CRYPTOGRAPHIA MILITARA

SAU

ARTA DE A CORESPUNDE

IN

MOD SECRET

IN

TIMP DE RESBEL

LUCRATA

DE

Căpitan D. CHRISTU

CONSILIUL DE RESBOIU, CRAIOVA

CRAIOVA

TIPO-LITOGRAFIA NATIONALE RALIAN ȘI IGNAT SAMITCA

1894.

CRYPTOGRAPHIA MILITARA

SAU

ARTA DE A CORESPUNDE

IN

MOD SECRET

IN

TIMP DE RESBEL

LUCRATA

DE

Căpitan D. CHRISTU

CONSILIUL DE RESBOIU, CRAIOVA

CRAIOVA

TIPO-LITOGRAFIA NAȚIONALE RALIAN ȘI IGNAT SAMITCA

1894.

UVRAGELE CONSULTATE

I. Écritures secrètes dévoilées par Charles Joliet.

II. Cryptograhpie militaire par Aug. Kerckoffs.

III. Cryptographie et ses application a l'art militaire par H. Josse.

IV. L'art de dechiffrer les écritures secrètes par Edme Simonet.

V. La correspondance secrète devoilée par J. de Rioles.

VI. Science et guerre par Henry Mami.

VII. La télégraphie optique par Max de Nansouty.

VIII. Etudes de guerres par Général Lewal.

IX. Science militaire cryptographie par Capitaine Valerio.

Dedic acéstă lucrare șefilor mei.

CRYPTOGRAPHIA MILITARA

SI

TELEGRAPHIA OPTICĂ

Cryptographia este un auxiliar puternic al tacticeĭ militare.

General **LEWAL.**

Aplicațiune la arta militară

In resboiul modern, fie că el se produce între două națiuni civilisate, fie că se produce între o națiune civilisată și una barbară, trebue să recurgem la tóte resursele sciințifice, pentru a accelera operațiunile.

Acéstă tendință s'a manifestat pentru prima óră în Statele-Unite, în timpul resbeluluĭ de succesiune; așa spre exemplu, în acest resboiŭ, tot ce se considera până în present că ține de domeniul fantasieĭ, în acest resboiŭ s'a pus în aplicare, spre exemplu: torpilele, bastimentele sub-marine, balónele și telegraphia electrică care jucară un rol neașteptat.

Origina Cryptographieĭ

Cryptographia vine de la cuvêntul grec (κρυπτος ascuns γραφος scriere), adică este arta de a scrie într'un mod secret și misterios. Acéstă sciință este veche ca

și lumea, origina sa se confundă cu a telegraphieĭ militare, ea a fost cultivată în timpurile cele maĭ vechĭ de Chinezĭ, Perșĭ și Cartaginezĭ, a figurat chiar în scólele tactice din Grecia, și era fórte mult cunoscută de ceĭ maĭ iluștri generalĭ Romanĭ.—Noĭ nu posedăm de cât știrĭ fórte incomplecte asupra procedeurilor Cryptographieĭ propriu dise. In timpul evuluĭ-mediu, ea n'a fost cultivată de cât fórte puțin; în al 17-lea secol, faptul de a conrespunde într'un mod secret, era considerat ca o circonstanță agravantă de tribunalele engleze.

Ast-fel în faimosul proces intentat conteluĭ de Sommerset pentru crima de otrăvire, cancelarul Baconn a ridicat ca o culpă gravă contra nobiluluĭ acusat, obiceiul sĕu de a scrie în mod secret

Sub Henric al IV-lea niște scrisorĭ secrete, carĭ emană de la membriĭ ligeĭ guvernuluĭ Spaniol, le-a dat matematiculuĭ Viete de a le găsi cheia; acesta reușĭ și ast-fel Regele putu în timp de 2 anĭ a'și surveghia intrigile inamicilor sĕĭ.

Sub Richelieu, arta de a descifra scrierile secrete se ridică la înălțimea uneĭ sciințe de Stat.

Un ilustru diplomat a dis: «Cuvêntul a fost dat omuluĭ pentru a'și ascunde gândirea»; putem dice însă cu maĭ multă esactitate, că: «omul a inventat scrierea pentru a deghiza gândirea.» — Cu tóte acestea nu se póte găsi urme sigure de întrebuințarea corespondenței Cryptographice în armată în al șése-spre-decelea secol, dar se știe positiv că în al XVII-lea secol, ordinile nu se transmiteau generalilor comandanți pe frontieră saŭ în țara inamică de cât cifrate.

In resbóele primuluĭ Imperiu, Cryptographia a jucat un mare rol, generaliĭ aveau douĕ cheĭ pentru a putea

corespunde între ei și cu Statul-Major General, marea cheie și mica cheie.

Baronul Fain, secretarul lui Napoleon I, spune că în timpul resbelului cu Rusia, Impĕratul întreținea corespondențe secrete.—Astă-di corespondența prin cifre secrete, este adoptată în tóte armatele Europei, dar nu este aplicată într'un mod sistematic de cât în biurourile cancelariilor diplomatice.

La început se serveau popórele antice de a corespunde în mod secret prin ajutorul obiectelor esterióre carî frapau vederea, spre exemplu: plante și diferitele florî, spre exemplu: un buchet dispus într'un mod órecare indica gândirea aceluia care îl trimitea, acel care îl primea cunoștea semnificarea dupĕ înțelegerea care o aveau maî înainte. Acest procedeu este fórte vechiŭ și nu indica de cât într'un sens general un *da*! sau *nu!* un *vino!* sau *stăi! a face* sau *a nu face* un lucru órecare, prin urmare nu puteau a transmite frase întregi.

Scrierea cu cernélă simpatică este asemenea un mod de a scrie secret; se știe că acéstă cernélă invizibilă în condițiunî obicinuite, apare scrierea îndată ce încălzim hârtia sau o supunem la acțiunea unuî reactiv chimic convenabil.

Un alt mod de a corespunde într'un mod secret era de a se servi de note de musică, combinându-le cu cheie și mĕsură pentru a representa literile alfabetuluî și a permite ast-fel cifrarea unuî text clar.

In fine un procedeu maî recent de a scrie și de a citi era de a citi rêndurile după o dată convenită, adică din două în două, saŭ din treî în treî rêndurî pentru a afla adevĕratul înțeles; ast-fel a fost scrisórea trimisă de Madame Saint-André prințuluî Condé.

Langajul de a scrie în mod secret consistă, după cum am vĕdut mai sus, a întrebuința cuvinte la care le dă un sens diferit;– ast-fel Meuseur Gisquet, vechiŭ prefect de poliție, istorisește în memoriile sale în corespondența relativă la complotul organisat în 1831 de Prințul Louis Napoleon; conjurații numeaŭ pe acest prinț în corespondență M-me Charles, poliția prin M. Pauberg, armata prin M-lle Amelie etc. etc.

Germanii au admis în principiu, că corespondența cryptographică trebue întrebuințată de maniera cea mai întinsă, programele scólelor militare prescrie nu numai de a exersa oficerii la compositiuni și la citirea depeșelor secrete, dar încă de a iniția la cunóșterea tutulor principiilor ale arteĭ de a descifra și Germania a admis-o chiar în reglemente.

Un sistem de cryptographie, de o întrebuințare ușóră este o lacună, a zis generalul Lewal.—Ceĭ mai marĭ generalĭ sunt de opiniune, că este indispensabil că diferiții comandanți aĭ uneĭ armate, să aibe la dispositiunea lor un sistem de comunicațiuni secrete, pentru a corespunde liber nu numaĭ între eĭ și cu comandantul En-Chef, dar încă cu sub-alternii lor; afară de acésta trebue ca din timp de pace a se exersa oficerii la mănuirea acesteĭ corespondențe. — Generalul Bardin în uvragiul sĕŭ dice: că în anul 1814, când Napoleon voia a reuni tótă armata și că Feltre și Berthie expediară ordinile sale, și puține depeșĭ parveniră la destinație, căcĭ inamicul prinse cea mai mare parte. Și se póte, dice generalul Bardin, că sórta Francieĭ și fața Europeĭ au depins de la deslegarea unuĭ cryptogram.—Nu este destul numaĭ de a scri o scrisóre cifrată, dar trebue să dea garanții serióse de indiscifra-

bilitate, căcĭ, partea slabă a celor maĭ multe sisteme imaginate până astă-dĭ, are defectul capital de a fi ghicite saŭ se află în presența unor inconveniente fórte marĭ. — In resbelul Turco-Rus s'a primit într'o Duminecă de la un atașat militar care urmărea operațiunile armatelor în luptă, o depeșă cifrată, și pentru că șeful de biurou care era însărcinat cu corespondența cryptographică era lipsă, n'a putut fi descifrată.

Ministrul care nu cunoștea cheea depeșeĭ, însărcină pe un ofițer de stat major de a căuta și a deslega fără cheiă și într'adevĕr în timp de câte-va ore cryptogramul a fost tradus. Cu tóte acestea, mulțĭ zic că cryptographia este un auxiliar puternic al tacticeĭ militare, pentru că sórta uneĭ armate, a unuĭ oraș și chiar destinele uneĭ țĕrĭ depinde maĭ mult sau maĭ puțin de la descifrarea maĭ curând sau maĭ târziu a unuĭ cryptogram; va trebui, prin urmare, a ne feri de a adopta sisteme dupe carĭ un individ, cât de puțin esperimentat, va descifra un cryptogram în timpul cel maĭ scurt. — Generalul Lewal în cartea sa *Etudes de guerre*, zice că cifrele cu basa variabilă sunt aprópe necitite, saŭ și décă se ajunge a le descifra acésta însă nu se capătă de cât cu dificultățĭ fórte marĭ. — Voltaire a zis că aceia carĭ se încércă a descifra o scrisóre fără a fi instruit în afacerile de care se tratează, și fără a cere ajutóre, care să-ĭ pue în cunoștințe, sunt ceĭ maĭ marĭ șarlatanĭ, sunt tocmaĭ ca aceia carĭ se încércă să înțelégă o limbă pe care nicĭ n'a învĕțat'o.

Desiderata Cryptographieĭ militare.

Trebue a distinge bine un sistem de scrierĭ secrete imaginate pentru un schimb momentan de scrisorĭ în-

tre câte-va persóne isolate, și între o metódă de cryptographie, destinată a regula pentru un timp ilimitat corespondența diferiților șefi ai armatei între dênșii. — Pentru că aceștia din urmă nu pot, dupe plăcerea lor, și la un moment dat a modifica convențiunile lor; mai mult încă, ei nu trebue să aibe asupra lor nici un obiect sau scriere care să fie de natură a lumina inamicul asupra sensului depeșelor secrete, cari s'ar putea să cadă în mâinile séle.

Un mare număr de combinațiuni ingenióse póte corespunde la scopul propus; în general însă un sistem trebue să îndeplinéscă următórele condițiuni:

I. Sistemul trebue a fi materialmente dacă nu matematic, cel puțin descifrabil.

II. Cheia trebue a fi comunicată și reținută fără ajutorul notelor scrise, și a fi schimbată dupe plăcerea corespondențelor.

III. Sistemul trebue să fie aplicabil la corespondența telegrafică.

IV. Sistemul să fie portativ și mănuirea să nu necesite concursul mai multor persóne.

V. Este necesar ca sistemul să fie de o întrebuințare ușóră, necerând multă tensiune de spirit, nici cunósterea unei lungi serii de regulĭ de observat.

Multe persóne autorisate susțin, că indescifrabilitatea absolută a unei scrieri secrete nu trebue a fi considerată ca o condițiune sine qua-non pentru a fi admisă în serviciul armatei, pentru că instrucțiunile cifrate transmise în timp de resboĭ, n'au de cât o importanță momentană și nu necesită păstrarea secretului de cât pentru 3 sau 4 ore de la data lui și puțin importă dacă dupe acest timp inamicul cunóște coprinsul.—Prin

urmare admite ca sistemul să fie combinat de o manieră ast-fel ca traducerea lui să necesite trei sau patru ore.

Acéstă argumentațiune la prima vedere pare justă, însă în fond este falsă, pentru că secretul unei comunicațiuni trimisă la o distanță óre-care 'și conservă prea adesea importanță mai mult timp; fără a mai enumera tóte eventualitățile cari se pot presenta, n'avem de cât să citãm casul unde un comandant al unui oraș asediat trimite știri armatei care să 'i vină în ajutor; ceva mai mult: o dată ce un cryptogram a fost descifrat de inamic tóte cele-l-alte ce 'i va cădea în mână va fi descifrate instantaneu.

Facultatea de a schimba chiar dupe voință cheia este o condițiune esențială a sistemului cryptographic și este un avantagiu care nu este bine definit și pentru realisarea practică póte să dea naștere la veri un tor, în raport cu diferitele peripeții ale unei lungi perióde de campanie. — Francia este pe punctul de a înlocui dicționarul cifrat printr'un sistem mai practic.

In Cryptographie se face us de un numĕr óre-care de termeni speciali de care se simte necesitate a le cunóște definițiunea exactă înainte de a începe studiul acestei științe.

Langaj clar: Este acela în care tóte cuvintele limbei întrebuințată într'o corespondență, au semnificarea reală, conform geniului limbei.

Cuvinte clare: Intr'o corespondență cryptographică sunt părți, cuvinte sau frase isolate, cari represintă un sens perfect definit în limba întrebuințată pentru a scri corespondența.

Langaj convenit: Este acela în care cuvintele în-

trebuințate au o semnificațiune cu totul diferită de aceia care o au în limba ordinară; acéstă semnificațiune nouă fiind determinată printr'o convențiune prealabilă între corespondenți.

Langaj cifrat: Este acela în care se întrebuințéză cifre, litere sau alte semne convenționale, pentru a representa literile, cuvintele sau chiar frasele langajuluĭ clar.

Cheie: Se numesce cheia unuĭ sistem cryptographic, convențiunea dupe care putem transforma un text clar, în text cifrat, sau a traduce în langaj clar un text cifrat. Cheia constitue prin urmare partea cea maĭ importantă a unuĭ sistem cryptographic.

Un sistem se ḑice cu cheie simplă, când are o singură convențiune și cu cheie multiplă când are maĭ multe convențiunĭ.

Se numesce cifre în cryptographie literile, cifrele sau semnele convenționale óre-carĭ, întrebuințate pentru a represinta o literă, un cuvênt sau o frasă a langajuluĭ clar. — Cryptographia se servă maĭ tot-d'auna de cifre arabe.

Cryptogram. Se numesce o scriere în litere secrete.

Cryptograph. Se numesce acela care execută diversele operațiunĭ de cryptographie; se maĭ înțelege prin cryptograph un aparat care permite d'a executa într'un mod mecanic o parte din operațiunile de cryptographie.

Se înțelege prin valoarea unuĭ sistem cryptographic, adunarea dificultăților carĭ presintă acel sistem pentru a descifra un cryptogram fără să cunóscem cheia. Acéstă valoare se compune din douĕ elemente.

I-iŭ. Valoarea matematică care este numĕrul total obținut prin calcul de convențiunile sau cheile diferite pe carĭ sistemul permite a le întrebuința.

II-lea. Valoarea materială este constituită prin dificultatea care încércă descifrorul a dirige căutările séle într'un sens sau într'altul, dupe dispositiunile date cifrelor carĭ compun cryptogramul; este evident că din punctul de vedere matematic, sistemul care posedă cel maĭ mare numĕr posibil de convențiunĭ diferite va fi cel maĭ bun, dar acésta nu póte fi de cât acel sistem care va avea o valoare absolută mare, sau maĭ bine dis acela care va oferi maximum de dificultățĭ descifrorilor.

Rensenimentele preliminare carĭ trebue a 'și le procura un descifror.

Un descifror trebue tot-d'auna a începe prin a se înconjura de documente carĭ 'l pot pune pe calea de descoperire, acestea sunt:

I. Numele și qualitatea persónei care trimite depeșa secretă.

II. Numele și qualitatea persónei căria 'ĭ este adresată depeșa secretă.

III. Este probabil că descifrorul să cunóscă limba în care depeșa este scrisă.

IV. Punctul de unde este trimésă depeșa și punctul unde trebue să mérgă.

V. Evenimentele importante carĭ pot motiva trimiterea uneĭ depeșe secrete.

Intrebuințarea Cryptographieĭ militare.

Cryptographia militară presintă două marĭ divisiunĭ:

I. Cryptographia militară propriu dișă în timp de pace și în timp de rĕsboĭ.

II. Cryptographia militară de circonstanțe în timp de pace și în timp de rĕsboĭ.

In timp de pace: Cryptographia militară propriu ḑisă, se aplică la corespondențele secrete ale Ministruluĭ de rĕsboĭ, cu generaliĭ comandanțĭ de corp de armată, de divisiĭ și de brigăzĭ, cu șefiĭ de corpurĭ și cu șefiĭ marilor serviciĭ ale armateĭ, prin urmare corespondența militară secretă în timp de pace trebue reglementată într'un mod uniform de la ministru, șeful armateĭ, până la șefiĭ de corpurĭ și între diversele autorităț militare.

Cryptographia militară de circonstanțe în timp de pace coprinde:

I. Corespondența secretă eventuală între șefiĭ militarĭ și funcționariĭ celor-l'alte departamente militare; acéstă chestiune trebue reglementată ast-fel ca să se evite încurcăturile carĭ s'ar produce în óre-carĭ casurĭ.

II. Corespondența secretă a serviciuluĭ rensenimentelor, corespondențe carĭ se sustrag de la orĭ-ce spețe de reglementațiune. Procedeurile întrebuințate variază cu inteligența agenților și în condițiunile în carĭ trebue a corespunde; aceste procedeurĭ trebue a fi fórte multiple.

In timp de rĕsboĭ: Cryptographia militară propriu ḑisă ia o importanță considerabilă. Istoria ne oferă numeróse exemple de operațiunĭ bine combinate carĭ n'au reușit, pentru că ordinele de execuțiune scrise în langaj clar au căzut în mâinile inamiculuĭ; dar chiar pe câmpul de bătae, cryptographia nu trebue a fi întrebuințată cu cea maĭ mare reservă, pentru că ordinile nu vor putea fi nicĭ o-dată prea clar, momentele sunt precióse și orĭ-ce întârḑiere póte deveni fatală.

Cryptographia militară de circonstanțe în timp de rĕsboĭ coprinde: I. Corespondența secretă a generaluluĭ en-chef cu guvernul. II. Corespondența serviciuluĭ rensenimentelor și III. Corespondența corpurilor de partisanĭ dacă este formată.

