie par ceux qui n'y comprennent rien.

Napoléon crée un service quotidien entre son camp et Paris. Il faut six jours pour que les dépêches arrivent à Berlin. Au XVIII° siècle, l'abbé Claude Chappe invente un appareil nommé télégraphe par lequel un bras articulé pouvait prendre sept positions pour transmettre les messages. Le personnel relaie les mouvements vers un nouveau destinataire sans en comprendre le sens, ce qui assure le secret. La Convention adopte le système et établit un réseau sur tout le territoire et même au-delà : Venise en Italie, Landau en Allemagne, Anvers en Belgique, Brest …

Un message émis à Strasbourg parvient à la capitale en 36 heures.

Au XIX° siècle est décidée l'assimilation des télégraphistes aux grades des armées avec un habit reconnaissable, la création d'un détachement télégraphique dans chaque corps d'armée pour le relier au grand Quartier général, une formation de télégraphistes qui deviennent des « sapeurs télégraphistes », et l'usage du morse.

ci-contre à droite : *La tour Eiffel devait être détruite conformément aux souhaits de la Ville de Paris qui voulait récupérer le terrain. Mais le général Ferrié reçoit l'autorisation de s'en servir comme support d'antenne. Dès 1908 est installée une nouvelle antenne qui permettra de communiquer pendant toute la Grande guerre.*



En 1912, l'armée française compte le 24° bataillon de sapeurs télégraphistes, le 8° régiment du génie, une compagnie radio, une compagnie de sapeurs télégraphistes de forteresse et trois compagnies de sapeurs télégraphistes pour l'Afrique du nord.

En 1914 l'armée française compte au total 12000 hommes dans les transmissions dont 150 officiers. Ils utilisent principalement des appareils morse, des lignes téléphoniques, des câbles de campagne très lourds pour établir les lignes et des postes radio d'une portée de 100 kilomètres, des appareils d'optique et des colombiers.

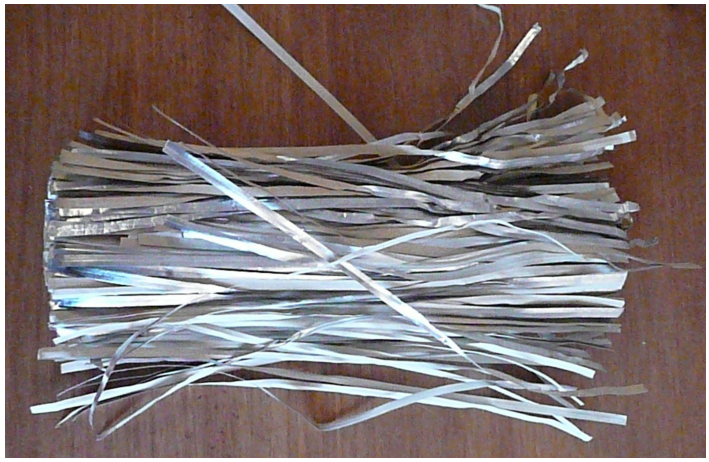
Les pigeons voyageurs ont aussi payé un lourd tribut à la Grande guerre.

Mais la guerre de position va entrainer une amélioration par le téléphone qui remplace le télégraphe. Les postes radiotélégraphistes deviennent plus légers et portatifs. C'est l'apparition des écoutes ennemies sur leurs ondes, de la radiogoniométrie pour les localiser, de l'installation d'émetteurs-récepteurs à bord des avions et des chars.

Mais le sapeur-télégraphiste ne se contente pas de communiquer en morse. C'est d'abord un soldat qui doit risquer sa vie, comme les autres militaires, pour assurer sa mission. Il doit pratiquer à la fois la guerre armée et la guerre des ondes.

