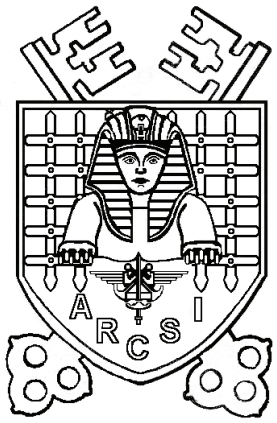

ASSOCIATION des RESERVISTES du CHIFFRE et de la SECURITE de L'INFORMATION

Nouvelle série
n° 28 - 2000

Document interne à l'Association
Réservé aux adhérents

6 . Nos Anciens

Le général de division Louis THEVENIN (1870 – 1948) et la Commission de Cryptographie Militaire

Le nom de THEVENIN apparaît dans la composition de la commission du CHIFFRE avant 1914, ainsi qu'à plusieurs reprises dans les souvenirs de GIVIERGE et d'OLIVARI mais nous manquions de renseignements sur l'homme, sur sa carrière et sur ses travaux. Cette lacune vient d'être comblée par son fils, l'Ingénieur Général du Génie Maritime Pierre THEVENIN qui a bien voulu nous remettre des photocopies de ses archives familiales.

La famille THEVENIN se retrouve en Alsace en 1732, année de la nomination de Jean-Baptiste comme "sergent royal" à Biesheim. Son petit-fils Louis, engagé aux hussards en 1807, termine sa carrière militaire en 1838 comme capitaine trésorier et meurt 3 ans plus tard. Son fils Anatole, admis à l'Ecole Polytechnique en 1844, artilleur, participe brillamment à la défense de Strasbourg en 1870, devint général de brigade et décède en 1908. Il eut plusieurs enfants dont "notre" THEVENIN (1)

Celui-ci, reçu à l'Ecole Polytechnique en 1887, à 17 ans, (même promotion qu'OLIVARI) commença sa carrière dans l'Artillerie. Il participe à l'occupation de Madagascar en 1896 - 1897, revient en France à la Fonderie de Bourges et est reçu à l'Ecole de Guerre en 1898. Il fait son stage d'état-major en Tunisie, où, il reste jusqu'en 1905 au commandement d'une batterie. Affecté alors à l'état-major de l'Armée, il suit les cours de CARTIER (on peut penser que c'est à l'instigation du général BERTHAUT, alors sous-chef d'Etat-major) et est nommé en 1906 membre de la commission du chiffre.

Tout en continuant à s'intéresser au chiffre et à y travailler, il poursuit une carrière normale : directeur de l'instruction militaire à l'Ecole Polytechnique en 1911, puis sous chef d'Etat-major au 21ème corps en 1914, au commandement de l'artillerie de la 61ème division en 1915 puis commandant de l'artillerie divisionnaire de la 53ème DI en 1917.

Il se retrouve en 1919 commandant en second de l'Ecole Polytechnique puis en 1921 commande l'artillerie du 32ème corps ; promu général de brigade, il suit les cours du CHEM en 1922. Promu général de division en 1927, il commande la 38ème DI, en Allemagne, puis, en 1930 est nommé au commandement de la 18ème région militaire (Bordeaux) jusqu'à la limite d'age en 1932, année de sa promotion à la dignité de Grand Officier de la Légion d'Honneur.

Retiré à Nice, il y décède le 1er mars 1948.

Il a paru intéressant de compléter cette brève biographie par quelques anecdotes de sa carrière.

- Ecole de Guerre (1898 - 1900).
Le général THEVENIN est très sévère à l'égard de la plupart de ses professeurs. Deux d'entre eux, qui eurent une "belle" carrière furent limogés dans les premiers en 1914. Quant au lieutenant-colonel FOCH, "c'était un fort mauvais professeur, il était peu éloquent et suppléait par des gestes à son insuffisance d'élocution".