Acéstă corespondență secretă ca și aceia a serviciuluĭ rensenimentelor, nu trebue a fi reglementată înainte, în ceia ce privesce procedeurile de întrebuințat.

Numĕrul sistemelor cryptographice a le întrebuința simultaneu.

Generalul Lewal a definit fórte clar trebuința Cryptographieĭ militare, el ḑice în tactica rensenimentelor:

«Trebue cifre personale pentru comandant en-chef, cifre speciale pentru comandanțiĭ de corpurĭ de armată sau diviziĭ de cavalerie, cifre generale pentru tóte unitățile: diviziĭ, brigade, regimente și șefĭ de serviciurĭ, cifre particulare pentru oficeriĭ aceluiaș regiment. Aceste 4 cifre nu presintă de cât o complicațiune aparentă: în realitate fie-care unitatate nu posedă de cât două. La marele quartier general trebue a avea tóte cifrele, caracterele sau semnele convenționale întrebuințate de armată.»

«Cifrele speciale, cifrele generale și cifrele particulare pot în fine aparține aceluiaș sistem cryptographic, întrebuințat cu una sau maĭ multe cheĭ diferite în fie-care cas. In fine trebue a se menagia posibilitatea de a schimba sistemul dacă se bănuesce că inamicul a parvenit a cunósce cheia; resultă prin urmare necesitatea absolută pentru oficeriĭ de Stat-Major de a se ține în curent cu diversele metóde cryptographice și de ameliorațiunile care li se póte aduce.»

Cryptographia maritimă.

Marina este familiarisată de mult timp cu cryptographia (mai cu sémă marina puterilor Europei).

Fie-care comandant de bastiment trebue să posede mijlóce de corespondențe secrete cu șefii ierarhici până la Ministru inclusiv, cu colegii sei, cu bateriile de cóste și cu cea mai mare parte din agenții diplomatici ai noștri în streinătate.

Aceste mijlóce de corespondențe secrete cari se aplică destul de bine la comunicațiunile scrise ca și la comunicațiunile telegrafice, consistă în întrebuințarea de cod de semnale și de dicționare cifrate, unele în litere, altele în cifre.

Transmisiunile telegraphice a căror esecuțiune este încredințată personal Timonieruluĭ, se face cu brațul pentru distanțele micĭ prin adjutorul Flamelor (torțe) și paviliónele patrate pentru distanțe mijlociĭ și prin mijlocul a treĭ semnale pentru distanțe marĭ.

Nóptea semnalele se fac prin adjutorul Fanarelor (lanterne marĭ care sunt pe vase), artificiĭ și chiar prin lovituri de tun.— Pentru a asigura secretul comunicațiunilor se întrebuințézĕ de preferință conveńțiuni variabile, mai cu sémă în timp de resboĭ.

In fine în cas de naufragiu sau de perderea unuĭ bastiment printr'o causă óre-care, comandantul este ținut, sub responsabilitatea sa, de a distruge tóte documentele confidențiale cari se află în posesiunea sa, așa spre esemplu conveńțiunile adoptate pentru semnalele de recunóscere în timp de rĕsboĭ și cele relative la corespondențe secrete. — Aceste documente sunt închise într'o cutie de plumb care trebue să fie aruncată în mare.

Redacțiunea cryptogramelor militare.

Un cryptogram militar trebue a fi tot-d'a-una concis și clar; aceste sunt două condițiuni indispensabile, dér carî nu pot fi tot-d'a-una ușor de a le îndeplini.

Adesea în scop de a scurta lucrarea nu se cifrează de cât o parte din text, lăsând cea-l-altă parte clară; alegerea părții care trebue cifrată este de cea mai mare importanță.

Dacă acéstă alegere este rău făcută, atunci riscăm ca cheia să fie descoperită.

Nu sunt regulî precise de dat în acéstă privință; alegerea părții din text care trebue cifrată și aceia care trebue lăsată clară, depinde fórte adesea de diverse circonstanțe, pe carî este imposibil a le precisa dinainte; în tot casul este absolut necesar ca ofițerul însărcinat de a cifra un text să posede o practică suficientă de cifrele carî trebue a le întrebuința.

Când va fi nevoie a transmite telegrafic o depeșă cifrată este indispensabil de a face us de semnele convenționale de punctuațiune, și depeșa va căștiga considerabil în claritate când va fi supusă descifrăriî.

I. Când nu este biurou de post de telegrafie în localitatea unde se scrie depeșa va trebui în tot-d'a-una a începe textul cifrat prin indicațiune clară, arătând locul, data și chiar indicațiunea oreî.

II. Nicî o dată nu va trebui expediată o depeșă cifrată fără a sci să o descifreze chiar acel care a făcut-o, sau a o da altuî ofițer a o descifra, ast-fel, cu modul acesta se va evita erorile carî s'ar fi putut comite la operațiunea cifrăriî.

III. Textele remise telegrafiștilor, trebue a fi scrise

cu îngrijire și citeț și a separa grupele de litere sau de cifre.

IV. Hârtia care a servit la operațiunea cifrării sau descifrării, trebuesce arsă.—Aceste regulĭ, pentru a avea sancțiunea lor practică, trebue a fi riguros observate în interesul siguranțeĭ corespondențeĭ cryptographice.

Se póte distinge printre diferitele sisteme de scrierĭ secrete treĭ metóde principale:

I. Metóda care se baséză pe o simplă transpositiune a literilor textuluĭ într'un mod clar.

II. Metóda care se baséză pe o combinare de cifre intervertind ordinea alfabetică a literilor.

III. Metoda este aceia care represintă silabele, cuvintele sau chiar frase întregĭ prin numere sau grupe de litere.

Intâia metódă prin transpositiune.

Sistemele carĭ se baséză pe transpositiunea literilor sunt fórte vechĭ, permit variațiunĭ numeróse și au servit de bază la óre-care aparate mecanice.

Iată un esemplu de transpositiune elementară.

Literile depeșeĭ trebuesc scrise în ordinea lor naturală, pe un numĕr de liniĭ determinate, atât orizontale cât și verticale. După acésta se copiază din nou acestă litere dupe o ordine convenită maĭ dinainte, și acésta a doua dispositiune constitue aceia ce se numește cheia cryptogrameĭ.

Iată un exemplu:

Un atacu va avea loc mâine de dimineață.

A	1	2	3	4	5	6	7	8	9	10	11	
1	u	n	a	t	a	c	u	v	a	a	v	Se scrie literile depeșeĭ în ordina lor naturală.
2	e	a	l	o	c	m	a	i	n	e	d	
3	e	d	i	m	i	n	e	a	t	a	l	
4	a	p	a	t	r	u	c	e	a	s	u	Pentru complectarea linieĭ a 5 se scrie literile alfabetuluĭ până la fine.
5	r	i	a	b	c	d	e	f	g	h	i.	

Acésta este cheia Cryptogrameï.

B	2	11	9	8	5	3	10	1	7	6	4
1	n.	v.	a.	v.	a.	a.	a.	u.	u.	c.	t.
2	a.	d.	n.	i.	c.	l.	e.	e.	a.	m.	o.
3	d.	l.	t.	a.	i.	i.	a.	e.	e.	n.	m.
4	p.	u.	a.	e.	r.	a.	s.	a.	c.	u.	t.
5	i.	i.	g.	f.	c.	a.	h.	r.	e.	d.	b.

Scriem literile din nou dupe ordinea în care se află pe cheie și acésta constitue secretul depeșeï, și avem: n v a v a a a u u c t a d n i c l e e a m o d l t a i i a e e n m p u a e r a s a c u t i i g f c a h r e d b.

Odată ce acela care este însărcinat cu citirea uneï cryptograme se înduoesce de procedeul care a fost adoptat și chiar dacă a fost schimbată cheia, atunci descifrorul n'are de cât o afacere de tatonament. Nu are de cât să numere numĕrul literilor din cryptogram și numĕrul găsit îl descompunem în duoï factorï și în casul de față avem 55 de litere; aplicând regula avem: $55=5\times11$. Prin urmare 5 va represinta numĕrul liniilor orizontale și 11 numĕrul liniilor verticale și prin urmare nu vom avea de cât o serie de tatonamente pentru a ajunge la resultat.

Cu ocasiunea celuï din urmă proces intentat nihiliștilor jurnalele ruse au făcut cunoscut sistemul de scriere secretă adoptată de acuzați; acest metod este basat pe dubla transpositiune, adecă literile, dupe ce au fost pentru prima óră transpuse în colóne verticale, sunt pentru a doua óră transpuse în sensul colónelor orizontale. Acelaș cuvênt servă de cheiă pentru amêndouĕ transpositiunile. In sfârșit le transformă în formula numerică, punênd în locul fie-căreï litere o cifră arabă. Iată procedeul aplicat la cuvêntul Schuvalow:

Exemplu: Vĕ invit a vĕ presenta de urgenţă la Ministerul de resbel mâine la opt ore precis cu planul.

Cheia

Schuvalow
623781459

achlosuvw
123456789

A	1	2	3	4	5	6	7	8	9
1	v.	e.	i.	n.	v.	i.	t.	u.	a.
2	v.	e.	p.	r.	e.	s.	e.	n.	t.
3	a	d.	e.	u.	r.	g.	e.	n.	t.
4	a.	l.	a.	m.	i.	n.	i.	s.	t.
5	e.	r.	u.	l.	d.	e.	r.	e.	s.
6	b.	e.	l.	m.	a.	i.	n.	e.	l.
7	a.	o.	p.	t.	o.	r.	e.	p.	r.
8	e.	c.	i.	s.	c.	u.	p.	l.	a.
9	n.	u.	l.	a.	b.	c.	d.	e.	f.

Facem transposiţiune verticală şi avem:

B	6	2	3	7	8	1	4	5	9
6	i	e	l	n	e	b	m	a	l
2	s	e	p	e	n	v	r	e	t
3	g	d	e	e	n	a	u	r	t
7	r	o	p	e	p	a	t	o	r
8	u	c	i	p	l	e	s	c	a
1	i	e	i	t	u	v	n	v	a
4	n	l	a	i	s	a	m	i	t
5	e	r	u	r	e	e	l	d	s
9	c	u	l	d	e	n	a	b	f

Acésta a doua transpunere se face în modul următor:

Ne uităm în transpunerea orizontală A şi căutăm la No. 6 orizontal şi vertical şi vedem că conrespunde litera i, o scrim sub 6 în tabloul B, dupe aceia ne uităm la No. 2 şi vedem că conrespunde litera e, 'l scrim sub 2, după aceia căutăm pe 3 şi vedem că găsim pe l 'l scrim sub treĭ şi aşa maĭ în colo.

Dupe ce am format acésta a doua transpunere, scriem pe hârtie literile în ordinea în care se află, şi avem: ielnebmalsepenvretgdeenaurtrop epatoruciplescaieituvnvanlaisamit erureeldsculdenabf.

Şi cu modul acesta am format cryptogramul dupe cheia Schuvalow cu dublă transpositiune.

Metoda lui Iuliu Cesare.

Acéstă metodă este fórte veche. Cartaginesii și Fenicienii au întrebuințat-o cu mult înaintea lui Cesare, pe care el i-a dat numele sĕu.

Acéstă metodă consistă de a interverti literile alfabetului ordinar în un ordin convenit și a înlocui în sfârșit literile alfabetului normal prin acelea carĭ corespund alfabetului nou, ordinea adoptată prin acest nou alfabet constitue cheia.

Valórea sistemului. Alfabetul românesc coprinde 26 de litere și dacă vom face a începe alfabetul prin una din aceste 26 litere pe rênd, cele-l'alte conservându-și rangul lor normal, vom obține 26 de alfabete de convențiune, spre exemplu:

a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z.
b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, a.
c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, a, b. etc.

Dar în fie-care alfabet putem interverti ordinea celor 26 de litere într'un mod arbitrar și numĕrul de convențiunĭ ce putem să 'l facem într'un alfabet óre-care este representat prin numĕrul de permutațiunĭ pe care 'l putem face prin cele 26 litere, fie:

$1\times2\times3\times4\times5\times6\times7\times8\times9\times10.....\times21\times22\times23\times24\times25\times26$ și cum se póte repeta aceeași operațiune în fie-care din cele 26 alfabete, numĕrul total de convențiunĭ printre carĭ vom putea alege, va fi de $1\times2\times3\times4.....\times21\times22\times23$, obținem cu modul acesta ca valóre matematică a sistemului un numĕr fórte mare,—cu tóte acestea acest sistem este cel maĭ ușor de descifrat; să facem un exemplu: să suposăm că adoptăm ca convențiune (cheie) următórea:

Tóte literile alfabetuluĭ normal vor fi înlocuite prin acelea carĭ urmézĕ imediat dupe dênsele.

Să cifrăm un exemplu: *Plecaţi imediat fără întârziere!!*

O să avem cryptogramul următor:

r m f d b u j j n f e j b u g b s b j o u b s q j f o f

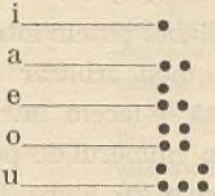
Alfabete de convenţiune.

Alfabetele de convenţiune intră de ordinar în metoda luĭ Iuliu Cesare.

Alfabetele Benedictine

Benedictine a semnalat alfabete de convenţiune întrebuinţate în al 4-lea secol al ereĭ nóstre.

I-iul *Alfabet.* In întâiul alfabet vocalele erau suprimate şi înlocuite prin puncte după cum se vede maĭ jos.



Exemplu: Să facem o aplicaţie la acest alfabet.

«*Am terminat planurile.*»

Vom avea cryptogramul următor:

•• m t :• r m •n •• t p l •• n :•:• r •l :•

Al douilea alfabet. Vocalele erau suprimate şi înlocuite prin consune care le urma imediat în alfabetul normal. *Spre exemplu:* «Mâine porneşte două companiĭ la 6 ore, şi vom avea cryptogramul următor:

m b j n f p p r n f s t f d p v f c p m p b n j l b 6 p r f.

Cu tótă aparența bizară a acestor alfabete, textele scrise în aceste sisteme nu oferă nicĭ o dificultate de descifrare.

La prima vedere în întâiul alfabet se vede lipsa vocalelor, semnul cel mai des repetat represintă vocala e, cele-l'alte se găsesc cu multă ușurință.

Alfabet normal dispus pe două liniĭ.

Acest sistem este fórte vechiŭ și consistă în a dispune alfabetul pe două liniĭ orizontale, ast-fel avem:

a b c d e f g h i k l m

n o p q r s t u v x y z.

Litera j și w este suprimată în acest alfabet, punem în locul fie-căreĭ litere din cuvêntul care voim a'l cifra litera care conrespunde în cea-l'altă linie. Ast-fel depeșa: «*Veĭ ataca flancul stâng*» va fi representată prin cryptogramul următor:

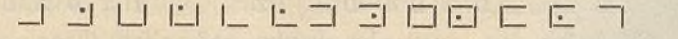
i r v n g n p n s y n a p h y f g n a t

Relativ la descifrarea unuĭ ast-fel de cryptogram se aplică sistema de metodă de descifrare a luĭ Iuliu Cesare.

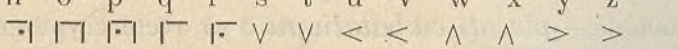
Alfabetul Franc-Mason

Franc-Masoniĭ au întrebuințat alfabetul următor:

a b c d e f g h i j k l m



n o p q r s t u v w x y z



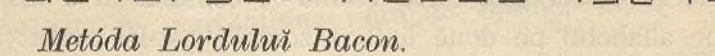
Acest alfabet s'a format din alăturatele două figurĭ, înlocuind fie-care literă prin figura formată de liniile ce o desparte de cele-l'alte.

a b	c d	e f
g h	i j	k l
m n	o p	q r

Să luăm și să cifrăm o depeșă dupe acéstă metodă.

Exemplu: Generalul plécă mâine.

Vom avea cryptogramul urmĕtor:



Metóda Lordului Bacon.

Lordul Bacon întrebuința un adevĕrat alfabet de convențiune, în care fie-care literă era represintată prin un aranjament cu repetiție de douĕ litere a și b luate câte 5 în 5.

a	a a a a a	g	b a a a b
b	a a a a b	h	b a a b a
c	a a a b a	i	b a b a a
d	a a b a a	j	b b a a a
e	a b a a a	l	b b a b a
f	b a a a a	m	b b b a a
n	b b b a b	t	a b b b b
o	b b b b a	u	a a b b b
p	b b b b b	r	a a a b b
q	b a a b a	x	b b a b b
r	b a b b a	y	a b a a b
s	b a b b b	z	a a b a b

Să luăm un exemplu pentru a'l cifra dupe acéstă metódă,—*plecați cu batalionu* o să avem cryptogramul următor:

b b b b b b b a b a a b a a a a a a b a a a a a a a b b b b b a b a a, a a a b a a a b b b, a a a a b a a a a a a b b b b a a a a a b b a b a b a b a a b b b b a b b b b a b a a b b b.

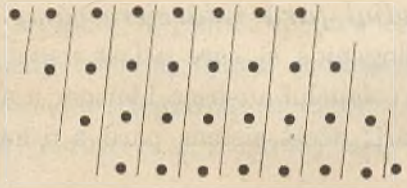
Metoda prin inversiune cea mai simplă este aceia care consistă în a scri cuvintele sau grupurile unui text clar, începând de la dreapta la stânga, ast-fel textul clar: *începeți atacul* vom avea cryptogramul *lucata ințepecni.*— Să luăm acum un text cifrat dupe metoda lui Iuliu Cesar.

Suposând că fie-care literă a fost înlocuită prin aceia care urmézá imediat în alfabet normalul. *Exemplu*: *ridică tabăra,*— o să avem cryptogram *sjejdb ubcbsb;* acum scriind acest cryptogram după metoda de inversiune care am enunțat-o, adică începând a scri de la drépta la stânga avem *bsbcbu, bdjejs* și scriindu-le într'un singur grup o să avem *bsbcbubdjejs.* Acéstă modificațiune care este fórte simplă la scrierea unui text cifrat póte ambarasa la prima vedere, dar nu-l ține mult timp pe un descifror orî cât de puțin ar fi exersat.

Metóda prin paralelograme. In acéstă metódă vom începe prin a conveni numĕrul de linii orizontale pe care vom dispune textul; în care să zicem că am fixat la 4,—și să presupunem a cifra textul următor.

Veniți imediatu în ajutoru astă-dĭ.