A la fin de la Première guerre mondiale, il apparaît que les transmissions deviennent une arme indispensable. Les régiments spécialisés se multiplient. Mais l'heure n'est pas aux dépenses et le faible budget de l'armée est principalement consacré à la construction de forteresses qui sont bien équipées en matériel de transmissions efficace et moderne. Par contre les unités combattantes sont restées à l'état de 1918 et doivent s'en contenter au cours des combats de 1940. Quant aux échelons les plus élevés de l'état-major, leurs transmissions ont été assurées par le dévouement du personnel des P.T.T. mobilisé. Enfin en 1943 les Américains mettent leur matériel à notre disposition. Les transmissions sont encore une arme récente lorsqu'éclate la Seconde guerre mondiale. Rapidement se crée une stratégie pour éviter que la moindre imprudence ne coute la vie à nos soldats. Des consignes de sureté sont élaborées et des principes mis en application :

- Un brouillage électronique destiné à perturber le fonctionnement des matériels électroniques ennemis.
- Une déception électronique qui consiste à envoyer à l'ennemi des faux messages pour le duper.
- Une écoute permanente des liaisons ennemies.
- Maintenir tout de même nos liaisons malgré l'effort de l'ennemi pour nous brouiller.
- Détecter les essais de déception par l'ennemi.
- Il faut à la fois intercepter et perturber les liaisons ennemies.
- Attaquer leurs installations.
- Introduire un poste dans leur réseau pour les duper.
- Localiser les postes ennemis par la radiogoniométrie.

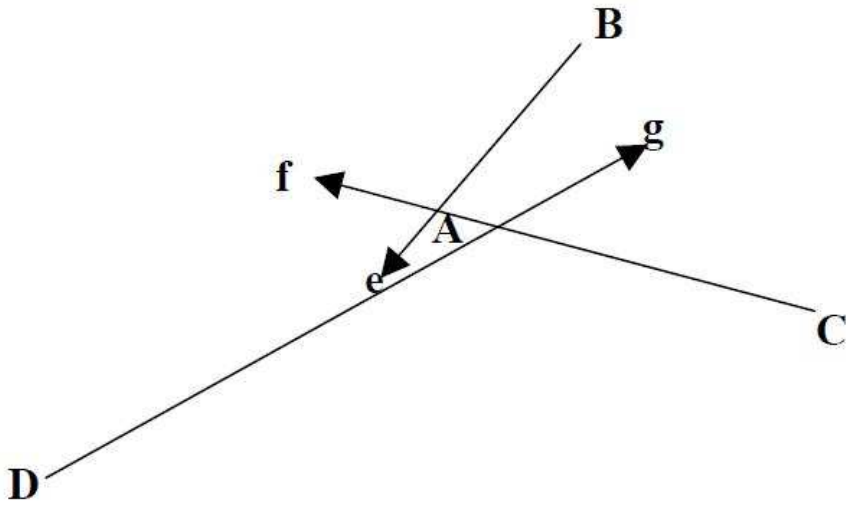


Pendant la Seconde Guerre mondiale, des bandes d'aluminium, telles que celles figurant ci-dessus, étaient jetées depuis les avions alliés. En réfléchissant les ondes radio allemandes, elles brouillaient les messages.

Mais ces mesures techniques ne suffisent pas. La guerre électronique comprend également la possibilité de coder ou de chiffrer les messages. Le degré de secret influe sur l'exécution du message.

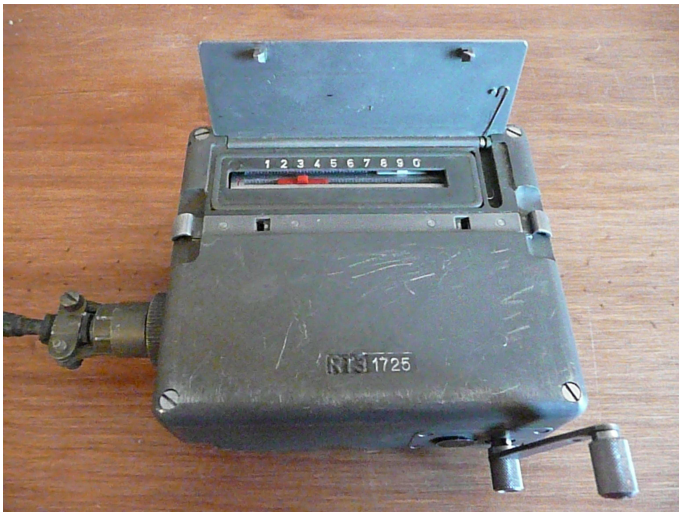
Si le message donne un ordre immédiatement exécutable, comme « monter à l'assaut » ou « ouvrir le feu », il est évident que l'encodage ou le chiffrement retarderait l'application.