- La bataille de Simmern.
En septembre 1927, aux grandes manœuvres de l'Armée du Rhin, le général THEVENIN commandait le parti rouge. Par une manœuvre de flanc habile, il bloqua l'attaque du parti bleu, repoussa celui-ci et fit échouer le scénario prévu.

- Le Maréchal PETAIN et le Général THEVENIN.
Pendant son séjour à l'école de guerre le jeune capitaine THEVENIN se trouvait fréquemment à proximité du capitaine (ancien) PETAIN, soit au restaurant GANGLOFF, près de l'Ecole Militaire (où il n'y avait pas de mess à l'époque) soit au Cercle militaire (Saint-Augustin). PETAIN était peu sociable, tenait des propos pessimistes, sarcastiques et souvent malveillants. Il le rencontra plus tard à plusieurs reprises pendant la guerre ou en Rhénanie, où PETAIN ne manifesta ni sympathie ni animosité particulières.
En 1927 l'ancienneté de THEVENIN le mettait sur les rangs des postulants pour le grade de général de division, or, à cette époque, aucune promotion ne se faisait sans l'aval de PETAIN. Quand on lui soumit sa candidature, il estima que "pour un cryptographe (sic !) le grade de général de brigade était une récompense bien suffisante". Il fallut l'intervention du général DOUCHY, commandant le 32ème C.A. pour faire revenir PETAIN sur cette position. Il est vrai que contrairement à CARTIER ou GIVIERGE, THEVENIN n'avait pas eu de poste proprement "chiffre". Après sa promotion, le même général DOUCHY l'envoya voir PETAIN, pour obtenir le commandement d'une division. PETAIN commença par se montrer très réticent car THEVENIN n'avait pas eu de commandement dans l'Infanterie, puis après avoir vu son excellent dossier du C.H.E.M., semble ne pas s'être opposé à sa nomination au commandement de la 38ème DI.
En 1929, PETAIN avait été chargé par le ministre de la Guerre de l'époque (P. PAINLEVE) d'une enquête sur les causes de nombreux décès dus à l'épidémie de grippe en Rhénanie, car les journaux de gauche accusaient le commandement d'incurie. THEVENIN était alors commandant d'armes à Coblence et lui fit visiter les diverses casernes de la ville. Cette inspection se passa fort bien, PETAIN n'eut pas à "engueuler" THEVENIN, l'invita à déjeuner et lui rappela des souvenirs du GANGLOFF et du Cercle Militaire.
En août 1943, à Nice THEVENIN apprit par le journal local que les membres de la Légion d'Honneur étaient convoqués pour prêter le serment à PETAIN prévu par une loi de 1941. Il écrivit aussitôt à deux de ses amis qu'il n'avait pas l'intention de se rendre à cette convocation, se "refusant catégoriquement à se plier à cette formalité" et les invitant à en faire part aux autres membres de la Légion d'Honneur : "en raison de ma qualité de Grand Officier, cette ligne de conduite peut avoir de l'influence sur la leur". Nous ignorons la suite (sans doute nulle) de ce refus.

Le chiffreur et la commission de cryptographie militaire.

C'est donc en 1905 que THEVENIN obtint des résultats positifs aux cours par correspondance du capitaine CARTIER. Il avait gardé quelques uns des exercices que nous sommes heureux de pouvoir mettre en annexe.

Il avait aussi conservé des notes établies par la commission avant 1914, et qui seront versées dans nos archives :