Acéstă depeșă coprinde 29 litere, împărțind 29 prin 4 adică liniile orizontale convenite o să avem $4 \times 8 = 32$; prin urmare ne dă un numĕr superior de treĭ mai mult, prin urmare, numĕrul colónelor verticale o să fie de 8 și o să avem douĕ litere nule de adăogat, și facem tabloul urmĕtor, care simplifică mult lucrul, și scade în același timp șansa erorilor.



Punem în acest tablou în locul punctelor literile depeșeĭ scrise de la stânga

la drépta, de manieră ordinară, începând cu prima linie horizontală.

f h sunt litere nule puse pentru complectarea tablouluĭ.

Luâm și scrim literile din fie-care colónă oblică, începând de la stânga tablouluĭ, și din stânga fie-căreĭ colóne, și vom avea cryptogramul următor:

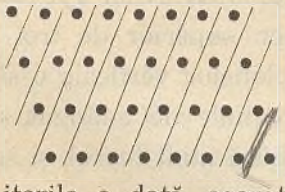
V-ee-adn-adii-sjat-tuti-atui-doim-irn-fu-h; acest cryptogram 'l putem scri într'o singură grupă sau 'l scrim în grupe diferite, avênd acelașĭ număr de litere, însă de regulă se scrie în grupe de atâtea litere câte colóne orizontale avem.

Fie, spre esemplu, a descifra cryptogramul urmĕtor:

pmlr-eeia-dcei-iarn-atet-tica-liar-amdp.

Acest cryptogram conține 32 litere, dupe regula care am admis'o, și admițênd că convențiunea n'a fost variată. — Vom începe prin a face tabloul urmĕtor: — No. I. Dupe acésta formăm un al II-lea tablou unde scrim cryptogramul întocmaĭ dupe cum am procedat la scriere.

No. I.



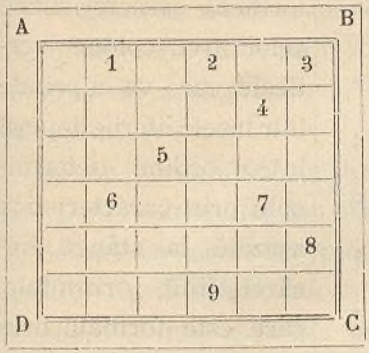
No. II.

Literile o dată așezate citim fără greutate depeșa urmĕtóre: *plecați imediat fără întârziere câmp.*

Un procedeu fórte ingenios și care a fost usitat secolul trecut, și la care colonelul austriac Fleisner a adus o mulțime de modificărĭ; acest sistem pare a fi indescifrabil.

Acest sistem constă dintr'o placă metodică potrivită, avênd 36 divisiuni, dintre carĭ nouĕ case numerotate sunt tăiate presentând pe placă golurĭ.

Să presupunem că voim a scri depeșa următóre: *Un atac va avea loc mâine diminéță la patru,*



formăm un patrat de aceeașĭ dimensiune cu placă unde se află cele nouĕ numere, dupe ce am format patratele de hârtie de aceiașĭ mărime cu placă scrim în locul patratelor góle care se presintă sub placă cele 9 litere d'întâiu ale fraseĭ dupe ordinea numerică; dupe aceia

a	u	i	n	v	a
n	e	a	a	t	t
l	e	a	a	d	o
l	ŭ	c	i	c	a
m	m	p	a	a	v
1	t	n	a	e	r

învârtim din nou placa de la drépta la stânga, ast-fel ca latura BC să ia locul laturiĭ AB, și scrim dupe aceia cele nouĕ numere care urméză, învârtim din nou placa în acelaș sens și continuăm operațiunea până vom scri tóte literile depeșeĭ.

Pentru maĭ multă înlesnire se scrie cu litere majuscule inițialele cuvintelor, și prin urmare vom avea cryptogramul următor: a u i n e v a n e a a t t e e a a d o l u c i c a n m p a a v i t n a e r.—Colonelul austriac Fleisner se exprimă în privința acestuĭ sistem că póte varia, la infinit, dar nu póte fi practic pentru campanie, din causă că necesită câte un aparat pentru fie-care serviciu.

Metóda telegrafieĭ aeriene. Acéstă metódă imaginată pentru a corespunde secret cu vechiul telegraf

chappe...., póte fi întrebuințată cu o combinațiune de 2, 3, 4, 5 în litere sau cifre.

Să luăm, spre exemplu, o combinațiune de treĭ litere A B și C. — Incepem prin a forma tabloul următor:

	A	B	C
C B A.....	r a n	o i e	p m e
B C A.....	s l i	n n s	e e t
B A C.....	e ș a	t a l	b a o
C A B.....	i u t	g l u	r t p
A C B.....	a s o	a o e	d t r

Cele treĭ litere A B C formézĕ caracteristicile celor treĭ colóne verticale care va coprinde într'însele literile depeșiĭ într'o ordine determinată prin caracteristica așezată la stânga fiecăreĭ liniĭ orizontale, care este formată prin permutațiunĭ succesive de treĭ litere A B și C. — Este bine înțeles că în loc de 3 litere, putem lua 3 cifre arabe.

Spre exemplu a cifra depeșa următóre:

Pornește brigada mâine la satul Stoenești la opt ore. — Maĭ întâiu formăm acéstă depeșă în grupe de câte treĭ litere. — Și avem por-neș-teb-rig-ada-mâĭ-nel-asa-tul-sto-ene-și-lao-ptu-ore. — Inscrim succesiv fiecare grupă, punênd fie-care din literile care 'l compun în colóna verticală indicată prin ordinea literilor de la caracteristica fie-căreĭ liniĭ orizontale. — Ast-fel în primul grup prima literă p va fi așezată în colóna verticală c., pentru că prima literă a caracteristic C B A din prima linie horizontală a tablouluĭ este C; pentru acelașĭ reson înscriem a doua literă o. a primuluĭ grup în colóna B și a treia literă în colóna A; — al II-lea grup se va scri în a doua linie orizontală prima literă n, se înscrie în colóna B, pentru că caracteristica

acesteĭ liniĭ este B C A, a doua literă e în colóna C și a treia în colóna A, — și urmăm tot ast-fel până terminăm tóte literile depeșeĭ și formăm cryptogramul urmĕtor: Cryptogram ran-oie-pme-sli-nns-eet-eșa-tal-vao iut-glu-rtp-aso-aoe-dtr.

Descifrarea unuĭ cryptogram în acest sistem se face de o manieră fórte simplă — întrebuințând procedeurĭ inverse de acelea care le am întrebuințat pentru cifra telegrama.

Să ne presupunem a descifra cryptogramul următor: sst-eii-ruo-sec-uai-rta-lop-eva-emĭ-ufa-nil-sut-tna-pv-ee.

Sciind că acest cryptogram a fost scris în combinațiunĭ de 3 litere, întrebuințate dupe cum am vĕḑut, începem și noĭ a forma tabloul urmĕtor:

	A	B	C
C B A.....	s s t	e i ĭ	r u o
B C A.....	s e c	u a i	r t a
B A C.....	l o p	e v a	e m i
C A B.....	u f a	n i l	s u t
A C B.....	t n a	p v.	e e.

După acésta înscriem succesiv tóte grupurile, începênd de la stânga și scriind câte treĭ grupurĭ în fie-care linie orizontală, extragem dupe aceia literile una câte una din fiecare linie orizontală, dupe ordinea indicată prin caracteristica fiecăreĭ liniĭ, începênd tot-d'a-una de la stânga fie-căruĭ grup. — Este bine, pentru a evita erorile, de a tăia fiecare literă pe mĕsura ce o scrim, — operând ast-fel vom obține:

res-urs-ele-sun-tep-uis-ate-vom-ufi-nev-oit-iac-api-tul-a,

adecă:

Resursele sunt epuisate vom fi nevoiți a capitula.

1) Metóda Colonelului Roche. Colonelul Roche, din artileria de marină francesă, a inventat un metod care oferă o mare analogie cu acela care l'am expus mai sus.—El ia de exemplu un text cifrat care are 38 litere, și împarte aceste litere într'un mod arbitrar în opt grupe și coprinḑênd fie-care grupă un număr arbitrar de litere—și obține ast-fel dispositiunea următóre:

3	5	7	2	4	6	8	3
• • •	• • • • •	• • • • • • •	• •	• • • •	• • • • • •	• • • • • • • •	• • •
I	II	III	IV	V	VI	VII	VIII

In acéstă figură cifrele romane ne arată numĕrul de ordine al compartimentelor, cifrele arabe indică numĕrul de litere ce trebue să conțină fie-care compartiment, punctele represintă literile textului clar.

Vom începe a pune în fie care compartiment cele d'ântâiŭ opt litere ale depeșeĭ, urmând ordinea naturală, de la stânga la drépta, sau o ordine arbitrară convenită mai înainte. Să suposăm că am urmat ordinea naturală, și că cele d'ântâiŭ opt litere le-am așezat la drépta fie-căruĭ compartiment, cele 7 litere care urméză, le așezăm începênd de la casa II la stânga fie-căruĭ compartiment, de la a 15-a literă exclusiv așezăm literile la stânga literilor sau grupurilor deja înscrise, luând drumul de la stânga la drépta și urmăm ast-fel alternativ, până așezăm cele 38 litere ale depeșeĭ — dacă într'o casă s'a complectat numĕrul literilor trecem imediat la cea urmĕtóre.

De la casa a opta când începem de la drépta la stânga, când am ajuns la I-iŭ începe invers de le așezăm la drépta numĕruluĭ aflat la stânga, operând de maniera acésta vom obține tabloul arĕtat mai jos, în

care cifrele arabe ne arată locul ce trebue să 'l ocupe cele 38 litere.

32, 22, 1	9,23,31,21,2	10,24,32,36,30,20,3	11, 4	12,25,19,5	13,26,33,29,18,6	14,27,38,37,34,28,17,7	15, 16, 8
I	II	III	IV	V	VI	VII	VIII

Dacă numĕrul literilor din depeșă nu este 38 sau un multiplu al luĭ 38, atuncĭ adăogăm litere fără valóre. Să facem un exemplu de 38 litere; fie depeșa următóre: *mâine plécă douĕ batalióne în avantposturĭ.* Conform regulelor stabilite și a tablouluĭ arĕtat formăm cryptogramul în mod următor:

p o m	a, n, t i a	c, e, o, r, n, l i	a n	d i a e	o n s, a t p	u, a, t i u v a l	a b e
I	II	III	IV	V	VI	VII	VIII

Cryptogramul fi=p o m a n t i a c e o r u l i a n d i a e o n s a t p u a t i ŭ v a l a b e, dacă avem o depeșă compusă numaĭ dc 22 litere atuncĭ usăm numaĭ de cele d'ântâiu 5 case.

2) *Metoda a Colonelului Roche.* Fie spre exemplu a cifra un text de 80 litere, vom dispune textul pe 8 linĭĭ orizontale și 10 colóne verticale, vom lua drept cheiă un cuvênt de 8 litere, sau primele 8 litere, sau 8 litere ale unuĭ cuvênt, sau a uneĭ frase óre-care, fie *magister* cuvêntul luat drept cheiă, acest cuvênt transformat în serie numerică dupe metóda espusă maĭ sus ne dă:

m	a	g	i	s	t	e	r
5	1	3	4	7	8	2	6

dedesuptul serĭĭ numerice ast-fel obținute, scriem cifrele de la 1 la 8, representând numĕrul de ordine

al celor d'ântâiu 8 litere ale textuluï cifrat vom începe de la stânga, și vom forma ast-fel tabloul următor:

A

5	1	3	4	7	8	2	6	Cheia transformată în serie numerică.
1	2	3	4	5	6	7	8	Numĕrul de ordine a celor d'ântâiu 8 litere ale textuluï de cifrat.

Dupe acest tablou prima literă a textuluï clar așezată sub prima cifră a cheieï (5), va fi înscrisă în a 5-a linie orizontală a tablouluï B, și rîndul care 'l va ocupa în acéstă linie va fi determinată prin cifra (1), care în cheia transformată vine imediat dupe cifra 5 care determină linia; a II-a literă a textuluï va fi înscrisă în prima linie orizontală, pentru că ea este așezată sub cifra 1 a cheieï transformată, și în al 3-lea rang al acesteï liniï, pentru că cifra 3 urméză imediat cifra 1 în cheiă; asemenea a III-a va fi pusă în a treia linie și în al 4-lea rang și urmăm ast-fel până la a opta literă care va fi așezată în a 6-a linie orizontală și în al 5-lea rang arĕtat prin cifra 1 a cheieï transformată; tot d'odată a 5-a literă a textuluï clar care, dupe regulă, trebue așezată în al 8-lea rang din a 7-a linie orizontală, va fi înscrisă în cea din urmă casă a aceleï liniï, operând ast-fel vom obține tabloul următor:

	I	II	III	IV	V	VI	VII	VIII	IX	X
I			2							
II						7				
III				3						
IV							4			
V	1									
VI					8					
VII										5
VIII		6								

După ce am transpus cele d'ântâiu 8 litere ale textului de cifrat le așezăm și pe cele-l-alte de maniera următóre:

Punem a 9-a literă în prima linie la drépta dacă este posibil, în cas contrariu înscriem acéstă literă în a II-a colónă verticală, mergênd ast-fel succesiv de la prima linie orizontală până la a 8-a înscriind succesiv, și pe cât este posibil o literă la drépta celeì-l'alte; dupe acésta revenim la I-a linie orizontală și operăm ca maì sus, însă înscriem noile litere la stânga celor precedente, dupe ce am ajuns iar până la a 8-a, revenim iar la întâia linie, scriind literile la drépta celor aflate până la a 8-a și urmând tot ast-fel succesiv până complectăm cu așezatul literilor aflate în text.— Modul de a așeza literile când la drépta când la stânga contribue a face maï dificil cryptogramul, se pune litere fără valóre când nu s'a complectat tabloul.—Aplicând principiele expuse

maĭ sus la un text clar de 80 litere cu cheia magister 51347826 vom avea tabloul următor unde literile sunt înlocuite prin numere de ordine.

	I	II	III	IV	V	VI	VII	VIII	IX	X
I	30	16	2	9	23	36	48	58	66	72
II	63	54	43	31	17	7	10	24	37	49
III	44	32	18	3	11	25	38	50	59	67
IV	70	64	55	45	33	19	4	12	26	39
V	1	13	27	40	51	60	68	73	76	79
VI	56	46	34	20	8	14	28	41	52	61
VII	80	78	75	71	65	57	47	35	21	5
VIII	22	6	15	29	42	53	62	69	74	77

Acest procedeu are singurul desavantagiu că necesită un timp prea lung atât pentru a cifra o telegramă cât și pentru a o descifra; pentru a cifra o telegramă dupe acest sistem n'avem de cât literile din telegramă să le numerotăm de la 1 până la 80,—și să le așezăm într'un tablou de felul acesta și pe urmă să le scrim la rând și cu modul acesta formăm cryptogramul, — pentru a descifra operăm în sens invers, adică când am primit cryptogramul, scrim literile care 'l compun la rând în tablou și dupe aceia le luăm și le scrim începând de la No. 1 până la 80, și ne va da sensul telegrameĭ.

II. Metoda prin interversiune.

In sistemele care se aplică metodele prin interversiune trebue să distingem:

I) Metódă cu basa invariabilă, în care literile alfabetuluĭ din acelașĭ cryptogram nu sunt schimbate, adică sunt representate prin aceleașĭ caractere, sau prin aceleașĭ semne, și:

II) Sistemul cu basă variabilă unde schimbăm alfabetul la fie-care cuvênt, sau la fie-care literă.— Primul sistem se numește cu *cheiă simplă* și al II-lea sistem se numesce cu *dublă cheiă*.—Sistemul cu simplă cheiă nu presintă nicĭ o siguranță, cele cu duble cheĭ forméză în adevĕr combinațiunĭ maĭ mult sau maĭ puțin indescifrabile.

I. Sistemul cu simplă cheiă.

Din punctul de vedere al formeĭ, sistemele cu simplă cheiă pot varia la infinit, dupe cum am vĕḑut maĭ sus, și putem nu numaĭ a combina alfabetul normal de un numĕr óre-care de numere diferite, dar putem încă a înlocui caracterele alfabetice prin cifre arabe, prin semne algebrice, astronomice, sau chiar prin grupe de alte litere, dupe cum am vĕḑut la metoda lorduluĭ Bacon. — Și tóte aceste combinațiunĭ nu dau loc de cât la un singur sistem, și la acelașĭ procedeu de descifrare; sistemul cel maĭ simplu și cel maĭ practic este acela care consistă în a schimba valórea literilor alfabetuluĭ dupe o cheiă convenită. — Noĭ am vĕḑut maĭ sus cum se schimbă un cuvênt în cheiă, prin urmare să maĭ facem un exemplu:

Spre exemplu să luăm cuvêntul *Cavalerie*, o să avem:

C a v a l e r i e
2 4 1 6 8 5 3 7 9

și dacă ordonăm alfabetul cryptographic dupe acest numĕr obținem:

2 4 1 6 8 5 3 7 9
b d a f h e c g i
k m j o q n l p r
t v s x z w u y

Prin urmare în locul alfabetuluĭ normal după acéstă cheiă o să avem alfabetul urmĕtor:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
b d a f h e c g i k m j o q n l p r t v s x z w u y

Să luăm un exemplu și să facem un cryptogram dupe alfabetul acesta.

Exemplu: *întăreștete în posiție* — se va scri: i q v b r h t v h v h iq l n t i v i h.—Acest sistem este fórte vechiu, aprópe de douĕ miĭ de anĭ.

Biblioteca națională din Paris posedă douĕ volume de scrisorĭ cifrate găsite la Offenbourg de Morau, în furgónele generaluluĭ austriac Klinglin, însărcinat cu serviciul corespondenței secrete; aceste scrisorĭ carĭ erau fórte compromițătóre pentru partida regalistă de atuncĭ; fie-care caracter al textuluĭ clar era figurat printr'un numĕr fix format din douĕ cifre arabe și separațiunea cuvintelor era indicată printr'un *(0)* zero.

Dupe cum susțin unĭĭ este fórte adĕvĕrat că generalul Klinglin era maĭ tare în tactica militară de cât în cryptographie, căcĭ ignora principiul cel maĭ elementar din

cryptographic, căci dênsul a crędut suficient a tăia arbitrar óre-care cuvinte, pentru a da în schimb descifroruluĭ cel maĭ mare avantagiu de descifrare. —

Iată prima frasă din una din aceste scrisorĭ, care datézĕ de la 31 Decembrie 1795.