Principe de la radiogoniométrie



Un émetteur radio est au point A. Un premier radiogoniomètre (B) capte les émissions en provenance de e, un second (C) les capte en provenance de f, et un troisième (D) en provenance de g. Il suffit de recouper les trois directions pour savoir où se trouve l'émetteur A.

<u>Ci-contre à droite :</u>



Le RT3 est un générateur de codes, petit appareil relié à un poste radio SP 15 et qui émette rapidement des codes de 25 caractères préenregistrés grâce à la petite manivelle située en bas sur la photo. La transmission radio étant aussi brève que possible, cet appareil permettait d'éviter la localisation par radiogoniométrie.

Il est certain qu'il était utilisé durant la guerre froide jusqu'à la chute du communisme. Employé avec l'émetteur SP20 il pouvait envoyer jusqu'à 750 lettres par minutes.

Si l’ordre est exécutable dans un quart d’heure, un encodage peut être envisagé comme « rendez-vous devant l’église de Neuville ».

Si l’ordre doit rester secret pendant deux jours, il est évident que le chiffrement ne le retardera pas.

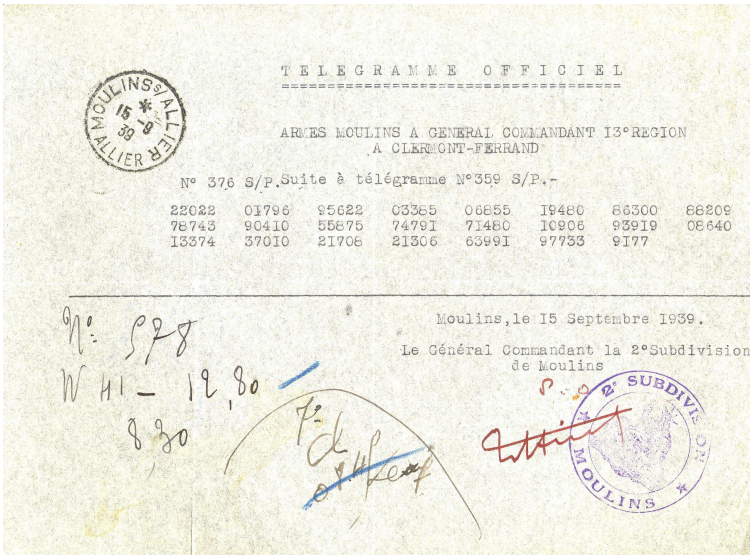
Rappelons que nous parlons des procédés utilisés à la fin de la Seconde guerre mondiale.

Par la suite sont apparus des téléphones chiffrant comme celui ci-contre à gauche.

Une fois la communication établie avec un autre téléphone de modèle similaire, pour rendre la conversation incompréhensible pour un pirate éventuel branché sur la ligne, il suffit d’appuyer sur le bouton rouge placé au premier plan.

<u>ci-contre à droite :</u>

Hagelin, le fondateur de la société Crypto AG en Suisse, a créé cet émetteur-récepteur de type CRM-008-002 qui permet des liaison vocales incompréhensibles pour un éventuel poste d’écoute ennemi. Ainsi une communication secrète permet de transmettre des ordres à exécution plus ou moins exécutables rapidement.