- note n°1 : sur le déchiffrement des systèmes cryptographiques de substitution à double-clé, comportant l'emploi d'alphabets multiples. cette note cite en référence les noms de PORTA, VIGENERE, BEAUFORT, de VIARIS, et ROZIER.
  Cette note de 57 pages, sans date, est signée par le général BERTHAUT et donc antérieure à sa limite d'âge en 1912.
- note n°2 : sur le déchiffrement des systèmes cryptographiques de substitution à alphabet unique, comportant l'emploi facultatif de plusieurs signes pour représenter une même lettre.
  Cette note de 49 pages, rédigée par THEVENIN, est signée par le général BERTHAUT, donc de 1912 ou antérieure. Les noms de POLYBE et DELASTELLE y sont cités.
- note n°3 : manque
- note n°4 : sur quelques nouveaux procédés de déchiffrement des systèmes cryptographiques de substitution à double-clé (cryptogrammes courts et très courts, autoclave, clé interrompue).
  Cette note de 39 pages, due au lieutenant BASSIERES et visée par le capitaine PAULIER, est signée par le général BERTHAUT, donc antérieure à 1912.
- note n° 5 : sur le déchiffrement des cryptogrammes en langue allemande obtenu par substitution simple ou substitution à double clé.
  Cette note à été rédigée par le chef d'escadron THEVENIN en 1913

Ces notes sont complétées par une note B d'étude sur la langue allemande, sans date, qui comprend également une cinquantaine de pages. La première partie aurait été rédigée par le commandant THEVENIN qui y a joint une note sur le déchiffrement des textes chiffrés par transposition où il montre qu'il faut tenir compte des bigrammes comme "vo" et non seulement de leur fréquence, en multipliant les probabilités et non en additionnant les fréquences.

Ces notes nous apprennent deux choses :

1) que la dénomination officielle de la commission était "Commission de Cryptographie Militaire" et non "Commission du Chiffre" comme on la trouve dénommée chez GIVIERGE et OLIVARI ;

2) que cette commission avait effectué avant 1914 beaucoup plus de travaux qu'on ne le pensait jusqu'à présent dans le domaine de la préparation aux décryptements, car les documents dont nous disposions jusqu'à présent ne les mentionnaient pas.

Revenons à la guerre et à THEVENIN. Depuis 1913 il est sous-chef d'état-major du 21ème corps. Comme le rapportent GIVIERGE et OLIVARI, il fait installer une station d'écoutes qui reçoit des messages complétant les interceptions des autres stations. Ses recherches sur la longueur de la clé de transposition des UB-CHI aident la section du chiffre à faire son premier décryptement. En octobre le système de chiffrement allemand change.

C'est THEVENIN qui le premier reconnaît qu'il s'agit d'un système de substitution à double-clé de type ABC, c'est à dire que les lettres de rang 1 + n ne sont pas modifiées, celles de rang 2 + n décalées d'un rang dans l'alphabet normal et celles de rang 3 + n décalées de 2 pas. Par exemple LEUTNANT devient LFWTOCNU. Et cette substitution est suivie par une transposition. Il trouve à plusieurs reprises la longueur de la clé de transposition. Son affectation en mars 1915 ne lui permet plus de s'occuper de chiffre, mais GIVIERGE continue à le consulter tant qu'il reste lui-même au G.Q.G.

En 1919 il revient à Paris comme indiqué plus haut, et CARTIER qui réactive la commission de cryptographie l'en fait aussitôt nommer membre (DM n° 257/CHI du 26/02/1920) et le colonel THEVENIN participe à ses travaux. Les recherches portent sur un nouveau système de surchiffrement des codes (ce surchiffrement avait été rendu obligatoire fin 1915 et avait fait l'objet de l'instruction secrète, jointe en annexe, en 1919). THEVENIN propose notamment un système simplifié pour les troupes en campagne. Nous ne connaissons les suites données à ses recherches. Il participe aussi à la recherche d'un nouveau système sans dictionnaire, destiné à remplacer le SD 12 mais sans résultat, puisque le SD 12 amélioré était encore en service en 1939.

Après son départ de l'Ecole Polytechnique en 1921, il ne semble pas que le général THEVENIN ait continué à participer aux travaux du chiffre.

Les archives THEVENIN nous ont donc apporté toutes les précisions souhaitables sur le rôle important de notre ancien mais elles nous ont beaucoup appris sur les travaux effectués avant la guerre de 1914 par la commission de cryptographie militaire sous la direction du général BERTHAUT dont le rôle a sans doute été plus important que nous le pensions jusqu'à présent. Nous en sommes très reconnaissant à l'Ingénieur Général du Génie Maritime THEVENIN.