899952420 44520 45566253652112 50 și ce n'est la 3152891499 14 254452 44520 2311094259467524 594995645 44118934 5294 445234114544520.

Deslegare

89 99 52 45 0 44 52 0 45 56 25 36 52 11 25 0
r i e n d e n o u v e a u
și ce n'est la 31 52 89 14 99 14 25 44 52 44 52 0
. . . . . c e r t i t u d e d e
23 11 0 94 25 94 67 52 45 94 99 56 45 44 11
l a s u s p e n s i o n d a
89 34 52 94 44 52 34 11 45 44 52 0.
r m e s d e m a n d e

prin urmare are înțelesul urmĕtor:

Rien de nouveau si ce n'est la certitude de la suspension d'armes demandée.

Nu putem numĕra aci tóte sistemele cu cheia simplă care sunt fórte numeróse, dupe cum am vędut deja parte dintr'însele, însă autorii ceĭ maĭ principalĭ în aceste sisteme sunt:

Blaise, de *Vigenère*, *Bacon*, *Herman* și *Mirabeau*, dar aceste invențiunĭ nu pot avea pentru noĭ de cât un interes maĭ mult arhiologic, pentru că nu sunt practice, și afară de acésta maĭ tóte se póte descifra.

Descifrarea sistemului cu cheia simplă.

Orĭ-care ar fi sistemul adoptat, fie cu basa variabilă sau invariabilă, pentru a descifra un cryptogram, nedispunând de cheiă, va trebui să întrebuinţăm două operaţiunĭ bine distincte:

I) Un calcul de probabilitate şi al II). O lucrare de tatonament; — calculul de probabilitate se basează pe o proprietate comună tutulor limbelor, adică a şti în fiecare limbă literile carĭ se repetă maĭ mult. — Ast-fel în limba română avem să găsim pe e că se repetă de maĭ multe orĭ, dupe aceia pe *a* şi în urmă pe *s*.—In limba Francesă, Germană şi Englesă litera *e* este iar frecuentă, în limba Spaniolă găsim pe *o* în cea Rusă pe *a*, iar în limba Italiană pe *e* şi *i*.

Generalul Lewal zice în uvragiul sĕu *Etudes de guerres* că o depeşă cu simplă cheiă garantéză îndestul secretul pentru trebuinţele ordinare şi pentru afacerile fără importanţă mare.

Cu tóte acestea depeşile cu simplă cheiă nu presintă garanţie de cât în urmĕtórele treĭ condiţiunĭ:

I) Separaţiunea cuvintelor să nu fie indicată în textul depeşeĭ.

II) Literile duble să fie suprimate şi:

III) Să nu se întrebuinţeze nicĭ litere marĭ la începutul cuvintelor, sau dupe punct, nicĭ semne de accentuaţie sau de punctuaţie; pentru a evita erorile de transcriere este chiar indispensabil de a fracţiona cryptogramele în grupe de patru sau cincĭ cifre.

Sistemele cu dublă cheiă.

La definiţiune am dis că literile cu dublă cheiă sunt acelea carĭ schimbă alfabetul la fie-care literă. O mul-

time de combinațiuni cu basa variabilă au fost imaginate, dar nu sunt de cât trei sau patru, cari se pot întrebuința în practică.

Aceste sisteme diferă între dênsele prin formă, dar în fond sunt identice și se asémănă cu sistemele expuse la finele secoluluĭ al XVI adică *Blaise* și de *Vigenère.*

In timp de trei secole aceste sisteme au servit de cifre secrete la cea mai mare parte din curțile germane și italiane; astă-dĭ ele trec încă de indescifrabile în ochiĭ persónelor carĭ nu sunt în curent cu procedeurile de descifrare.

Fiind-că tóte metodele de scriere cryptographică destinate la trebuințele armateĭ, trebuesc a fi aplicate la telegrafie, noĭ nu ne vom ocupa de cât de sistemele carĭ sunt basate pe întrebuințarea literilor sau cifrelor arabe, sau în genere de tóte sistemele carĭ vor fi combinate cu cifre și litere.

Sistemul luĭ Porta.

Invențiunea primuluĭ sistem în dublă cheiă ia naștere de la fisicianul *Porta.*—Cu tóte că a fost departe de a cunóște importanța introducereĭ uneĭ cheĭ propriu dise în metóda scrierilor cifrate, dar cu tóte acestea 'l putem considera ca fundatorul cryptographieĭ.

Porta întrebuință un-spre-zece alfabete diferite, pe care le însemna dupe cum se vede în figura de maĭ jos.—Adică alfabetul AB—CD ect.

Dacă voim a scri cu vre unul din aceste alfabete enumĕrate în tablou spre ex. cu CD,—vom representa pe a cu z și vice-versa pe z cu a, pe b cu n și n cu b și așa maĭ departe; dar pentru a îngreuia calculul

investigatarilor, Porta — om care știa a descifra un cryptogram,—recomandă de a scri fie-care literă cu un alfabet deosebit; ceva mai mult: pentru a nu obliga pe corespondenți a lua un-spre-zece alfabete, pe rând, ceea-ce ar înlesni de sigur trădarea secretului, el propune de a nu întrebuința de cât 5 sau 6 alfabete de a alege și a forma un cuvênt și acest cuvênt va forma cheia cryptogramului. — Iată un exemplu cu cheia. — *rege*.

Tabloul lui Porta.

A	B	a n	b o	c p	d q	e r	f s	g t	h v	i x	l y	m z
C	D	a z	b n	c o	d p	e q	f r	g s	h t	i v	l x	m y
E	F	a y	b z	c n	d o	e p	f q	g r	h s	i t	l v	m y
G	H	a x	b y	c z	d n	e o	f p	g q	h r	i s	l t	m v
I	L	a v	b x	c y	d z	e n	f o	g p	h q	i r	l s	m t
M	N	a t	b v	c x	d y	e z	f n	g o	h p	i q	l r	m s
O	P	a s	b t	c v	d x	e y	f z	g n	h o	i p	l q	m r
Q	R	a r	b s	c t	d v	e x	f y	g z	h n	i o	l p	m q
S	T	a q	b r	c s	d t	e v	f x	g y	h z	i n	l o	m p
V	X	a p	b q	c r	d s	e t	f v	g x	h y	i z	l n	m o
Y	Z	a o	b p	c q	d r	e s	f t	g v	h x	i y	l z	m n

Exemplu: *Depeșa trimésă s'a descifrat.* Împărțim și noi cuvêntul în grupe de câte 4, dupe cheia *Rege* și căutăm la fie-care literă a depeșei ce literă corespunde în cheiă și căutăm în tabloul lui Porta la alfabetul din literă liberă corespundétóre și avem:

d e p e	ș a t r	i m e a	s ă s a	d e s c	i f r a	t u
R e g e	R e g e	R e g e	R e g e	R e g e	R e g e	R e
V p f p	b y l g	o y o y	b y i y	v p i n	o q h y	c u

și prin urmare o să avem cryptogramul urmétor:

= v p f p b y l g o y o y b y i y v p i n o q h y c u.

Invențiunea lui Porta a adus o nouă eră în istoria cryptographiei, dar presantă două mari inconveniente

carĭ aŭ și făcut să fie părăsită de mult timp.—Pentru a descifra un cryptogram dupe sistemul luĭ Porta n'avem de cât să 'l împărțim în grupe de atâtea litere câte coprinde cheia, și pe urmă să căutăm fie care literă în alfabetul care corespunde la literă și vom parveni cu modul acesta a afla înțelesul cryptogramuluĭ.

Metoda luĭ de Vigenère.

Metoda luĭ de Vigenère, zisă a cifrelor pătrate, sau a cifrelor nedescifrabile, sau a cifrelor prin excelență, nu este alt ceva de cât sistemul luĭ Porta simplificat, care l'a dispus ast-fel, că este și astă-dĭ în usagiŭ;—acéstă metodă a fost întrebuințată în cancelariele diplomatice în al XVIII-lea secol și s'a servit cu dênsa chiar în ministerul de resbel frances dupe campania de la 1870.

Dlandol, un cetățean frances, a pus la cunoștința publiculuĭ în epoca revoluțiunĭĭ, că cifrele patrate ale luĭ de Vigenère, sunt cele maĭ bune, pentru că reunește un mare numĕr de avantage pentru acela care face o corespondență secretă dupe acest sistem. Dlandol adaogă că universul întreg nu póte să descifreze un cryptogram dacă nu cunóște cheia convenită între corespondenți, și că póte să se arate scrisórea la tótă lumea fără ca să pótă cineva să parvie a o descifra.

De sigur se exprimă Kerchoffs, cetățeanul Dlandol era maĭ bun patriot de cât îndemânatic descifror, căcĭ în ḑiua de astă-dĭ s'a parvenit prin calcule de probabilitate și prin tatonamente a deslega depeșile cele maĭ complicate.

Dispositiunea tablouluĭ luĭ Vigenère diferă de aceia a tablouluĭ luĭ Porta prin aceia că alfabetul este pus

în număr patrat și că prin urmare obținem un număr de alfabete egal cu numărul literilor. — Când maniăm acest tablou procedăm întocmaĭ ca și la tabloul luĭ Porta; trebue a remarca că alfabetul orizontal superior nu este de cât alfabetul normal și că cele 26 care urméză sunt alfabete cryptographice.

Tabloul luĭ Vigenère.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	z

Să luăm un exemplu și să facem un cryptogram dupe acest sistem.

Exemplu: *Distruge de urgență podu.*

Și să luăm drept cheiă cuvêntul cal. — Impărțim și

noĭ exemplul nostru în atâtea grupurĭ de câte treĭ litere câte va coprinde, și o să avem:

d i s	t r u	g e d	e u r	g e n	ț ă p	o d u
CAL	CAL	CAL	CAL	CAL	CAL	CAL
f i d	v ă f	i e o	g u c	i e y	v a a	q d f

O să avem cryptogramul următor: f i d v r f i e o g u c i e y v a a q d f.

Pentru a descifra un cryptogram făcut dupe acest sistem, n'avem de cât să împărțim literile cryptogramuluĭ în câte o grupă de litere de câte orĭ se va coprinde cheia în depeșă și să urmăm în sens invers de cum a cifrat.

Metoda căpitanuluĭ Delauney.

Căpitanul Delauney a imaginat de a utilisa un joc de tachinărie cu aparat de cryptographie. A luat un patrat care conține 16 cuburĭ de lemn și care póte fi înlocuite prin 16 patrate de hârtie sau de carton. = Se ia un cuvênt sau o expresie de 16 cuvinte care să servească ca cheiă.

I

j	u	d	e
c	u	l	m
e	h	l_2	d_1
i	n	t	i_1

j m t p	u a u t	d i l e	l u p o
c c o r	u p p e	l e o	m e v
l_1 i e	h a n	l_2 t i	d_1 i e
i l a	n a s	ț s e	i n a

Spre exemplu luăm drept cheiă expresia următóre: *Județul Mehedinți;* scriem fie-care din literile acesteĭ

cheĭ în câte un cub, avênd grijă a pune câte un indice la literile care se repetă, și obținem dispositiunea prevĕdută în tabloul I.

Dupe acésta scriem depeșa în cuburile patratelor într'un mod regulat; să luăm exemplul urmĕtor:

Mâine plecați la satul Popoveni la șeapte ore.— Dupe ce am scris depeșa în cuburĭ la rând, scótem cuburile și le așezăm dupe voe, într'un mod arbitrar cuburile, și 'l trimetem la corespondent. — Acesta primind cuburile, și cunoscând cheia, n'are de cât să le așeze și pe urmă să citéscă depeșa fără nicĭ o greutate.—Acest procedeu n'are nicĭ o siguranță; va fi în tot momentul posibil ca inamicul, prin un numĕr fórte restrâns de tatonamente, să pótă restabili cuburile în ordinea convenită, căcĭ póte să se orienteze nu numaĭ dupe literile cheeĭ dar și dupe literile depeșeĭ.—In acest procedeu numĕrul tatonamentelor este representat prin numĕrul aranjamentelor de 16 objecte luate câte 4 în 4: acest numĕr póte să fie redus când ținem cont și de particularitatea limbeĭ în care este scrisă depeșa.

Căpitanul Delauney, pentru a crește dificultățile, a propus întrebuințarea unuĭ patrat care să aibe 25 la 36 cuburĭ.

Sistemul de la Saint-Cyr.

Acest sistem care este un usagiŭ de mult timp, nu este alt-ceva de cât forma deghisată a tablouluĭ luĭ Vigenère, și care pórtă numele scóleĭ unde se predă și se preconisează. Iată tótă descripțiunea acestuĭ sistem.

El este predat în cursul de cărți militare și a fost autografiat pentru eleviĭ din prima divisiune, și se

compune dintr'un alfabet fix, sub care alunecă un dublu alfabet mobil, două bande de hârtie quadrilată este suficientă.

Se ia un cuvênt óre-care de trei saŭ cinci litere care să formeze cheia, fie s. e. cheea B A C, și să formăm cryptogramul din depeșa următóre: *dați foc satuluĭ și plecați*,—împărțim și noĭ depeșa în grupe de câte treĭ dupĕ cheiă, cheea avênd treĭ litere, pentru a cifra prima literă a depeșeĭ, așezăm litera B a alfabetuluĭ mobil sub litera A a alfabetuluĭ fix și luăm prima literă d în alfabetul fix și căutăm cu ce conrespunde în alfabetul mobil și găsim că litera D conrespunde cu e, litera a o să conrespundă tot cu a, litera t o găsim făcând să alunece rigla saŭ maĭ bine dis alfabetul mobil până când C vine sub A și căutăm pe t care conrespunde cu v, și așa maĭ departe până terminăm tóte grupurile.

d a ț	ı f o	c u l	s a t	u l u	ı ș i	p l e	c a ț	ı
B A C	B A C	B A C	B A C	B A C	B A C	B A C	B A C	B
e a v	f f q	d u n	t a v	v l w	j s k	q l g	d a v	j

și avem cryptogramul următor:

e a v j f q d u n t a v v l w j s k q l g d a v j

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	alfabet fix
a b c d e f g h i j k l m n o p q r s t u v w x y z a b c etc.	alfabet mobil

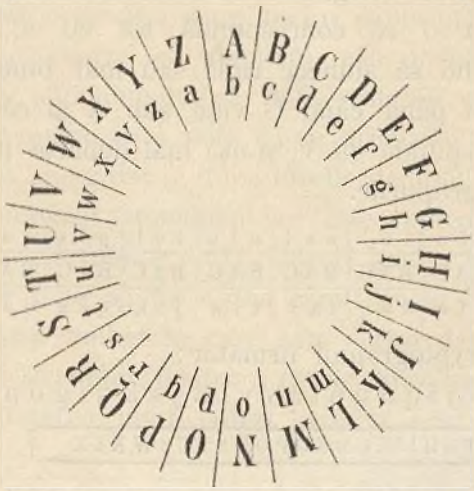
Acest sistem are desavantagiul de a-se deslega fórte ușor, un descifror îndemânatic care ar pune mâna pe o depeșă fără să aibe cheia, nu-ĭ trebue maĭ mult de cât $^1/_2$ oră pentru e descifra cryptogramul.

Are însă avantagiul că perdênd instrumentul în timpul cel maĭ scurt se póte face altul în loc. O casă din Berlin a fabricat un instrument mecanic pentru a cryptographia cu acest sistem.

Sistemul de Saint-Cyr

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z a b c d e etc.
a b c d e f g h i j k l m n o p q r s t u v w x y z a b c d e f etc.
a b c d e f g h i j k l m n o p q r s t u v w x y z a b c d e f g etc.

Se specifică în cursul de artă militară că se va putea stabili instrumentul în condițiuni ast-fel ca să-l facă mai portativ; formându l din două cercuri concentrice din care unul să fie mobil, învârtindu-se împrejurul axului său. — Acéstă dispositiune care este representată în figura alăturată a fost imaginată în anul 1563



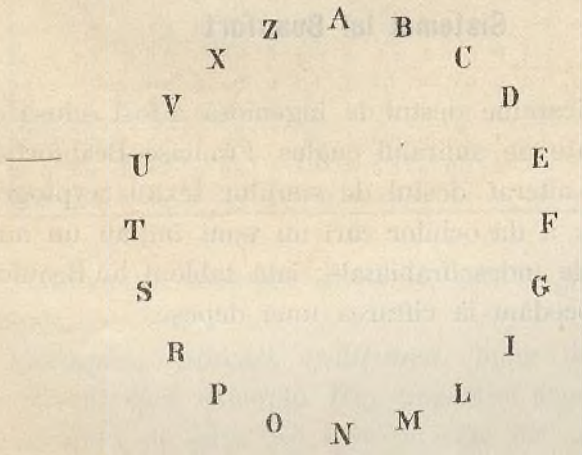
de Porta și a primit de atunci o mulțime de aplicațiuni; ast-fel este cryptographul Weastone și cutia cu cadran mobil ce s'a vĕdut în epoca resbelului Italiei.

Tóte aceste aparate sunt representate în uvragele recente de telegrafie ca niște invențiuni nouĭ, și nu sunt alt-ceva de cât simple tablourile luĭ de Viginère.

Metoda diferenţelor

Acesta este un sistem tot cu cheiă variabilă, dar care pare a fi fórte greu de descifrat pentru un descifror care nu posedă cheia. — Se scrie alfabetul normal, suprimând pe q şi k care se póte înlocui prin c şi suprimând asemenea pe j, y şi h, care se va înlocui prin i, vom forma un alfabet care nu va avea de cât 20 litere, şi dacă dispunem un cerc, saŭ într'un lanţ fără sfârşit aceste litere, distanţa care le va separa douĕ litere nu va fi maĭ mare de 10.