TELEGRAMME OFFICIEL

ARMES MOULINS A GENERAL COMMANDANT I3°REGION
A CLERMONT-FERRAND

N° 376 S/P.Suite à télégramme N°359 S/P.-

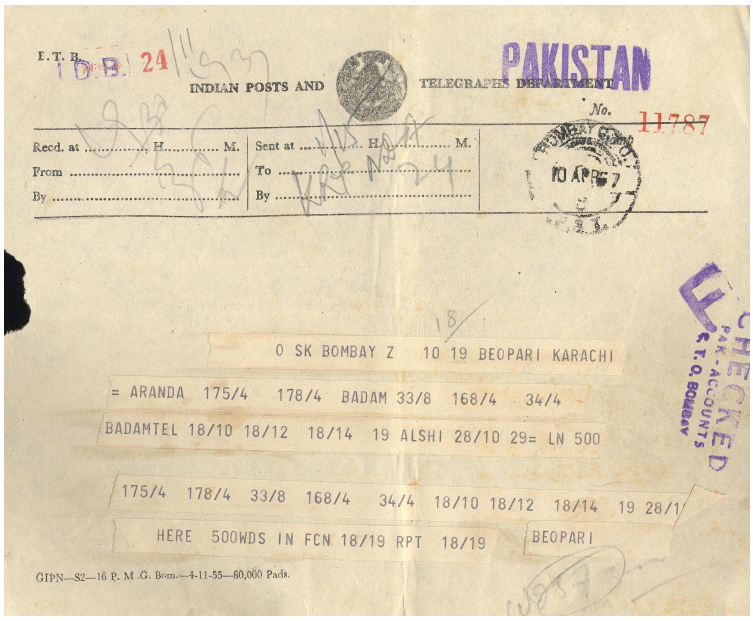
22022	01796	95622	03385	06855	19480	86300	88209
78743	90410	55875	74791	71480	10906	93919	08640
13374	37010	21706	21306	63991	97733	9177	

Moulins,le 15 Septembre 1939.

Le Général Commandant la 2°Subdivision
de Moulins

L'armée a son propre service de chiffrement et de transmissions du message chiffré.

Les administrations et les banques peuvent aussi communiquer par des messages partiellement chiffrés comme ci-contre à droite ou totalement chiffrés comme ci-dessous.



I.T.B. 24

INDIAN POSTS AND TELEGRAPHS DEPARTMENT

PAKISTAN

No. 11787

Recd. at ..... H. ..... M. Sent at ..... H. ..... M.
From ..... To .....
By ..... By .....

10 APR 57

0 SK BOMBAY Z 10 19 BEOPARI KARACHI

= ARANDA 175/4 178/4 BADAM 33/8 168/4 34/4

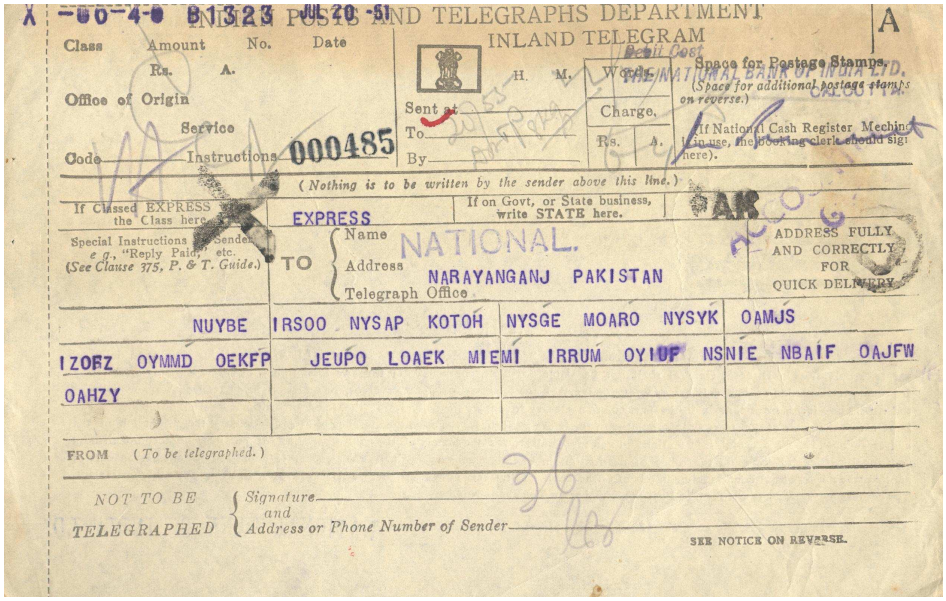
BADAMTEL 18/10 18/12 18/14 19 ALSHI 28/10 29= LN 500

175/4 178/4 33/8 168/4 34/4 18/10 18/12 18/14 19 28/1

HERE 500WDS IN FCN 18/19 RPT 18/19 BEOPARI

CHECKED PAK-ACCOUNTS C.T.O. BOMBAY

GIPN—S2—16 P. M. G. Bom.—4-11-55—80,000 Pads.