Louis RIBADEAU DUMAS

(1) Cette dynastie THEVENIN n'est pas un exemple isolé ; je donnerai comme exemple la famille CHAUMONT dont l'ancêtre termina aussi sa carrière comme capitaine après l'Empire. Son fils et son petit-fils, passés par Saint-Cyr, furent respectivement général de division et général de brigade des Troupes de Marine. Il eut 3 arrière-petits-fils, 2 polytechniciens (promotions 1895 et 1896), artilleurs dont l'un termina sa carrière comme intendant général de 1ère classe, et un saint-cyrien, mort pour la France en 1915

Annexes

1 - Cours par correspondance de 1905
- exercice n° 3 (transposition simple - allemand)
- exercice n° 28 (substitution simple - allemand)
- exercice n° 30 (transposition simple - français)

2 – Annexes 1 et 2 à l'instruction secrète du 11 octobre 1919
(méthodes de surchiffrement des codes)

ANNEXE n° 1

Cours par correspondance de 1905

COMMISION
de
CRYPTOGRAPHIE MILITAIRE
-++++++++++-
Langue allemande

Transposition simple (Exercice n°3)
-+++++++++++++-++-

Les 4 cryptogrammes suivants ont été obtenus avec le même mot clef. Ce sont les phrases successives, d'un article sur le nouveau matériel de l'artillerie allemande.

I (384 lettres).

onrht deetm wsgnu huabi dnnre fuekr uinnt dtnze
dswne lnwsn ünnhw airer mtsve hdfue hnaik crede
deesn dhrsi rhrft wdash cnâve ezaet snbun induw
neoüh inmre acetf iwbet eögid nhtae sasns hntdl
osszr tennü fdrun egdee sidhe iauls awnar eechk
hobem onelc nuegc eaclh aiehe gimhe uzoge rsazw
ndeni ädcns nlhhr enaed unzwv escab innmt uniac
refmn gebth ainzn daelo amtin tnetl ewemr zbscr
cnüvo redli ozfis gtsct fweul wreez cente üenüw
irgee mdsea ilcce tregn lanw

II (112 lettres).

usgsi ecall dnill eedte endcn aolcg nbdrl rcecg
fhrhn herwt tdein kbnie sgbdg hitcl igeüt elnhe
trish üineh kuödi naean seank siens dl

III (240 lettres).

imadn heets ievco uieue dtügn iâdmi giuhd eegng
dtreu onaia sssea reumd iridu anunt ngetb eugbg
fnreo ndehn fneet ündll eirüg cnrne ettsi tseus
atzan bbsen ngozf bsncl etcnl wrnie desea wizeh
uigib dewni cgtss ebesi ahght rahis elgtn rinju
reala anfta eopeh snewe evgsn htnbs nhztc essnt

IV (144 lettres).

blwit abtac anasl arssi erier arsed nhrsp eeico
pgrbm eiesu xednr cntni nithg gnddl ataeg essih
otfrb abott idiwr reema behrr esesr ievab fidhi
dgswe winre chdvt lelte edgm

Langue allemande Substitution simple Exercice n° 28

Znjnifaztxsnijnxi ktkidpte.

Bdn ixyydyhrn znefamctadmdp dj ldjjafjb rfm jxj fxhr btim edn
yhrtj yt tlm du ndznjmadhrnj ixygafjb oxi ltazn znrfkm bfyg
bdn xjgxlidnbnjnj gxu fnygniymnj udmmna bny citmnymy gx
zindlnj ydhr lxni kninhrmdzm rdnamnj jfnuadhr gxu fmmnjmfm.