Luăm dupe acésta un cuvênt ca cheiă pentru a cifra depeşa dupe acest sistem, fie *Buzeu*, cuvêntul luat drept cheiă şi voim a cifra frasa următóre: *trimeteţi douĕ batalióne la Piatra*, scriem sub acéstă depeşă



de atâtea orĭ cheia de câte orĭ o va coprinde şi avem:

t	r	i	m	e	t	e	ţ	i	d	o	u	a	b	a	t	a	l	j	o	n	e	l	a	P	i	a	t	r	a
B	u	z	e	u	B	u	z	e	u	B	u	z	e	u	B	u	z	e	u	B	u	z	e	u	B	u	z	e	u
6	3	8	5	8	6	8	4	3	7	9	10	1	3	4	6	4	9	3	5	9	8	9	4	4	6	4	4	9	4

Este destul a usa de cele 10 numere 0, 1, 2, 3, 4, 5, 6, 7, 8 și 9 pentru a cifra cryptogramul—și operăm în modul următor: dedesubtul literei t se află B, numĕrăm de la B la T pe drumul cel mai scurt și vedem câte numere îl desparte și vedem că sunt 6; scriem pe 6 subt B. Trecem la a II-a literă r care conrespunde cu u din cheiă, numĕrăm și noi de la u la r și vedem că îl desparte No. 3, scriem pe 3; trecem acum la a treia literă din depeșă care este i și conrespunde litera z din depeșă de la z la i este 8 scriem pe 8 subt z, și urmăm tot ast-fel până când complectăm cryptogramul și avem depeșa cifrată = 6385868437910134649359894464494; a descifra un ast-fel de cryptogram este fórte lesne când avem cheea, și contrariu este fórte greu de descifrat pentru unul care n'are cheea.

Sistemul luĭ Beaufort

O modificațiune destul de ingeniósă a fost adusă cifrelor patrate de amiralul engles Francisc Beaufort în 1857, el a alterat destul de simțitor textul cryptographic pentru a da ochilor carĭ nu sunt inițiați un adevĕrat aer de indescifrabilitate; iată tabloul luĭ Beaufort și cum procedăm la cifrarea uneĭ depeșe.

Tabloul luĭ Beaufort.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a

Să luăm un exemplu și să 'l cifrăm dupe acéstă metodă.

Exemplu: atacați înălțimea, luăm drept cheiă un cuvênt, spre exemplu *Bic*, împărțim depeșa în atâtea grupurĭ de câte treĭ litre de câte orĭ se coprinde cheia.

a t a	c a ț	ĭ i n	ă l ț	i m e	a
B I C	B I C	B I C	B I C	B I C	B
b p c	z i j	t a p	b x j	t w y	b

Iată cum începem: luăm litera *a* a depeșii, o căutăm în întâiul alfabet orizontal, și ne coborîm în jos până dăm de litera *b*, dupe aceia ne ducem pe linia orizontală a luĭ b, până la capătul tablouluĭ și acolo găsim litera b care este semnul cryptographic și pe care 'l scrim sub B în grupa I; dupe aceia luăm litera t din depeșĭ din I-iul grup și o căutăm în întâiul alfabet și ne coborîm în jos până dăm peste litera i din cheiă, dupe aceia ne ducem sau la drépta sau la stânga pe linia orizontală unde am găsit pe i și la capătul tablouluĭ dăm peste p, pe care 'l scrim supt i, dupe aceia luăm a III-a literă a, și ne coborîm în jos până dăm peste C, ne ducem pe linia luĭ c la drépta până la capătul tablouluĭ și dăm peste c, pe care 'l scrim și urmăm tot ast-fel cu cele-l-alte grupe până terminăm cryptogramul — și o să avem depeșa cifrată în modul următor = b p c z i j t a p b x j t w y b.

Descifrorii englezĭ pe carĭ sistemul luĭ Beaufort i-a încântat atât de mult, nu se gândea nicĭ de cum că acelașĭ resultat 'l putea obține și cu sistemele luĭ Viginère și Saint-Cyr, resturnând într'un mod simplu alfabetul normal.—Este probabil că Amiralul Englez n'a crezut nicĭ o dată posibilitatea de a transforma sistemul sĕu în cifre patrate ordinare.—Și chiar Moris Beaufort fiul Amiraluluĭ, reclamă și astă-dĭ într'un mod energic că ilustrul sĕu părinte a dotat țara sea cu un sistem de cryptographie nedescifrabilă.

Sistemul luĭ Gronsfeld.

Acest sistem nu diferă de cele douĕ precedente de cât prin acela că lucrarea póte fi făcută din cap, în

loc de a necesita concursul unuĭ tablou sau a unuĭ aparat óre-care.

Iată cum inspectorul liniilor telegrafice din Franța Bontemps se exprimă relativ la acest subiect.

Să presupunem că am ales pentru cheiă un numĕr óre-care, pe care 'l scrim sub frasa pe care voim a o transmite, de atâtea orĭ, de câte orĭ se va coprinde și stabilind corespondența între litere și cifrele succesive, se ia drept literă de trămis, aceia care este așezată în alfabet, la o distanță exact egală cifreĭ pusă de desupt și formând ast-fel un sistem secret, de care putem zice că este imposibil de a descoperi cheia. — Sistemul comiteluĭ de Gronsfeld nu este de cât o formă deghisată a tablouluĭ luĭ Viginère. Să luăm un exemplu:

Atacați flancul stâng cu două batalióne, luăm drept cheiă un numĕr óre-care, spre ex. 503, avem:

a	t	a	c	a	t	i	f	l	a	n	c	u	l	s	t	a	n	g	u	c	u	d	o	u	ă	b	a	t	a	l	i	ó	n	e
5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3	5	0	3
f	t	d	h	a	z	n	f	o	f	n	f	y	l	v	x	a	q	l	u	f	y	d	r	y	a	e	f	t	d	q	i	r	s	l

luăm prima literă a și a 5-a literă dupe a numĕrând avem b c d e f, prin urmare f este semnul cryptographic pe care 'l scrim subt 5, luăm pe t care are *o* dedesupt punem iar pe t luăm a treia literă a din întâiul grup și supt dênsul se află 3, avansăm pe a cu 3 litere și dăm peste d care 'l scrim supt 3 și urmăm tot astfel până terminăm, și o să avem, dupe sistemul luĭ Gronsfeld, următorul cryptogram = f t d h a z n f o f n f y l v x a q l u f y d r y a e f t d q i r s e.

Metóda Auvray.

In 1870 Auvray, comis principal de clasa I-a la ministerul de marină și al colonielor, a imaginat metóda urmĕtóre: el numerotă douĕ alfabete coprinḑênd fie-care 36 semne, adică 36 litere ale alfabetuluĭ și 10 semne de numerotaţiune, primele servind pentru literile textuluĭ clar este numerotate de la 1 la 36,—al II-lea servind pentru literile cuvêntuluĭ cheiă și este numerotat ca și cel d'ântâiŭ, dar cu o creștere ușóră de ţinut minte din memorie.

Să suposăm că am ales 100, pentru creștere, cele douĕ alfabete vor fi atunci:

I-a

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

t	u	v	w	x	y	z	I	II	III	IV	V	VI	VII	VIII	IX	X
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

II-a

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120

u	v	w	x	y	z	I	II	III	IV	V	VI	VII	VIII	IX	X
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136

Să luăm și să cifrăm un exemplu ca să vedem cum operăm cu acéstă metodă. — Luăm drept cheiă o expresie spre exemplu: *nimic fără Dumnedeu* și să luăm frasa următóre cu telegramă, *ridică tabăra și pornește Craiova;* prin urmare vom face tabloul următor:

n	i	m	i	c	f	ă	r	ă	d	u	m	n	e	d	e	u	n	i	m	i	c	f	ă	r	ă	d	u	m	n	I-a
114	109	113	109	103	106	101	118	101	104	121	113	114	105	104	105	121	114	109	113	109	103	106	101	118	101	104	121	113		II-a
r	i	d	i	c	a	t	a	b	a	r	a	s	i	p	o	r	n	e	s	t	e	c	r	a	i	o	v	a		III-a
18	9	4	9	3	1	20	1	2	1	18	1	19	9	16	15	18	14	5	19	20	5	3	18	1	9	15	22	1		IV-a
96	100	109	100	100	105	81	117	99	103	103	112	95	96	88	90	103	100	104	94	89	98	103	83	117	92	89	99	112		V-a

Textul cifrat al depeșeĭ de maĭ sus va fi = 96-100-109-100-100-105-81-117-99-103-103-112-95-96-88-90-103-100-104-94-89-98-103-83-117-92-89-99-112.

Am operat în modul urmĕtor:

I. In rubrica I-a am scris literile cheeĭ nóstre.

II. In rubrica II-a am pus valórea literilor din cheiă dupe alfabetul No. II.

III. In rubrica III-a am scris literile depeşeĭ care voim a cifra.

IV. In rubrica IV-a am pus valórea literilor depeşeĭ din alfabetul No. I.

V. In rubrica V-a am pus diferența numerilor din rubrica 4 şi a II-a,—Şi acéstă diferență este text cifrat. —Pentru a descifra un cryptogram scris în acest sistem, n'avem de cât pe o rubrică să punem cuvintele cheiĭ, sub literile cheiĭ să punem valórea lor din alfabetul No. II, pe a III-a rubrică să punem semnele cryptogramuluĭ primit, şi printr'o simplă sustracțiune ne va da numere care le găsim valórea în alfabetul No. I.

Sistem cu cheia variabilă.

Vom vedea maĭ departe că descifrarea sistemelor cu dublă cheiă, este basată pe cunóşterea numĕruluĭ de litere care compune cheia.

S'a imaginat diverse combinărĭ pentru a împedica pe descifratorĭ de a maĭ face calcule; unul din sistemele cele maĭ bune, este acela imaginat de un membru din comisia de telegrafie militară din Franța; el propune de a se opri la intervale neregulate ordinea succesiuniĭ alfabetelor pe care le indică cheia, pentru a reveni brusc la litera inițială sau primul alfabet.

Ast-fel décă cheia este *Bucureşti*, în loc de a o repeta regulat prin seriĭ de 9 litere, el tae arbitrar cheia şi scrie. — Buc+Bucureşti+Bucureşti+Bucur+Bucu-

reș+etc. etc..... punctul de oprire este indicat prin o literă a cheeĭ, care se intercalează în text cifrat.

Să luăm un exemplu și să 'l cifrăm dupe metoda luĭ Viginère.

Spre exemplu: *străbăteți pădurea*, având *cheia București*,

s t r	+	a b a t e t i p ă	+	d u r e a	+		
Buc	+	B u c u r e ș t ĭ	+	B u c u r	+	etc. etc.	
t n t	u	b v c n z x a i i	u	e o t y v	u		

litera *u* este litera din cheia care indică oprirea bruscă a cheeĭ.

Pentru a evita confusiunea în semnificarea atribuită literei de oprire, se ramplasează în textul cryptographic prin o cifră arabă corespunḑênd loculuĭ ce ocupă în cuvêntul cheeĭ; ast-fel un exemplu de sus, litera *u* ocupă în chee a doua literă, o înlocuim și noĭ cu 2 în tóte părțile unde litera u nu jócă rol de cât de literă de oprire. — Cifrând cryptogramul avem: = t n t 2 b v c n z x a i i 2 e o t y v.

Un exemplu ingenios. — Să presupunem că am primit urmĕtorul cryptogram: 29-75-41-79-48-25-49-71-28-21-45-78 împreună cu tabela alăturată.

	1	9	8	5
7	d	o	u	i
4	n	e	i	t
2	a	v	i	m

Pentru a afla înțelesul cryptogramuluĭ de maĭ sus, n'avem de cât să luăm cel d'antâiu numĕr al fie-căreĭ cifre pe linia orizontală, iar al II-lea numĕr pe linia verticală spre exemplu: luăm pe 2 pe linia orizontală și pe 9 pe linia verticală și unde se întâlnesc la punctul de intersecție dăm peste v, — dupe aceia luăm pe 7 pe linia orizontală și pe 5 pe cea verticală și dăm peste

litera *i*, și urmămtot ast-fel până terminăm tóte cifrele și găsim frasa urmětóre: *vino imediat.* — Numerile 2, 4, 7, 1, 9, 8, 5, servesc drept cheiă, - pentru a așeza literile uneĭ depeșĭ într'un ast-fel de patrat n'avem de cât să le așezăm într'un mod arbitrar și pe urmă căutăm cifrele carĭ corespund pentru a forma cryptogramul.

II-a Metodă. Se ia un alfabet și se numerotéză sp. ex. în modul urmětor:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
3	4	1	2	6	8	5	7	10	11	9	13	12	15	24	18	14	16

s	t	u	v	z	x	y
20	19	22	21	23	25	17

pentru a transmite o depeșă dupe metoda aceasta se operéză ast-fel: luăm exemplu *trimete planu.*—In locul literilor din depeșă punem numerile carĭ corespund în alfabet, și avem:=19-16-10-12-10-19-7-18-13-3-15-22; aceste numere le înscriem într'un patrat, avênd cu cheia tot numerile din întâia metodă. — Aceste numere le intercalăm în patratele góle într'un mod arbitrar și acesta va fi cryptogramul.

	1	9	8	5
7	19	19	7	3
4	18	16	15	12
2	10	13	22	10

Acuma combinând întâia metodă cu a II-a formăm din nou alt cryptogram și avem:

71-49-25-45-21-79-78-41-29-75-48-28, — pe care 'l deslegăm dupe cum am vĕdut în întâia metodă.

III-a Metodă. Acéstă metodă constă dintr'un patrat care are 36 case; și drept cheiă s'a ales un-spre-zece litere.—Literile depeșeĭ se așéză în case într'un mod

arbitrariu și se ia ca semn cryptografic în locul aceleĭ litere două litere carĭ sunt așezate la extremitatea verticală și orizontală a tablouluĭ, — literile cheeĭ sunt: N U A O E H L M B S N. Acéstă metodă are mare asemânare cu cele expuse maĭ sus, cu deosebire că aci cheia este în litere și cryptogramul se scrie tot în litere, iar nu în cifre, ca metodele de maĭ sus.

H	L	M	B	S	N
E	i	o	r	e	a
O	u	t	n	r	i
A	m	f	a	e	n
U	m	r	a	i	t
I	i	x	h	e	s

Luăm exemplul urmĕtor: *trimeți hrană, suferă ómeniĭ*, aședăm literile din depeșă în casele góle într'un mod arbitrat, și trimitem drept cryptogram cele două litere carĭ se află considerând litera din depeșa ca intersecția a două liniĭ care plécă spre literile cheeĭ, spre exemplu în locul literei t punem OM, în locul literei *r* punem EB și așa maĭ încolo până terminăm cryptogramul,—și vom trimete depeșa sub forma urmĕtóre:

OMEBELALESUNONI IBUMENOBNB INOLAMASOSAB EMULISANILUS

Pentru a descifra un cryptogram trimes după acéstă metodă n'avem de cât să luăm câte două litere din cryptogram; spre exemplu O M, ne ducem pe orizontala luĭ O până întâlnim vertical plecată din M și la punctul de intersecție găsim litera t care va fi prima literă din depeșă; dupe aceea luăm pe E B, ne ducem pe orizontala luĭ E până întâlnim vertical plecată din B la intersecție, întâlnim a doua literă r a depeșiĭ, și urmăm tot ast-fel până descifrăm tot cryptogramul,

Descifrarea sistemelor cu triplă cheiă.

Am vorbit deja că sistemele cu cheiă variabilă, orĭce depeșă scrisă dupe dênsele garantéză secretul atât timp cât descifrorul nu póte găsi literile de oprire bruscă, ceea ce este fórte greu într'o depeșă scurtă; dar îndată ce depeșa are 6 sau 7 linii, atunci orĭ-ce descifror constată îndată întâlnirea aceleiașĭ litere de maĭ multe orĭ într'un rând, și îndată ce a descoperit acéstă literă atunci descifrorul este asigurat de depeșă, căcĭ n'are de cât a pune în colónă diferitele grupurĭ formate de intervalele literei de oprire de la una la cea l'altă, și făcênd calculul pe care orĭ-ce descifror trebue să 'l cunóscă, va termina prin a descifra cryptogramul. — Descifrarea nu póte presenta dificultățĭ de cât numaĭ atunci când ordinea alfabetică a fost intervertită.

Resultă prin urmare că tóte sistemele de cryptographie cu basă variabilă, care sunt usitate astă-dĭ, nu presintă nicĭ o garanție seriósă de indescifrabilitate.

Se póte că cutare sau cutare depeșă de o lungime de patru sau cincĭ linii cryptographice cu alfabete neintervertite și cu o cheiă neavênd de cât 5 sau 6 litere, să resiste eforturilor celor maĭ bunĭ descifrorĭ, dar cu tóte acestea nimic nu este maĭ ușor pentru unul care știe a descifra, de cât a combina cryptogramul indescifrabil cu cele maĭ vulgare sisteme și dacă cryptographia trebue a deveni, dupe cum am maĭ zis, un axiliar puternic al tacticeĭ în mâinile celor maĭ bunĭ generalĭ; trebue ca sistemul să presinte garanțiĭ solide, că cryptogramul intrând în mâinile celuĭ maĭ puternic descifror să nu pótă parveni a afla secretul.

Și dacă pentru un moment neglijăm partea cea mai esențială adică: practica, care trebue să presinte orice sistem cryptographic destinat la trebuințele armatei, vom putea adopta un sistem în triplă cheiă, și a combina un procedeu de transpositiune cu un sistem de interversiune cu basă variabilă.

Ast-fel sistemul de Saint-Cyr combinat cu metoda întrebuințată de nihiliști în Rusia, va permite minimum de note scrise, și ne va da un cryptogram, dacă nu matematic indescifrabil, cel puțin nu dă nici un indiciu de calcul de probabilitate, sau tatonament.

Cele două cheĭ va trebui a fi representate prin două cuvinte diferite, ast-fel ca unul să fie adiectiv și altul substantiv, primul cuvênt compus din un număr mic de litere va servi drept cheiă la interversiune și al II-lea cuvênt de un număr de litere mai mari ne va da formula de transpositiune.

Să luăm un exemplu și să cifrăm dupe modul cum l am expus mai sus spre a vedea cum se presentă cryptogramul.

Luăm drept cheiă, dupe cum am spus, *Senatu — Română*, iată exemplu de cifrat.

Simulați un atac in aripa stângă.

Cu cheia *senatu* facem cryptogramul dupe tabloul luĭ Viginère — și avem:

s i m u l a ț ĭ u n u a t a c î n a r i p a s t â n g ă	depeșa.
s e n a t u s e n a t u s e n a t u s e n a t u s e n	punem cheia.
k m z u e u l m h n n u l e p m t m a t n s m u f k n	dupe tabloul luĭ Viginère.