INDIAN POSTS AND TELEGRAPHS DEPARTMENT

INLAND TELEGRAM

A

Class Amount Rs. A. No. Date

Office of Origin

Service Instructions

Code

000485

Sent at H. M. Words

To

By

Recd. Cost

Charge, Rs. A.

Space for Postage Stamps.
(Space for additional postage stamps on reverse.)

If National Cash Register Machine in use, the booking clerk should sign here).

(Nothing is to be written by the sender above this line.)

If Classed EXPRESS the Class here

EXPRESS

If on Govt. or State business, write STATE here.

Special Instructions e.g., "Reply Paid," etc. (See Clause 375, P. & T. Guide.)

TO Name NATIONAL. Address NARAYANGANJ PAKISTAN Telegraph Office

ADDRESS FULLY AND CORRECTLY FOR QUICK DELIVERY

NUYBE IRSOO NYSAP KOTOH NYSGE MOARO NYSYK OAMJS

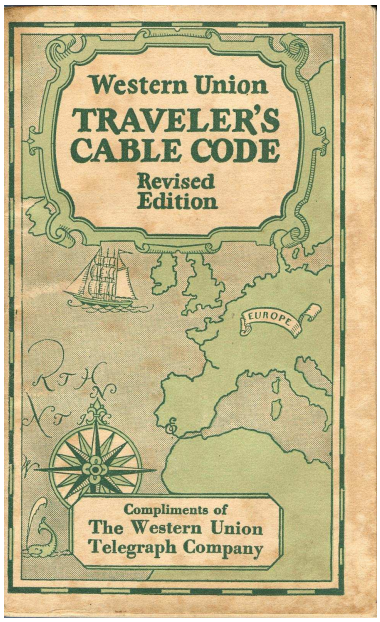
IZOFZ OYMMD OEKFP JEUPO LOAEK MIEMI IRRUM OYIUP NSNIE NBAIF OAJFW

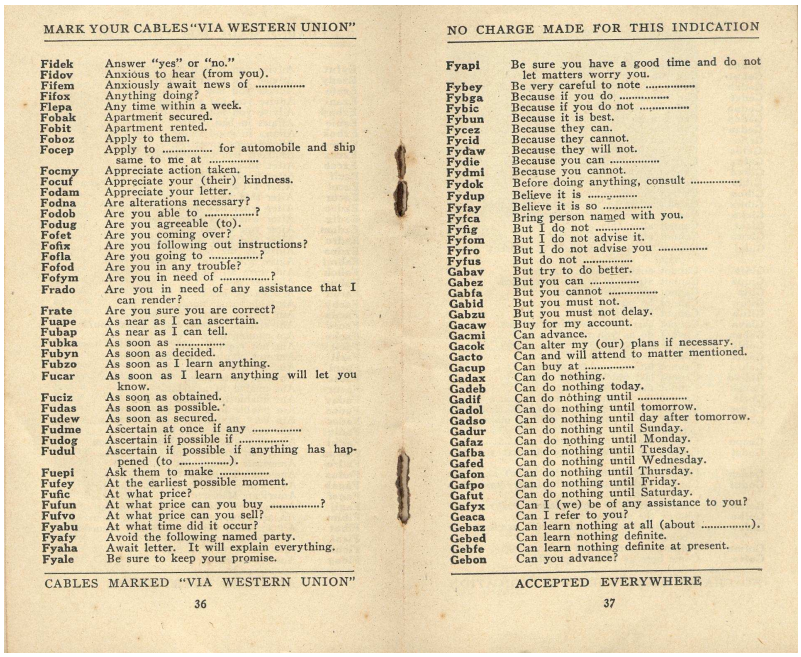
OAHZY

FROM (To be telegraphed.)

NOT TO BE TELEGRAPHED Signature and Address or Phone Number of Sender

SEE NOTICE ON REVERSE.