II

uqbkj cgyqp axbxb kqpau ckcxx brxcx zbrbr ubrav bpakx brymk
kqkpa brhbc jxbru bkryv kdimb ykxbr xmjki qrrgc ruubr zbrby
cgzvm ebyrb myrqw vgcqq scrvs qxkpa hvhyq wvshy

III

mstsl ydsrb jgwfd sbgsb deisd btktl dikoy dwudw wqgwf ykjmy
njgwk rwsfg jdbfs wgwyh rqgeg qyykq hrswx slbsd fdesw nmokq
qswfk hrnme stswf gynfs lwmwe sybkl tswse swslg qekmx slwsm
lgqqs yesbg wrgbm jydhr tdsfs wudww qgswf slwel mswfq dhrxs
lrgyn bnm g hrswr

IV

89880 10185 07013 10582 89820 51550 05098 89029 40050 30701
01508 58890 29090 58850 31052 30509 15015 00582 31058 28205
95880 58215 01250 78505 10070 13105 82098 01523 40050 95007
01315 00588 85821 50980 85070 13109 95059 16982 31050 19107
82310 58282 05902 95005 05880 10509 03690 10950 88501 55088
69010 58585 05010 95007 07500 50931 05828 21509 09880 99029
05090 58540 09502 90582 82099 02905 82910 78288 01898 80101
85070 13105 88019 58269 09808 91505 92095 03105 82316 98250
01158 29505 09501 50550 80500 71589 31880 50950 07050 13105
62058 25082 05501 50195 82059 58805 82050 10369 01015 00532

Langue Française Exercice n° 30

Transposition simple

Les cryptogrammes de l'exercice n° 30 sont relatifs à la guerre russo-japonaise.
Ils sont tous chiffrés avec des clefs différentes.

Le premier contient le mot japonaise.
Le second contient le mot dépourvu.
Le troisième contient le mot japon.
La clef du quatrième a 13 lettres.

La clef du cinquième a 16 lettres.
La clef du sixième a 20 lettres.

1.
srsau nieeu ssast lpdnu elgne rclud jxmdb dbsdo caidr eehsa
lreie atdua reoat usenu ioaov txnee eisqn srtou tntne aaoei
eeelr ciu

2
rdrse nnnal ahmle rreer asaii eosph tagao dsdnu rotne piuoe
sseuc eelee deeer aneas oecio vrcpv gtiar ruaue plsae miego
tieoi nadun epmue cefet fnett irpde uvrqi smrru apttl sriur
escoc h

3
apoee eopte tvpii eiene lutir apare jqptu isurn rrsos sgnri
tatce lrdct innae aaeau uttta isiem cegre etrmv pneee eopt

4
ennsp potsi uidis ttrnp pttts eneou rrnns pilne artse evaen
leniu sapid uasss nleda ssrla oeesi eorho clnin ttept cqaun
eiiea drala snste euisd debdn oetgt erlo

5
eaiiu lsfeo ebvds salil taeel creju agtei lnnsu rvqnq tlred
rttsn euine teenl senso pieeo uuduo atree srots rxsun onqru
teser ntatd oecaa gurbd taaie eerce neome

6
mcipe neoee evrla ideob mlstr ledpi ineae oumee asnts tsn

7
ieudp eeoec ioaed veavp tisac rirfu enatt ioers eqenq ieuee
deeep seoar udtur seris arvua prtnd italo snaoe vueop nrhtu
unlse orsms rvnpv r

8
ureie neuiu mseue ldact aeedt iarto atuss unieo loeed vitbs
aerti uivao trape taleu plero sfltt strei rretn esdis racso
ipnal alasp netar iegfo uiiur rainl uliai urri1 uaerd aeciu
seotx ermau odrac lesns tibnr uonrv tsaes mnedl slese aeass
sruil tjets snlnr uiene uviin esees htnmr aaelf iehpe sieee
qesld inul

ANNEXE n° 2

Annexes 1 et 2 à l'instruction secrète du 11 octobre 1919
(méthodes de surchiffrement des codes)