Română dă ca formulă numerică — 653124, între-

buințând sistemul nihiliștilor din Rusia pentru cryptogramul aflat dupe metoda luĭ Viginère avem:

R o m ă n u

6 5 3 1 2 4

	1	2	3	4	5	6
1	k	m	z	u	e	u
2	l	m	h	n	n	u
3	l	e	p	m	t	m
4	a	t	n	s	m	u
5	f	k	n	a	b	c
6	d	e	f	g	h	i

	6	5	3	1	2	4
6	i	h	f	d	e	g
5	c	b	n	f	k	a
3	m	t	p	l	e	m
1	u	e	z	k	m	u
2	u	n	h	l	m	n
4	u	m	n	a	t	s

terminând acéstă transpositiune avem cryptogramul următor: = i h f d e g c b n f k a m t p l e m u l z k m n u n l h m n u m n a t s. Dar repetăm încă o dată ca acest procedeu garantéză aprópe complect indescifrabilitatea, dar lasă mult de dorit din punctul de vedere practic, pentru că sistemele cele maĭ bune care se aplică în timpul de resboiu trebue să fie cât se póte simple, dar în acelaș timp să presintă cât se póte maĭ multe dificultăți aceluia care s'ar încerca să descifreze o depeșă.

Metoda divisorilor.

In acéstă metodă se întrebuințéză un numĕr órecare de colóne orizontale și verticale, avênd grijă de a disposa literile depeșeĭ să fie tot d'a-una de o manieră ast-fel, ca numĕrul total al literilor din depeșă să fie produs a douĕ numere întregĭ, este destul pentru acéstă condițiune de a micșora numĕrul total al literilor, sau a adăoga litere fără valóre; să luăm un exemplu și să 'l cifrăm. *Indoește survegherea este multă probabilitate să fiĭ atacat,* vom avea tabloul următor:

In depeșa nóstră sunt 53 litere, prin urmare până la complectare, punem litere fără valóre din alfabet a b c d etc., trebue ca literile să corespundă esact în acelaș mod, în fie-care linie orizontală.

	1	2	3	4	5	6	7	8	9	10	11	12
1	I	n	d	o	e	ș	t	e	s	u	r	v
2	e	g	h	e	r	e	a	c	s	t	e	m
3	u	l	t	a	p	r	o	b	a	b	i	l
4	i	t	a	t	e	s	e	f	i	i	a	t
5	a	c	a	t	u	a	b	c	d	e	f	g

Intervertim dupe acésta într'un mod arbitrar numerile carĭ constitue cheia cryptogramuluĭ cu tóte literile care se află în colónele verticale și obținem tabloul următor:

	1	10	7	5	9	6	2	11	3	12	4	8
1	I	u	t	e	s	s	n	r	d	v	o	e
2	e	t	a	r	s	e	g	e	h	m	e	e
3	u	b	o	p	a	r	l	i	t	l	a	b
4	i	i	e	e	i	s	t	a	a	t	t	f
5	a	e	b	u	d	a	c	f	a	g	t	c

scriind fie-care linie orizontală, începênd de la stânga pentru a merge către drépta vom obține cryptogramul următor = Iutessnrdvoeetarsegehmeeubopar litlabiieeistaattfacbudacfagtc.

Pentru a da maĭ multă siguranță tablouluĭ, putem scrie literile din tablou dupe metóda paralelogramelor.

Este evident că pentru a găsi ordinea nouă în care sunt scrise colónele verticale, sau maĭ bine zis cheia

sistemului, trebue a recurge la note scrise, căci memoria nu póte nici o dată ține minte atâtea interveniri de cifre (cheia). — Se remediază fórte ușor acest inconvenient, prin mijlocul unuĭ cuvênt, sau a maĭ multor cuvinte ușor de ținut minte, care transformate în cheiă numerică ne va permite de a găsi cu ușurință ordinea în care trebue a fi dispuse colónele verticale.

Spre exemplu luăm numele unuĭ general.

General Pilat, acest cuvênt 'l transformăm în serie numerică și vom avea:

g'	(I-iu)	care începe cuvêntul general va fi înlocuit prin	1
l'	(II-lea)	care se află în cuvêntul general » » » »	2
P'	(III-lea)	care se află în cuvêntul Pilat » » » »	3
a'	(IV-lea)	care se află în cuvêntul Pilat » » » »	4
e'	(al II-lea)	care se află în cuvêntul general » » » »	5
e'	(I-iu)	care se află » » » » » » »	6
n'		care se află » » » » » » »	7
t'		care se află » » Pilat » » » »	8
r'		care se află » » general » » » »	9
a'		care se află » » » » » » »	10
l'		care se află » » Pilat » » » »	11
i'		care se află » » » » » » »	12

De modul acesta vom înlocui cifrele și vom avea:

g e n e r a l P i l a t
1 6 7 5 9 10 2 3 12 11 4 8

Cu modul acest am format o cheiă care o putem ține minte deslul de bine.

Metoda divisorilor cu dublă transpositiune.

Până aci noĭ am suposat că am intervertit numaĭ ordinea colónelor verticale, fără a ne atinge de colónele orizontale.—Dacă intervertim ordinea liniilor orizontale în acelașĭ timp cu al colónelor verticale, întrebuințăm, ceea ce numim în cryptographie, metoda di-

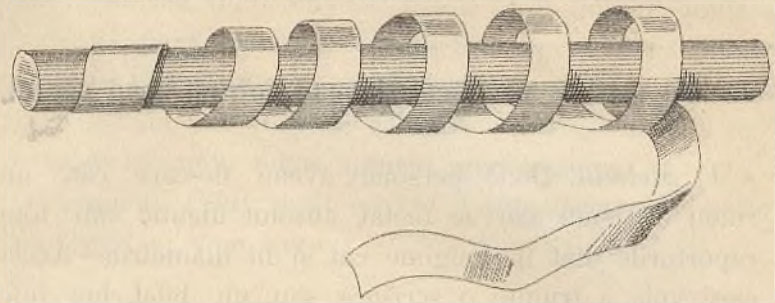
visorilor cu dublă transpositiune sau cu dublă cheiă. Dacă vom observa bine acéstă metodă este tocmaĭ metoda cu dublă transpositiune întrebuințată de nihiliștĭ în Rusia, și pe care am descris-o deja maĭ sus.

Vechile metode de a corespunde într'un mod secret.

1) *Metodă.* Douĕ persóne aveau fie-care câte un rulou de lemn sau de metal, absolut identic sub tóte raporturile atât în lungime cât și în diametru.—Acela care voia a trimite o scrisóre sau un bilet, lua fóie strâmtă de papyrus, sau de pele de berbec preparată pentru a scri, sau o bucată de stofă gomată, o învêrtea împrejurul ruloului (cylindru) în așa mod ca să concidă extrămitățile și cylindrul se găsea ast-fel complect acoperit, atuncĭ expeditorul scria de la un capĕt la altul a crytogramuluĭ urmând axa, seria I-a linie, a doua, a treia etc.

Operațiunea terminată, trimițătorul desfășura hârtia dupe cylindru și atuncĭ hârtia se găsea încărcată de o mulțime de litere, fără nicĭ o legătură și fără nicĭ un sens, expeditorul strângea acéstă bombă de hârtie, o închidea cu îngrijire într'un plic sau o cutie, și o tri-

metea la corespondentul seu; acela care primea biletul n'avea de cât să o resucéscă împrejurul cylindrului



ce poseda, și hârtia venea cu cuvintele în ordinea lor naturală, și frasele reapăreau lisibile. Mult timp cei vechi se serveau de focuri aprinse pe înălțimi, însă aceste semnale nu arĕtau de cât un *da* sau *nu*, arĕtând că s'a îndeplinit sau nu s'a îndeplinit cutare act.

Dintre semnale cele mai principale în vechime eraŭ telegraphia brațelor, supranumită și telegraphia aeriană Cu ajutorul brațelor se transmite literile alfabetului și în consecință chiar frase întregi, și înaintea electricității telegraphia aeriană constituia un mijloc de a corespunde secret. Literile alfabetului erau întocmite prin semne convenționale formate dinainte.

Metoda cărților de joc.

Corespondența cu cărțile de joc póte să conteze de a fi citată în numĕrul cheilor nedescifrabile. Iată cum procedăm: putem să întrebuințăm sau 52 cărți sau numai 32, adică cărțile de pichet, așezăm cărțile într'o ordine convenită, care póte fi arbitrară și scrim literă cu literă pe fie-care carte; să suposăm că am luat

32 cărți și că am adoptat o ordine óre-care atât în culori cât și în valori.

Culorile, spre exemplu, le așezăm în ordinea următóre:

Careau-cupă-pică-treflă, iar valorile le așezăm în ordinea următóre:

As-damă-zece-opt-nouĕ-rege-șépte-valetu; să luăm un exemplu de 32 litere, *trecĭ podu atacă pădurea cu o companie*, cărțile depuse în ordinea care am convenit mai sus avem:

Vom scri depeșa în modul următor:

Ax de caro	a Ax de pică
t e Damă ____	d Damă ____
r zece ____	u zece ____
e opt ____	r opt ____
c nouĕ ____	e nouĕ ____
i rege ____	a rege ____
p șépte ____	c șépte ____
o Valetu ____	u Valetu ____
d Ax de cupă	o Ax de treflă
u Damă ____	c Damă ____
a zece ____	o zece ____
t opt ____	m opt ____
a nouĕ ____	p nouĕ ____
c rege ____	a rege ____
a șépte ____	n șépte ____
p Valetu ____	i Valetu ____

Dacă depeșa este mai mare punem literile unele lângă altele, dupe ordinea scrierii la dreapta, luându-se cea din stânga întâiŭ, aci avem o literă mai mult, pe e, 'l scrim lângă t la drépta.

Dupe ce am terminat amestecăm cărțile și le expe pediăm la corespondent, care stabilindu-le în ordinea convenită, citesce depeșa; acest ordin de a aranja cărțile este arbitrar și póte varia la infinit. Noĭ am ales aci într'un mod maĭ clar pentru a se înțelege maĭ bine exemplul. Cheia jocurilor de cărțĭ este originală; se póte chiar scri pe cărțĭ în loc de litere cu semne, dar maĭ simplă și maĭ practică este metoda expusă maĭ sus.

Metoda cu cheiă repede.

In cryptographie este stabilit principiul, că: orĭ-ce perfecționare trebue să aducă o simplicitate, natura ca și arta ne arată perfecțiunea în simplicitate. Supt acest raport, sistemul grilelor, al cărților de joc, cheile cu cadran, sunt cheĭ defectuóse prin singurul reson că ele sunt ușóre, dar complicate, și necesită timp.

Un general în campanie voește a transmite un avis sau un ordin, aci minutele sunt mĕsurate și trebue nu numaĭ ca depeșa să fie inviolabilă, dar ca să nu fie descifrată de inamic, dacă i-ar cădea în mână, și efectul uneĭ depeșĭ póte să 'șĭ piardă importanța dacă a întârziat, și în acest cas depeșa trebue repede cifrată. Iată dar o cheiă indescifrabilă, ea este cunoscută de ceĭ inițiațĭ în cryptographie și trebue prin urmare vulgarisată.

Cheia care vom enunța are treĭ calități: I-a este simplă, a II-a se cifréză cu ea repede și a III-a este inviolabilă, și este nefolositor a o complica; iată în ce constă:

Se ia de către ambiĭ corespondenți o carte ca să aibă amândouĕ aceiașĭ ediție.

Literile primuluĭ cuvênt al depeșeĭ se va lua din

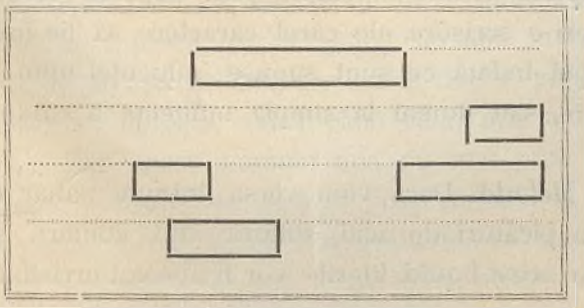
prima pagină a acesteĭ cărți, literile cuvêntuluĭ al II-lea din a II-a pagină, literile cuvêntuluĭ al III-lea din a III-a pagină și așa maĭ încolo. Așa spre ex.

Dacă voim a transmite o frasă, *părăsește posiția*, cuvêntul părăsește 'l cifrăm în prima pagină în modul următor: căutăm litera p și o găsim la a 13 literă, însemnăm 13, căutăm pe a 'l găsim la 30, însemnăm 30, căutăm pe r 'l găsim la 5-a literă, însemnăm 5, și urmăm tot ast-fel până terminăm cuvêntul; literile sunt despărțite între dênsele prin virgule, iar cuvintele prin puncte sau alte semne convenționale. Dupe ce am terminat cuvêntul întâiŭ ne întórcem la pagina II-a și cifrăm al II-lea cuvênt și așa maĭ încolo.

Metoda grilelor.

Fórte adesea se servă pentru a transmite depeși, prin aceia ce se numesce grile sau bare de liniĭ simple, se ia o bucată de carton sau fóie de metal subțire, în care vom întrerupe, în sensul lungimiĭ, spațiurĭ pentru a face să se intercaleze alte cuvinte pentru a denatura sensul fraseĭ.

Figura de maĭ jos este un aparat de care ne servim la scrierea depeșeĭ și se operează în modul următor:



Se aşéză acéstă grilă (sau fóie de carton) şi scrim depeşa în spaţiurile egale, ridicăm aparatul şi umplem liniile cu cuvinte care denaturéză complect sensul fraseĭ.

Să presupunem că voim să trimetem frasa următóre: *vino imediat cu compania la stab*, o vom scri în modul următor:

părăseşte satu *vino* cu ofiţeriĭ
imediatŭ fără să se simtă, *cu*
compania lăsând unŭ mic
post de 30 ómenĭ în ajutor

Persónele la carĭ depeşa este adresată pe hârtie, posedând o grilă dupe modelul de maĭ sus, punênd pe hârtie va apare imediat cuvêntul înţeles al fraseĭ care voim a'l transmite.

Recete de cerneală invisibilă pentru a corespunde într'un mod secret.

Voiŭ da acum principalele recete cunoscute pentru a compune lichide în culorĭ, prin mijlocul cărora putem scri o scrisóre, ale căreĭ caractere să fie invisibile, dar apoĭ îndată ce sunt supuse influenţeĭ unuĭ reactiv óre-care, sau numaĭ la simplă influenţă a căldureĭ, ne apare.

I-a *Metodă*. Dacă vom vĕrsa într'un pahar de apă câte-va picăturĭ de acid sulfuric din comerţ, şi vom scri cu acest liquid, literile vor fi absolut invisibile, dacă

dosa de acid sulfuric nu a fost prea mare, espunênd la foc scrisórea literile vor apare cu o culóre négră.

II-a *Metodă*. Dacă luăm jumĕtate de pahar cu apă și dacă adăogăm în acéstă apă o cantitate egală de acid nitric, și dacă facem la răcéală să se disolve în acéstă amestecătură puțin mercur, literile scrise cu acéstă soluțiune vor fi absolut incolore, dar dacă punem hârtia la căldura unuĭ foc, literile vor apare într'o culóre neagră.

III-a *Metodă*. Dacă luăm o soluțiune de azotat de bismut și ne servim cu acest liquid pentru a scri, literile vor fi invisibile. Dacă vom face ca foaia de hârtie să trécă printr'o fusiune concentrată de *noix de galle*, literile vor apărea imediat în negru. Insă expunerea hârtiĭ la foc nu o va face să apară de loc literile.

Acéstă cerneală simpatică are avantagiul asupra celor l-alte că necesită existența unuĭ reactif pentru a face ca caracterele să fie visibile, și prin urmare cu fórte mare greutate se póte găsi la îndemână ast fel de liquid, póte numaĭ hasarduluĭ să datoréscă cine-va să 'l posede și o depeșă scrisă în acéstă metodă cu greu va parveni inamicul a o descifra, maĭ cu sémă că nu știe ce liquid să întrebuințeze pentru a le face visibile literile.

IV-a *Metodă*. In loc de azotul de bismut putem să facem să se topéscă într'un pahar de apă sulfatul de fer, lăsând în apă cristale de sulfat de fer până ce disoluțiunea se oprește, adică până când apa a ajuns la saturație. Din acest moment apa nu maĭ póte asimila o singură moleculă de sare și póte sta un an întreg fără a perde un miligram din greutatea sa. Dacă scrim cu acest liquid literile vor fi invisibile, pentru a le face

să reapară n'avem de cât a muia hârtia (scrisórea) într'o soluțiune de noix de galle, literile vor apare îndată într'un negru pronunțat. Trebue a remarca că cele două corpuri, sulfatul de fer și noix de galle, sunt cele două părți cari constituesc cernéla négră ordinală, cu deosebire că în loc de a opera într'un vas cu apă, noi le întrebuințăm aci separat, și se produce urmétórea reacțiune. Acidu galic, din noix de galle descompune sulfat de fer, elimineză acidul sulfuric din acéstă stare și se combină cu acid de fer devenit liber, (pentru că are mai multă afinitate pentru oxid de fer de cât pentru acid sulfuric) și în loc de un sulfat de fer, lichidul conține un galat de fer, a căruĭ culóre este neagră; pentru a muia hârtia într'un acid n'avem de cât să ne servim cu o pensul muiată în soluțiune trebuinciósă.

V-a *Metodă.* Luăm sublimat corosiv (deuto chlorură de mercur) și facem a se disolva acéstă sare în apă, literile invisibile făcute cu acest lichid apar imediat în negru; când imbuibăm hârtia într'o soluțiune de chlorhydrat de cositor.

VI-a *Metodă.* Disolvăm alun sau mai bine zis sulfat dublu de aluminium și de potasă într'o cantitate de apă. — Literile scrise cu acest lichid vor fi invisibile. Dacă vom face să curgă apă mai multă peste rândurile scrise cu acéstă soluțiune, atunci vom vedea că caracterele vor apare într'o culóre neagră puțin pronunțată; pe mĕsură însă ce hârtia se va usca atunci și literile dispar, și vom repeti acéstă experiență de câte orĭ vom voi. — Acésta este o cernélă fórte puțin costisitóre și a căreĭ întrebuințare este fórte mult rĕspândită.—Se póte ca între liniile uneĭ scrisorĭ fără nicĭ o însemnătate să se scrie cu acéstă cernélă, și

dacă scrisórea cade în mâinile uneĭ persóne indiscrete, sau streine, acésta nu se póte îndoi și nicĭ chiar nu'ĭ trece prin minte că la adăpostul scrisoriĭ se află vre-o depeșă confidențială, între liniĭ.

Cernélă simpatică grenat.