MARK YOUR CABLES "VIA WESTERN UNION"

Fidek	Answer "yes" or "no."
Fidov	Anxious to hear (from you).
Fifem	Anxiously await news of .....
Fifox	Anything doing?
Flepa	Any time within a week.
Fobak	Apartment secured.
Fobit	Apartment rented.
Foboz	Apply to them.
Focep	Apply to ..... for automobile and ship same to me at .....
Focmy	Appreciate action taken.
Focuf	Appreciate your (their) kindness.
Fodam	Appreciate your letter.
Fodna	Are alterations necessary?
Fodob	Are you able to .....?
Fodug	Are you agreeable (to).
Fofet	Are you coming over?
Fofix	Are you following out instructions?
Fofla	Are you going to .....?
Fofod	Are you in any trouble?
Fofym	Are you in need of .....?
Frado	Are you in need of any assistance that I can render?
Frate	Are you sure you are correct?
Fuape	As near as I can ascertain.
Fubap	As near as I can tell.
Fubka	As soon as .....
Fubyn	As soon as decided.
Fubzo	As soon as I learn anything.
Fucar	As soon as I learn anything will let you know.
Fuciz	As soon as obtained.
Fudas	As soon as possible.
Fudew	As soon as secured.
Fudme	Ascertain at once if any .....
Fudog	Ascertain if possible if .....
Fudul	Ascertain if possible if anything has happened (to .....).
Fuepi	Ask them to make .....
Fufey	At the earliest possible moment.
Fufic	At what price?
Fufun	At what price can you buy .....?
Fufvo	At what price can you sell?
Fyabu	At what time did it occur?
Fyafy	Avoid the following named party.
Fyaha	Await letter. It will explain everything.
Fyale	Be sure to keep your promise.

CABLES MARKED "VIA WESTERN UNION"

36

NO CHARGE MADE FOR THIS INDICATION

Fyapi	Be sure you have a good time and do not let matters worry you.
Fybey	Be very careful to note .....
Fybga	Because if you do .....
Fybic	Because if you do not .....
Fybun	Because it is best.
Fycez	Because they can.
Fycid	Because they cannot.
Fydaw	Because they will not.
Fydie	Because you can .....
Fydmi	Because you cannot.
Fydok	Before doing anything, consult .....
Fydup	Believe it is .....
Fyfay	Believe it is so .....
Fyfca	Bring person named with you.
Fyfig	But I do not .....
Fyfom	But I do not advise it.
Fyfro	But I do not advise you .....
Fyfus	But do not .....
Gabav	But try to do better.
Gabez	But you can .....
Gabfa	But you cannot .....
Gabid	But you must not.
Gabzu	But you must not delay.
Gacaw	Buy for my account.
Gacmi	Can advance.
Gacok	Can alter my (our) plans if necessary.
Gacto	Can and will attend to matter mentioned.
Gacup	Can buy at .....
Gadax	Can do nothing.
Gadeb	Can do nothing today.
Gadif	Can do nothing until .....
Gadol	Can do nothing until tomorrow.
Gadso	Can do nothing until day after tomorrow.
Gadur	Can do nothing until Sunday.
Gafaz	Can do nothing until Monday.
Gafba	Can do nothing until Tuesday.
Gafed	Can do nothing until Wednesday.
Gafon	Can do nothing until Thursday.
Gafpo	Can do nothing until Friday.
Gafut	Can do nothing until Saturday.
Gafyx	Can I (we) be of any assistance to you?
Geaca	Can I refer to you?
Gebaz	Can learn nothing at all (about .....).
Gebed	Can learn nothing definite.
Gebfe	Can learn nothing definite at present.
Gebon	Can you advance?