Le document reproduit ci-dessous se présente sous la forme d'un petit fascicule de 12 pages de format réduit (10 cm x 14 cm)

Page de couverture

MINISTERE
DE LA GUERRE
CABINET DU
MINISTRE
Section du Chiffre

REPUBLIQUE FRANCAISE

SECRET

ANNEXES 1 ET 2
A L'INSTRUCTION SECRETE
DU 11 OCTOBRE 1919
RELATIVE
A L'ORGANISATION ET AU FONCTIONNEMENT
DU SERVICE
DE LA CORRESPONDANCE CHIFFREE
DANS L'ARMEE
EN TEMPS DE PAIX

Annexe n° 1. - SURCHIFFREMENT
Annexe n° 2. - CHANGEMENT DE CHIFFREMENT

Texte des annexes

ANNEXE 1
A L'INSTRUCTION SECRETE
DU 11 OCTOBRE 1919
RELATIVE
A L'ORGANISATION ET AU FONCTIONNEMENT
DU SERVICE
DE LA CORRESPONDANCE CHIFFREE
DANS L'ARMEE
EN TEMPS DE PAIX

SURCHIFFREMENT

(§ 4 de l'instruction)

On n'emploiera, jusqu'à nouvel ordre, qu'un seul surchiffrement, le **surchiffrement A**

1. CARACTÉRISTIQUE DES TÉLÉGRAMMES SURCHIFFRÉS.

Avant le groupe indicatif du dictionnaire et après celui qui indique le nombre de groupes du texte chiffré, il y a un groupe *additionnel* de cinq chiffres constitué, comme il est indiqué ci-après, par le numéro répété de la *lettre initiale* (voir plus loin § 3) avec un zéro au milieu (voir plus loin § 6).

2. PRINCIPE DU SURCHIFFREMENT A.

Le surchiffrement A consiste en une *transposition simple* effectuée sur le chiffrement simple, d'après une *clef secrète*, mot ou groupe de mots ayant un total de 15 à 25 lettres, faciles à retenir par cœur et dont l'orthographe ne puisse donner lieu à aucune ambiguïté.

3. CLEF.

La clef littérale précitée est transformée en *clef numérique*, en numérotant ses lettres d'après leur ordre *relatif* dans l'alphabet normal. Ce numérotage ne commence pas par la lettre A, mais par une lettre quelconque qui est choisie arbitrairement par le chiffreur et qu'on appelle *lettre initiale*. Cette lettre initiale est désignée par son numéro d'ordre dans l'alphabet normal. Ainsi, si l'on prend la lettre L comme lettre initiale, cette lettre étant la douzième de l'alphabet normal, c'est le numéro 12 que le chiffreur inscrira dans un groupe additionnel de cinq chiffres, placé immédiatement avant le groupe indicatif du dictionnaire et constitué par le numéro 12 répété avec un zéro entre les deux répétitions : 12012

Il n'est pas nécessaire que la lettre initiale soit une lettre de la clef : il convient même de prendre également des lettres qui ne figurent pas dans la clef. Sans cette précaution, le relevé des lettres initiales donnerait une anagramme plus ou moins complete de la clef.

Si la clef littérale secrète est, par exemple, "**DOUBLE CHIFFREMENT**" et si le chiffreur choisit comme lettre initiale la douzième lettre de l'alphabet (L), on établira comme suit la clef numérique :

D	O	U	B	L	E	C	H	I	F	F	R	E	M	E	N	T
10	4	7	8	1	11	9	16	17	14	15	5	12	2	13	3	6

4. TRANSPOSITION.

a) On commence par chiffrer simplement le texte clair en remplaçant chaque mot ou expression usuelle par le groupe correspondant du dictionnaire employé : ces groupes sont écrits, chiffre par chiffre, sous les numéros de la clef numérique, par lignes horizontales successives.

b) Puis on relève les chiffres du tableau ainsi formé, par colonnes verticales, de haut en bas pour les colonnes qui ont un numéro impair, de bas en haut pour celles qui ont un numéro pair, en commençant par la colonne qui a le numéro 1, continuant par celle qui a le numéro 2, et ainsi de suite jusqu'à ce que tous les chiffres du tableau aient été relevés.

c) Les chiffres ainsi relevés sont groupés par cinq à partir du commencement, et ces nouveaux groupes constituent le texte surchiffré à transmettre.