VII-a *Metodă*. Dacă săturăm o cantitate de apă cu o soluțiune de nitro-muziat-de aur, sau maĭ bine dis chlorhydrat de aur, și scrim cu acest lichid incolor, literile vor fi invisibile și vor apărea într'o frumósă culóre purpurie sau grenat, îndată ce vom uda scrisórea cu o soluțiune de chlorhydrat de cositor.

VIII-a *Metodă*. Se ia două părțĭ egale de oxid de cobalt și de sub-carbonat de potasă. — Facem să se disolve oxidul de cobalt în acid nitric și prin acésta disolvăm sarea dispare complect și puțin câte puțin turnăm sub-carbonatul de potasă. — Lăsăm 24 ore acéstă soluțiune, și dupe aceia adăogăm o cantitate egală de apă. Literile scrise cu acest lichid rĕmân invisibile. Dacă expunem hârtia la o căldură lentă atuncĭ literile apar cu o culóre purpurie.

IX-a *Metodă*. Dacă în soluțiunea de la metoda VIII-a înlocuim carbonatul de potase prin azotat de potasă, literile vor apărea într'un roșu deschis, când apropiăm hârtia de foc și va dispărea pe mĕsură ce hârtia se răcește.

X-a *Metodă. Cernélă verde.* Dacă scrim o scrisóre cu o soluțiune de arseniat de potasă săturată, atuncĭ literile vor apărea într'un verde frumos, dacă muiăm hârtia într'o soluțiune de azotat de aramă.

In operațiunile chimice resultant a două sărurĭ for-

méză tót-d'a-una un verde fórte usitat în industrie, în darea culorilor la stofe și la hârtie.

XI-a *Metodă. Cernéla albastră.* Dacă scrim o scrisóre cu o soluțiune concentrată de acid oxalique, literile vor apărea într'un albastru deschis; dacă udăm hârtia cu o soluțiune concentrată de azotat de cobult.

XII-a *Metodă.* Dacă scrim o scrisóre cu o soluțiune concentrată de sulfat de fer, literile vor apare în albastru frumos; dacă udăm hârtia cu o soluțiune de cyanhydrat de potase (prusiat) reacțiunea chimică este resultanta contactului a două săruri producênd o a III-a sare care tótă lumea o cunóște sub numele de albastru de Prusia (cyanhydrat de fer).

XIII-a *Metodă. Cerneală violet.* Dacă scrim cu o soluțiune saturată de nitrat de cobalt, literile vor apărea de culórea violet instantaneu ce vom uda hârtia cu o soluțiune de acid-oxalic.

XIV-a *Metodă. Cerneală galbenă.* Dacă scrim scrisórea cu o soluțiune saturată de biclorură de mercur, literile vor apărea îndată ce udăm hârtia scrisă cu apă caldă simplă.

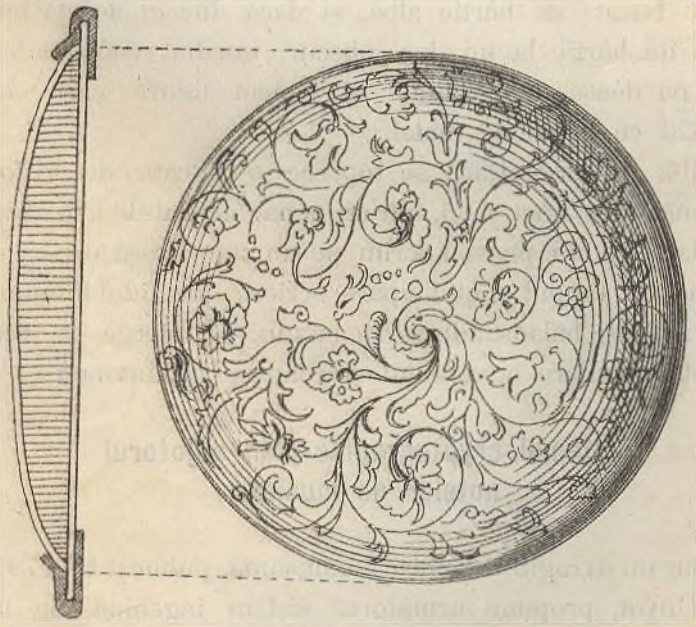
XV-a *Metodă.* Dacă scrim cu soluțiune saturată de nitrat de bismut, și vom uda hârtia scrisă cu o soluțiune de chlorydrat de potase, literile vor apărea îndată într'o culóre galbenă frumósă.

XVI-a *Metodă.* Dacă scrim cu o soluțiune de subacetatu de plumb, pentru a face să reapară tot galbene udăm hârtia cu o soluțiune de acid oxalique.

XVII-a *Metodă.* Dacă scrim cu o soluțiune de chloridrat de antimonium, literile vor apărea în galben destul de pronunțat, dacă vom uda hârtia cu o soluțiune de noix de galle.

XVIII-a *Metodă*. Dacă scrim cu o soluțiune de chlorhum de cobalt, literile vor apărea verde sau albastru, dupe gradul de simetrie al soluțiunii, dacă espunem hârtia la căldura unuĭ foc dulce; dacă lăsăm hârtia să se răcéscă literile vor dispare imediat.

I-a *Metodă originală*. Se ia o sticlă de geam de la un ceasornic care să fie puțin recurbată marginele, pe fundul acesteĭ sticle în interior se fixéză o bucată de hârtie care să fie exact de aceleași dimensiunĭ, și scrim pe dênsa depeșa nóstră; luăm dupe acésta o placă de sticlă rotundă de același diametru ca sticla de ceasornic, putându-se exact să se aplice amândouĕ



sticlele, umplem sticla de ceasornic cu ceară topită; după aceea frecăm cele douĕ sticle pe părțile din afară ast-fel că una din ele, nu cea de ceasornic, cea-l-altă,

să fie muiată în ceară topită, le frecăm până sticla de ceasornic devine mată, din causa cereĭ care s'a răcit, și pe urmă gravăm pe céra aplicată pe geamul de ceasornic o figură óre-care, spre exemplu o flóre, și trimitem acest obiect care pare a fi maĭ mult un obiect de lux de cât o depeșă, acela care primește, n'are de cât să încălzéscă ceara de pe geam, și imediat depeșa va apare și va fi citită, și îndată ce ceara se va usca scrierea nu va fi vĕdută.

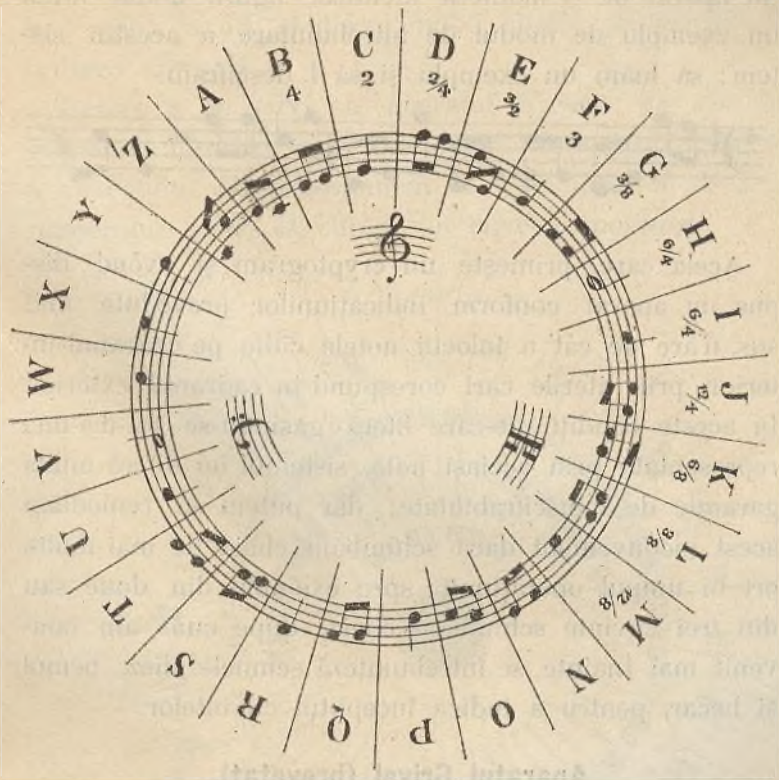
II-a *Metodă*. Se ia o placă de aramă și se adaptéză la dênsa un mâner la centrul plăceĭ; pe fața opusă a plăceĭ se scrie o depeșă (gravată) sau orĭ-ce altă figură, se încălzește bine placa și se aplică fórte tare pe o bucată de hârtie albă, și dacă ducem acéstă bucată de hârtie la un loc obscur, imediat vom putea citi pe dênsa depeșa, sau să vedem figura care s'a aplicat cu placa de metal.

III-a *Metodă*. Dacă se topesce o bucată de fosfor de mărimea uneĭ nucĭ, într'un pahar de unt-de-lem cald și dacă cu un penson scrim pe un zid o frasă óre-care, atuncĭ, în timpul nopțiĭ, apare scrierea pe zidul luminos și vaporos, balansându-se în spațiu, se șterge la cea d'ântâiŭ suflare a vêntuluĭ și reapare instantaneu.

Sistemul cryptographic prin adjutorul notelor de musică.

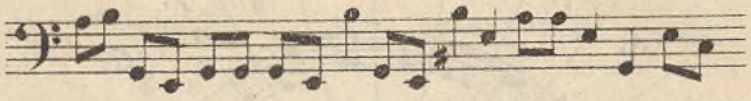
Într'un uvragiu de phisică amusantă, publicat în 1799 de Guyot, propune următorul sistem ingenios. Se ia douĕ cadrane concentrice, avênd fie-care pe dênsele 26 divisiunĭ, cel maĭ mare cadran este fix și are pe dênsul 26 litere ale alfabetuluĭ, ordonate într'un mod

natural sau dupe o cheiă, cadranul cel mai mic care este mobil împrejurul centrului comun presentă pe dênsul 5 linii circulare în care se scriu note, și pórtă pe dênsele divisiuni, cari corespunde fie-care divisiune la o literă a alfabetului.



In interiorul cadranului mobil sunt înscrise trei chei usitate în musică; pentru a cifra un text în acest sistem, se ia o fóie de hârtie de musică, și dispunem

cele două cadrane de o manieră convenită mai înainte, scrim în capul primeĭ liniĭ cheia musicală care corespunde la prima literă a textuluĭ clar (sau orĭ-care altul, dacă există vre-o convenţiune). Acésta servesce şi mĕsura care are litera corespundĕtóre. Aceste indicaţiunĭ servesc aceluia care primesce depeşa pentru a dispune un aparat de o manieră identică, figura aflată arată un exemplu de modul de întrebuinţare a acestuĭ sistem; să luăm un exemplu şi să 'l descifrăm.



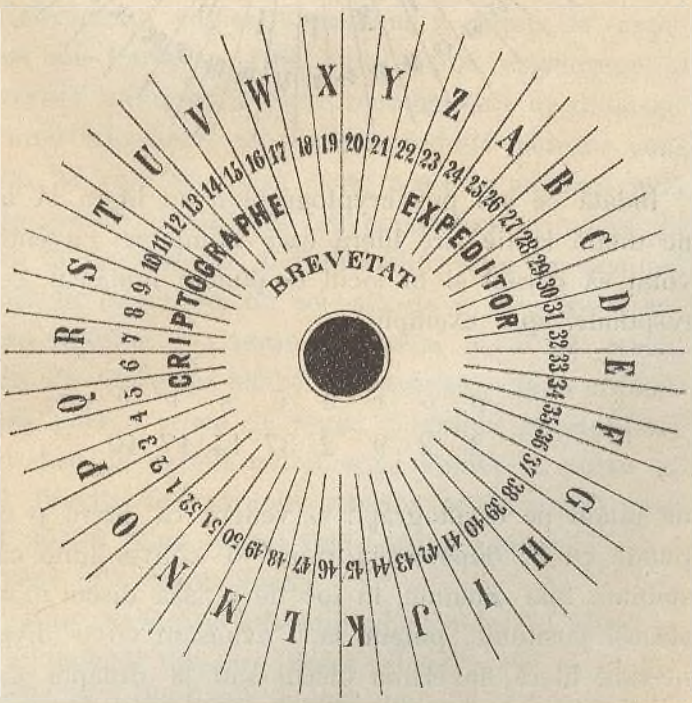
Acela care primeşte un cryptogram şi avênd dispus un aparat conform indicaţiunilor prevĕdute maĭ sus, n'are de cât a înlocui notele citite pe cadranul interior, prin literile carĭ corespund în cadranul exterior. In aceste condiţiĭ fie-care literă găsindu-se tot-d'a-una representată prin aceiaşĭ notă, sistemul nu diferă multă garanţie de indiscifrabilitate; dar putem să remediăm acest inconvenient dacă schimbăm cheia de maĭ multe orĭ în timpul operaţiunĭĭ; spre exemplu din două sau din treĭ cuvinte schimbăm cheia, dupe cum am convenit maĭ înainte, se întrebuinţéză semnele diez, bemol şi becar, pentru a indica începutul cuvintelor.

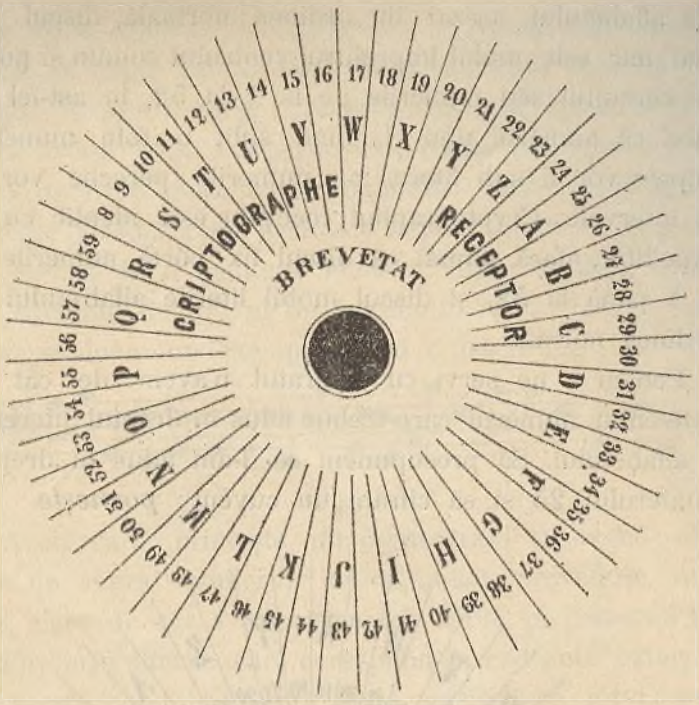
Aparatul Grivel (brevetat).

Este de mult timp că Grivel a imaginat un aparat în două părţĭ, care unul se numeşte cryptographul receptor şi altul cryptographul expeditor. Cryptographul expeditor se compune din două discurĭ concentrice de carton, cel maĭ mare disc pórtă pe dênsul 26 litere

ale alfabetului, așezat în ordinea normală, discul cel mai mic este mobil împrejurul centrului comun și pórtă pe cercuitul său numerile de la 1 la 52, în ast-fel de mod că numĕrul unu (1) fiind subt o tóte numerile impair vor fi sub litere, iar numerile pereche vor fi în intervale. Cryptographul receptor este identic cu cel expeditor, afară numai că discul fix pórtă numerile de la 1 până la 52, și discul mobil literile alfabetului în ordinea normală.

Pentru a ne servi cu aparatul n'avem de cât să convenim numĕrul care trebue adus în dreptul literei A a alfabetului. Să presupunem că 'l-am adus în dreptul numĕrului 25 și să cifrăm un cuvênt: *pornește.*





Indată ce am pus cryptographul cu litera A la 25, ne uităm la fie-care literă care compune cuvêntul ce voim să cifrăm și în locul ei punem numĕrul ce corespunde, spre exemplu:

p o r n e ș t e
3 2 9 2 37 14 17 40

ne uităm pe cryptograph și vedem că litera p corespunde cu 3; dupe aceia, dupe o convențiune care o stabilim mai dinainte, în loc de a lăsa discul mobil în aceiași posițiune, putem să 'l avansăm cu o divisiune fie-care literă, învêrtind discul sau la dreapta sau la stânga. Să presupunem că am convenit să mișcăm dis-

cul de la drépta la stânga cu o divisiune, dupe ce am însemnat pe 3, mișcăm discul cu o divisiune, atunci o, o să corespundă cu 2, litera r cu 9, litera n cu 2, litera e cu 37 și așa mai încolo până terminăm cryptographul și cuvêntul pornește, se va scri în cryptographul urmĕtor: 3, 2, 9, 2, 37, 14, 17, 40.

Când se primește cryptographul atunci se descifréză cu receptor în modul următor: dupe ce s'a dispus ca litera A să corespundă cu No. 25, cum am convenit la prima literă, și pentru a le descifra și pe cele-l-alte execută cu receptor o mișcare inversă de la dreapta la stânga.

Aparatul Vheastone.

Un electrician englez Vheastone, a trimis la exposițiunea din Paris, în 1867, un aparat cryptographic care constă într'o mică cutie rectungulară de dimensiunile uneĭ tabachere, care conținea douĕ cadrane concentrice, pe care se mișca douĕ ace prin mijlocul uneĭ róte de orologiu, mișcarea era combinată în ast-fel de mod că la fie-care tur al cadranuluĭ, unul din ace (cel mic) era în întârziere, de cel-l-alt, de o divisiune a cadranuluĭ interior. — Cadranul exterior purta pe cercuitul sĕu 26 litere ale alfabetuluĭ, aranjate dupe ordinea normală, plus o cruce de reper. Cadranul interior forma un disc de carton mobil dupe voință și purta în aceiașĭ direcție cu cadranul exterior pe cercuitul unuĭ alfabet de 26 litere, așezat într'o ordine convenită, dupe un cuvênt luat drept cheiă.