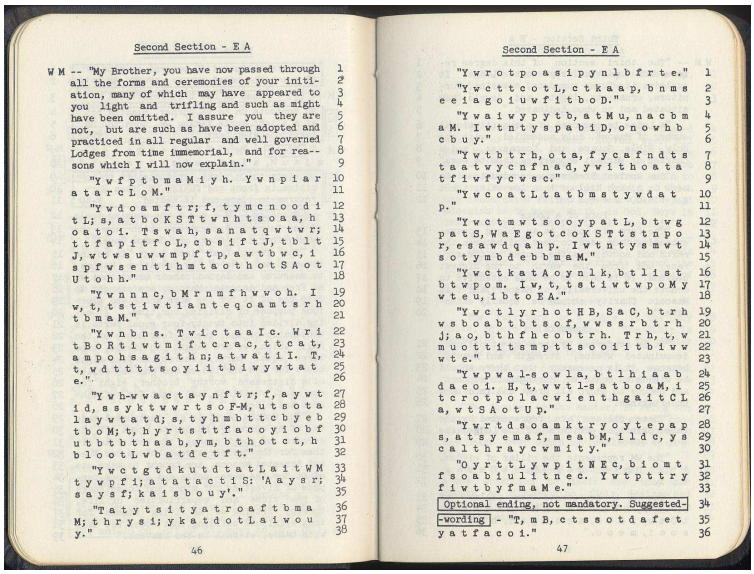
ACCEPTED EVERYWHERE

37

Pour des raisons économiques, les banques codaient également leurs messages, car au temps du télégraphe les frais de transmissions étaient fonction de la longueur du texte à expédier.

ci-contre à gauche : les particuliers peuvent aussi expédier des courriers chiffrés.

ci-contre à droite : n'oublions pas les Francs-maçons, grands créateurs et consommateurs de codes devant l'Eternel.



Second Section - E A

WM -- "My Brother, you have now passed through all the forms and ceremonies of your initiation, many of which may have appeared to you light and trifling and such as might have been omitted. I assure you they are not, but are such as have been adopted and practiced in all regular and well governed Lodges from time immemorial, and for reasons which I will now explain."

"Ywfptbmamiyh. Ywnpiaatarc LoM."

"Ywdoamftr; f, tymcnoodi tL; s, atboKSTtwnhtsoaa, h oato i. Tswah, sanatqwtwr; ttfapitfoL, cbsiftJ, tblt J, wtwsuwwmpftp, awtbwc, i spfwsentihmtaothotSAot Utohh."

"Ywnnnc, bMrnmfhwwoh. I w, t, tstiwtianteqoamtsrh tbmaM."

"Ywnbns. Twictaa Ic. Wri tBoRtiwtmiftcrac, ttcat, ampohsagithn; atwatiI. T, t, wdttttsoyiitbiwywtat e."

"Ywh-wwactaynftr; f, aywt id, ssyktwwrtsoF-M, utsota layytsd; s, tyhmbttcbyeb tboM; t, hyrtsttfacoyiobf utbtbthaab, ym, bthotct, h blootLwbatdetft."

"Ywctgtdkutdtat LaitWM tywpfi; atatactiS: 'Aaysr; saysf; kaisbouy'."

"Tatytsityatroaftbma M; thrysi; ykatdotLaiwou y."

46

Second Section - E A

"Ywrotpoasipynlbfrte."

"Ywcttcot L, ctkaap, bnms eeiagoiuwfitboD."

"Ywaiwypytb, atMu, nacbm aM. Iwtntyspabi D, onowhb cbuy."

"Ywtbtrh, ota, fycafndts taatwycnfnad, ywithoata tfiwfycwsc."

"Ywcoat Ltatbmstywdat p."

"Ywctmwtsocypat L, btwg pat S, WaEgotcoKSTtstnpo r, esawdqahp. Iwtntysmwt sotymbdebbmaM."

"Ywctkat Aoynlk, btlist btwpom. Iw, t, tstiwtwpoMy wteu, ibtoEA."

"Ywctlyrhot HB, SaC, btrh wsboabtbtsof, wwsrbtrh j; ao, bthfheobtrh. Trh, t, w muottitsmpttsooiitbiww wte."

"Ywpwal-sowla, btlhiaab daeoi. H, t, wwtl-satboaM, i tcrotpolacwienthgaitCL a, wtSAotUp."

"Ywrtdsoamktryoytepap s, atsyemaf, meabM, ildc, ys calthraycwmity."

"OyrttLywpitNEc, biomt fsoabiulitnec. Ywtpttry fiwtbyfmaMe."

Optional ending, not mandatory. Suggested-wording - "T, mB, ctssotdafet yatfaco i."

47

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information
Association régie par la loi de 1901 - N° SIRET : 511 069 569 00016
Tous droits de propriété intellectuelle réservés à l'ARCSI, association loi 1901, selon les règles du droit français