5. EXEMPLE DE SURCHIFFREMENT.

Clef littérale : DOUBLE CHIFFREMENT (17 lettres)
Lettre initiale choisie par le chiffreur : L (12ème lettre de l'alphabet normal)
Texte obtenu par un premier chiffrement simple :

15987 30461 59326 30048 02954 45287 69305 51237
84261 04268 57931 61583 74130 60793 45106 73549

Tableau de transposition

D	O	U	B	L	E	C	H	I	F	F	R	E	M	E	N	T
10	4	7	8	1	11	9	16	17	14	15	5	12	2	13	3	6
1	5	9	8	7	3	0	4	6	1	5	9	3	2	6	3	0
0	4	8	0	2	9	5	4	4	5	2	8	7	6	9	3	0
5	5	1	2	3	7	8	4	2	6	1	0	4	2	6	8	5
7	9	3	1	6	1	5	8	3	7	4	1	3	0	6	0	7
9	3	4	5	1	0	6	7	3	4	5	9					

Relèvement par groupe de cinq chiffres

72361 02623 38039 54598 01975 00981 34512 08058
56975 01397 10347 36966 57651 52144 78444 64233

6. CONDITIONNEMENT DU TÉLÉGRAMME.

Le nombre de groupes (16) s'exprime par un groupe de 5 chiffres constitué par ce nombre répété avec un zéro au milieu :16016. Dans la pratique, le nombre de groupe est inférieur à cent.

La lettre initiale (12ème de l'alphabet normal) s'indique aussi par un groupe de cinq chiffres, numéro répété avec un zéro au milieu : 12012.

Si le chiffrement est fait avec un dictionnaire dont le groupe indicatif est 99999, le texte chiffré à expédier sera le suivant :

Numéro 16016 12012 99999 72361 02623 38039 54598
01975 00981 34512 08058 56975 01397 10347 36966
57651 52144 78444 64233

7. EXEMPLE DE DÉCHIFFREMENT.

Supposons qu'on ait à déchiffrer le télégramme suivant qui a été chiffré avec la clef secrète : DOUBLE CHIFFREMENT (17 lettres) :

Numéro 16016 12012 99999 72361 02623 38039 54598
01975 00981 34512 08058 56975 01397 10347 36966
57651 52144 78444 64233

Le groupe 12012 indique que la lettre initiale est la 12ème lettre de l'alphabet (L).

Le nombre de groupes de cinq chiffres du texte surchiffré étant de 16, le nombre de chiffres est 16 fois 5 ou 80.

On divise ce nombre par 17, nombre de lettres de la clef. Le quotient est 4 et le reste 12 : cela indique que le tableau de transposition a 4 lignes complètes (c'est-à-dire de 17 chiffres) et une cinquième ligne de 12 chiffres seulement.

On peut alors préparer le tableau de transposition et limiter inférieurement ses colonnes, comme suit :

D	O	U	B	L	E	C	H	I	F	F	R	E	M	E	N	T
10	4	7	8	1	11	9	16	17	14	15	5	12	2	13	3	6
				7									2		3	
				2									6			
				3									2			
				6									0			
				1												

Nous avons indiqué ci-dessus la préparation du tableau et le relèvement des deux premiers groupes de cinq chiffres : de haut en bas dans les colonnes de numéro impair, de bas en haut pour celles de numéro pair.

L'achèvement du travail ne présente aucune difficulté.

Il suffit ensuite de lire les groupes de cinq chiffres suivant les lignes horizontales successives de ce tableau et de les remplacer par les mots ou expressions usuelles qui leur correspondent dans le dictionnaire 99999.

8. OBSERVATIONS.

Il est indispensable d'effectuer avec le plus grand soin le numérotage de la clef littérale. On doit changer fréquemment de lettre initiale, en principe à chaque télégramme : chaque clef littérale donne autant de clefs numériques qu'elle a de lettres différentes.

L'indication exacte du nombre de groupes et de la lettre initiale est indispensable : c'est pourquoi pour tenir compte des erreurs de la transmission télégraphique, cette indication est répétée dans les groupes correspondants.

On doit également, notamment pour le déchiffrement, préparer avec le plus grand soin le contour du tableau de transposition.

Quand le nombre des groupes reçus est bien conforme à celui annoncé dans le groupe indicatif relatif, le déchiffrement ne présente aucune difficulté.

Il n'en est plus de même quand il manque des groupes.

Toutefois, si les groupes manquants sont peu nombreux, on pourra le plus souvent les reconstituer. Pour cela, on préparera le tableau de transposition d'après le nombre des groupes annoncé. puis on y recopiera le texte par le commencement : si les groupes manquants sont à la fin du texte, ils produisent des vides d'un seul chiffre dans un certain nombre de groupes qu'on pourra souvent deviner d'après le sens général et en faisant état des chiffres reçus. Si les groupes manquants étaient au commencement du texte, on commencerait à remplir le tableau de transposition par la fin. Enfin si les groupes manquants sont au milieu, on pourra remplir le tableau de transposition simultanément par le commencement et la fin.

Ce travail de reconstitution devra être essayé chaque fois qu'il manquera des groupes, et avant toute demande de répétition. Les officiers qui auront à recevoir fréquemment des télégrammes surchiffrés devront être exercés particulièrement à ce travail qui exige de la méthode, une certaine perspicacité et beaucoup de persévérance.

ANNEXE 2
A L'INSTRUCTION SECRETE
DU 11 OCTOBRE 1919
RELATIVE
A L'ORGANISATION ET AU FONCTIONNEMENT
DU SERVICE
DE LA CORRESPONDANCE CHIFFREE
DANS L'ARMEE
EN TEMPS DE PAIX

CHANGEMENT DE CHIFFREMENT

(§ 10 de l'instruction)

Au cours d'un chiffrement *simple*, l'opérateur peut modifier les groupes du dictionnaire en employant l'une quelconque des cinq variantes suivantes qu'il indique par le groupe correspondant du dictionnaire :

Chiffrement n° 1 ; chiffrement n° 2 ; chiffrement n° 3 ; chiffrement n° 4 ; chiffrement n° 5.

On peut employer le changement de chiffrement soit au commencement, soir à partir d'un groupe quelconque et utiliser, dans un ordre également quelconque, les cinq changements prévus : le groupe indiquant le changement de chiffrement doit être évidemment chiffré comme les groupes précédents, le nouveau chiffrement ne commençant qu'immédiatement après.

Chiffrement n° 1 : Ajouter une unité à chaque chiffre du dictionnaire.
Chiffrement n° 2 : Ajouter 2 à chaque chiffre du dictionnaire
Chiffrement n° 3 : Ajouter 3 à chaque chiffre.
Chiffrement n° 4 : Ajouter 4 à chaque chiffre.
Chiffrement n° 5 : Ajouter 5 à chaque chiffre.

Les additions se font sans retenue : exemple 7 plus 4 égale 1.
Le groupe du dictionnaire **86731** deviendrait :

97842 *avec le chiffrement n° 1*.
08953 *avec le chiffrement n° 2*.
19064 *avec le chiffrement n° 3*.
20175 *avec le chiffrement n° 4*.
31286 *avec le chiffrement n° 5*.

Les changements très simples indiqués ci-dessus pourront être modifiés de temps en temps : les variantes seront communiquées en temps utile par la Section du Chiffre.

Imprimerie Nationale -- 10 -1919