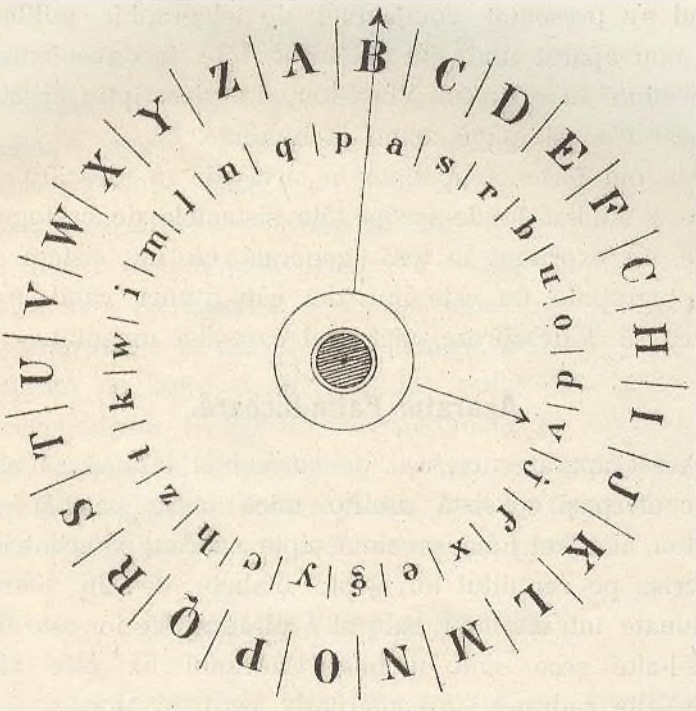
Iată cum dispunem alfabetul din cadranul interior: se ia un cuvênt óre-care drept cheiă, spre exemplu: *projectile,* se scrie acest cuvênt despărțind literile una

de alta, și suprimând pe cele care se repetă și avem:

p r o j e c t i le
a b d f g h k m nq
s u v x y z w.

Sub aceste litere scrim alfabetul normal, afară de literile carĭ se găsesc în cuvêntul proectiv; dupe acésta luăm literile și le scrim pe rând în colóne verticale, începênd de la stânga la dreapta, și avem alfabetul următor: p a s r b u o d v j f x e g h c h z t k w e m l n e q; acest alfabet este scris pe cercuitul cadranuluĭ interior, pentru a cifra un text dupe aparatul luĭ Vheastone procedăm în modul următor: punem prima literă p a alfabetuluĭ interior în fața crucii de reper a cadranuluĭ exterior, și dupe aceia punem cu mâna acul cel mare în dreptul primeĭ litere a textuluĭ care voim să cifrăm pe cadranul exterior și scrim litera marcată de acul cel mic pe cadranul interior, și urmăm tot ast-fel până când terminăm depeșa. Pentru a descifra o depeșă dupe acest sistem n'avem de cât să punem acul cel mic pe prima literă a depeșeĭ în cadranul interior, și citim litera textuluĭ clar pe cadranul exterior marcată de acul cel mare. Vheaston a complectat invențiunna sa punênd cadranul sĕu într'o cutie închisă cu cheiă, conținênd un mecanism care operează automatic, traducțiunea depeșeĭ, fără ca operatorul să aibă cunoștință de modul aranjării.

Colonelul frances Laussedat, se exprimă în modul următor asupra acestuĭ aparat: luând o depeșă cifrată dupe acest aparat a parvenit a o descifra într'un timp neașteptat de scurt și a zis că sistemul nu posedă de cât un numĕr prea limitat de alfabete diferite; și aceleașĭ dispositiunĭ alfabetice revine dupe un numĕr de oprirĭ determinate.



Să suposăm că dupe a 26 sau a 30 literă începe repetarea, atunci n'avem de cât a considera cryptogramul scris cu o cheiă de 26 sau 30 alfabete și a'l pune în colónă prin serii de 26 sau 30 cifre; dar cel mai mare inconvenient care presintă aparatul, este că cere un secret absolut, căci odată căḑut în mâinile inamiculuĭ este destul ca dupe câte-va tatonamente asupra primelor litere ale depeșeĭ pentru a găsi imediat punctul inițial. Când mai multe depeși scrise cu aceiași cheiă au fost interceptate nu mai este nevoe de a poseda un aparat pentru a face descifrarea, căci n'avem de cât a aplica la descifrare sistemul alfabetelor intervertite.—Se zice că sunt vre-o cinci ani de

când s'a presentat comisiuneï de telegraphie militară un nou aparat unde s'a înlăturat tóte inconvenientele prevĕdute în aparatul Vheaston, dar descripția acestuï aparat n'a eșit până acum la lumină.

Un om fórte competinte în arta de a descifra și care a studiat în de-aprópe tóte sistemele de crytographie, s'a exprimat în tesă generală, că un sistem de cryptographie nu este bun de cât atunci când n'ar putea să 'l descifreze, nicï acel care 'l-a inventat.

Aparatul Patin-Richard.

Acest aparat care, eșit de curând la lumină, se află în comerț, și consistă dintr'o mică cutie patrată cu carton, al căruï fund presintă șépte cadrane concentrice înscrise pe cercuitul lor, șépte alfabete de 26 litere; ordonate într'un mod natural. Cadranul inferior este fix, cele-l-alte șése sunt mobile. Cadranul fix este alb, cele-l-alte cadrane sunt alternativ verdï și albe.

Pentru a face să se misce cadranele mobile n'avem de cât a deșurupa un mic șurup care ocupă centrul feței interióre al cutiï, pe fața superióră se află lipită o mică instrucțiune asupra întrebuințăriï aparatuluï. Cu un cuvênt ne servim întocmaï ca tabloul luï Vigenere.

Se ia un cuvênt drept cheiă, de care utilisăm de cele 7 litere d'ântâiŭ sau 7 din urmă, spre exemplu: caravană; deșurupăm șurupul de presiune și punem litera A a primuluï disc mobil în dreptul literei C a cadranuluï fix și litera R a cadranuluï al II-lea mobil în dreptul literei a și așa maï încolo. Aparatul fiind ast-fel dispus citim succesiv literile textuluï cifrat pe cadranul fix, și le înlocuim alternativ prin literile corespundĕtóre pe fie-care cadran mobil.

Aparatul Lemarchand.

Lemarchand, stenograph al senatuluĭ, a imaginat un ingenios aparat de dimensiunĭ restrânse, care se repauséză pe douĕ base, cu totul diferite de cele-l-alte aparate de cifrare. Cifrarea se face prin silabe în loc de litere; resultă prin urmare o economie puțin simțitóre în a se descifra o depeșă. Este o nenorocire că cryptogramele scrise în acest sistem, coprind o amestecătură de litere și cifre, și nu putea fi admise în corespondența telegrafică internațională, în urma conveńțiunii de la Roma; afară de asta, se întrebuința 4 cheĭ diferite pentru a corespunde, ceea ce făcea sistemul prea complicat pentru a fi în usagiul practic.

Aparatele Vinay și Caussin.

Aceste aparate ale căreĭ operațiunĭ se fac într'un mod automatic, atât operațiunile cifrăriĭ cât și ale descifrăriĭ resultă de aci o acceleraţie în lucru, însă are desavantagiul că aceste aparate sunt fórte delicate la maniare și prin urmare fórte puțin practice pentru a fi întrebuințate în serviciul armateĭ.

Există în sfârșit o mulțime de aparate care maĭ de care maĭ ingenióse; ast-fel este sistemul luĭ *Moulleron*, este un mecanism ridicat pe un pupitru destul de complect și nu presintă nicĭ un avantagiu practic. Autorul pare că nu 'l ar fi studiat destul de bine, căcĭ cu tot sistemul sĕu complect, nu ne dă de cât telegrame cifrate aprópe dupe sistemul luĭ Vigenère; ast-fel s'a constatat că cu aceiașĭ cheiă dupe sistemul luĭ Vigenère ne dă acelașĭ cryptogram cu sistem luĭ *Moulleron*.

Ast-fel este cryptographul sau phirographul lui *Rondepierre* este basat pe sistemul de transpositiune pe care 'l-am vĕḑut în text deja. Colónele verticale sunt representate prin bagete în ivoriu, pe care sunt trasate divisiuni destinate a primi o literă, și le transpunem literile dupe o formulă numerică, și scrim depeșa chiar pe bagetă. Acestea sunt în sfârșit puse la locul lor primitiv și literile sunt copiate în ordinea unde ele se presintă. Sistemul acesta este destul de practic, dupe cum se vede din descripție, dar nu oferă nicĭ o siguranță absolută.

Maĭ există un aparat inventat de *Silas*, vechiŭ atașat la ambasada francesă la Viena; cu tóte că acésta este o lucrare seriósă și destul de combinată, este cu tóte acestea destul de complicată și nu are nicĭ o întrebuințare pe timpul de rĕsboiŭ din causa complicațieĭ.

Și dacă observăm tóte descripțiile făcute până acum, am vĕḑut tóte părțile slabe ale sistemelor cryptographice, și prin urmare a cunóște tóte dificultățile carĭ au; prin urmare este imposibil de a înlocui frasele și cuvintele prin grupe de litere sau cifre fără a crea un dicționar care cere cel maĭ mare secret; în consecință procedeurile de transpositiune nu garantează indiscifrabilitatea de cât cu condițiune de a fi basat pe óre-care aparate secrete.

Este adevĕrat că dacă sistemul este simplu și se basézĕ pe óre-carĭ procedeurĭ regulate, sau óre-carĭ combinațiunĭ secrete sistematice, și în acelașĭ timp puțin complicate și să permită cât se póte de multe combinațiunĭ, și în orĭ-ce cas trebue a căuta aplicațiunea în óre-carĭ aparate mecanice, basate pe principiul de interversiune.

Dicționare cifrate și table.

Este fórte greu de a da detalii suficiente asupra diferitelor sisteme cryptographice carĭ au fost în us la diferite armate în secolul trecut; cu tóte acestea se știe positiv că înaintea revoluțiunii francese s'a făcut întrebuințare în corespondența secretă de tabele analoge pe care se întrebuințéză astă-zĭ în ministerele afacerilor streine. Aceste tabele conțineau de o parte frase, și un numĕr óre-care de cuvinte usuale, în față se găsea unul sau douĕ numere pentru a le representa.

Generalul Lewal citéză în «Journal de sciences militaires» fragmente de o literă adresată sub data de la 2 Maiŭ 1815, de ministerul de resbel Davout, către colegul sĕu al afacerilor streine, pentru a-ĭ cere douĕ cifre de acest gen pentru corespondența militară. Aceste cifre sau table cifrante, cum se numea altă dată, sunt numite astă-dĭ dicționare cifrate și care se servă în armată.

Tabelele cifrate și descifrate, se întrebuințéză fórte mult în armatele moderne, și sunt puse sub formă de tablouri; ele oferă douĕ particularități, adică are douĕ table, una servă pentru a cifra depeșa și alta pentru a descifra; în tabelele cifrate, literile, silabele și chiar părți din frasele cele maĭ usuale sunt aranjate dupe ordinea alfabetică.

In tabelele descifrante sunt aranjate diferite cuvinte, litere și părți de frase dupe ordinea naturală, atâtea numere câte cuvinte sunt în tabelele cifrate.

Sub formă de tablou tablele nu pot coprinde de cât un numĕr restrâns de cuvinte, el presintă incovenientul de a putea fi ușor și copiate de ceĭ interesanți. S'a imaginat o mulțime de cheĭ și convențiunĭ pentru a crește siguranța tablelor.

Tablele lui Grivel. Grivel a imaginat tablele cifrante și descifrante care presintă un mare avantagiu asupra tablelor actuale cunoscute până acum.

Grație unor serii de dispositiuni ingenióse, aceste table, supt o formă potrivită, permite de a schimba cheia la fie-care depeșă și acéstă dispositiune este fórte necesară.

Și cu aceste table, chiar dacă ar fi copiate de ceĭ interesați, tot nu póte face nicĭ un us de dênsele.

Pentru a mări siguranța tablelor se înrebuințéză diferite cheĭ carĭ au fost semnalat într'un mod fórte detaliat de către generalul Lewal în uvragiul sĕu intitulat «Tactique des renseignements,» unde a propus următórele: 1) Să se numeroteze a doua óră tablele din dicționar, începênd de la fine de manieră a obține o serie maĭ ridicată la drépta, și una maĭ scoborândă la stânga și se servă alternativ de douĕ serii, urmând modul convenit, sau cifréză maĭ întâiŭ la stânga și pe urmă la drépta, sau douĕ cifre la stânga și douĕ la drépta, sau o cifră la stânga și douĕ la drépta etc. etc. etc. sau representau cuvêntul prin cifre complimentare ale numerilor prin raportul la numĕrul fix care devine cheiă.

Dicționarul Sittler.

Dicționarul Sittler este un mic volum de 100 pagine, care coprinde una-sută cuvinte din ordinea alfabetică, numerotate de la 0 la 99 și imprimate pe douĕ colóne; óre-carĭ numere sunt lăsate în alb, pentru a primi cuvinte carĭ se vor adăoga în urmă, paginele nu sunt numerotate.

Pentru a se servi de acest uvragiu, este suficient de

a indica corespondentuluĭ sĕu pagina şi linia unde se găsesce cuvêntul pe care 'l voim a-l transmite; pentru acest motiv să convie în comun acord o paginaţiune convenţională, întrebuinţând într'o ordine óre-care la numerile de la 00 până la 99, şi o combinaţiune egală convenţională de douĕ cifre cu douĕ cifre ale liniĭ. Să suposăm că prima pagină a volumuluĭ are numĕrul 82, o expresiune óre-care va fi representată prin numerile corespunzĕtóre convenţiuneĭ.

Dicţionarul Sittler nu póte presenta siguranţa de cât cu condiţiune de a schimba cât se póte de des cheia, sau paginele şi combinaţiile numerilor cu câte douĕ cuvinte.

Se raportézĕ că de la 8 Ianuarie 1871, un cryptogram venit din cuartirul general al regeluĭ Prusieĭ, fu dat generaluluĭ Verder, şi nu putu a o descifra imediat, din causă, că dicţionarul care conţinea cheia corespondenţeĭ secrete se găsea închis într'o ladă care se afla într'o trăsură la o mare distanţă.

In timpul resbeluluĭ Turco-Rus din 1877, Selim-Paşa sub-şeful politic al luĭ Mehmet-Ali, se absentă pentru câte-va ţile în luna luĭ Septembrie 1877, şi fără voia luĭ a luat cartea care era pentru descifrarea depeşilor. Generalul en-chef primi în acest timp o mulţime de depeşĭ cryptographice care ĭ fu imposibil a le descifra.

Nu este mult timp că ministrul afacerilor streine din Italia a fost intrigat printr'o noutate care a fost trimisă de ambasadorul sĕu de la Petersburg, că contele Andrassy este aşteptat în capitala Rusieĭ.

Acésta nu era de cât o eróre de cifre, care a fost luat numele unuĭ ataşat de la ambasadă în locul cele-

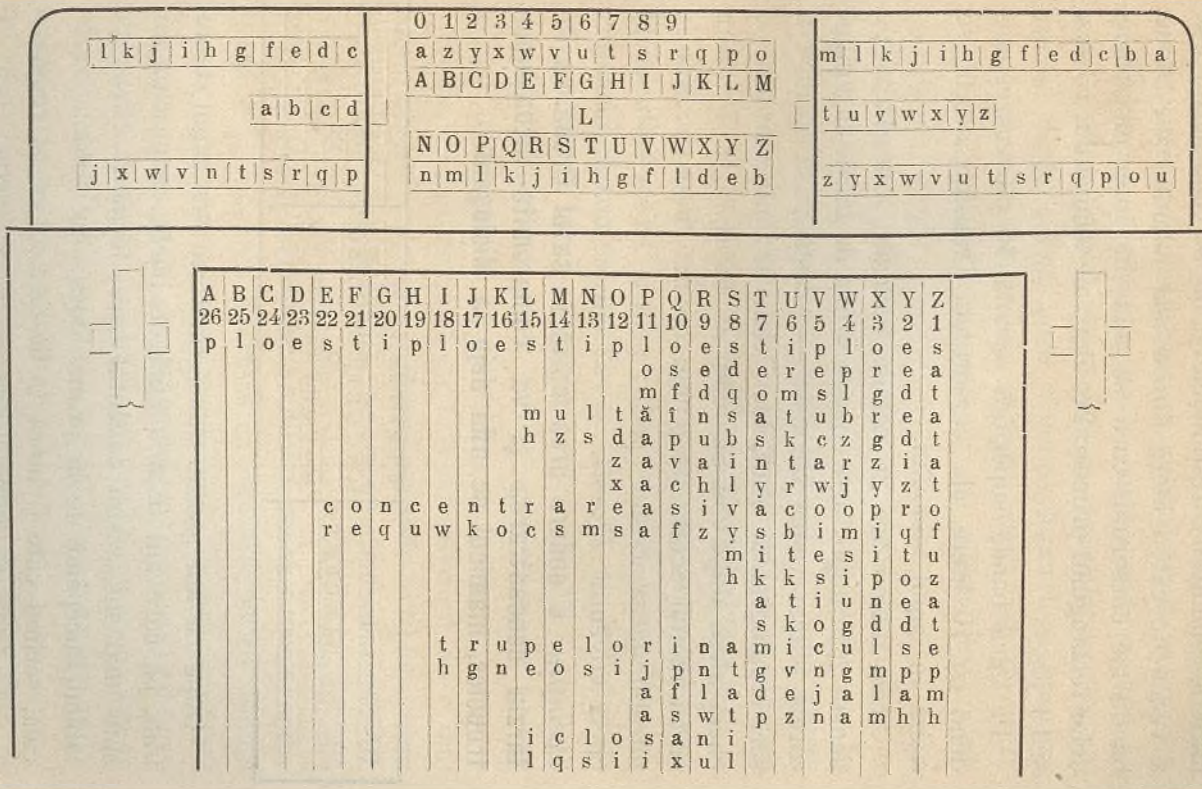
bruluĭ om de stat. Din tóte acestea putem deduce că dicționarele cifrate nu sunt de un usagiu practic, maĭ cu sémă în rĕsboiŭ, unde s'a vĕdut transmițêndu-se chiar de telegraphiștĭ o notă greșită care a denaturat cu totul înțelesul fraseĭ, convine până la un punct órecare pentru cancelariile diplomatice, unde bagajele și corespondențele sunt inviolabile în tóte țerile civilisate, și unde 'și fac cifrarea și descifrarea prin amploiațĭ bine exercitațĭ în acest gen de lucru, și avênd tóte mijlócele de a verifica, dupe plăcerea lor, transmisiunea fidelă a corespondenței.

Aparatul luĭ Bossuat.

Acest aparat se compune din douĕ părțĭ, un tablou și un transformator, care se așéză în capul tablouluĭ și care póte fi fix sau independent, în ansamblu acest aparat ne dă 0,12 centimetri de lărgime și 0,19 centimetri înălțime; transformatorul este dintr'un rectang plin pe care se mișcă un cursar. Pe acest rectang sunt dispuse treĭ bande orizontale paralele, prima bandă și a treia sunt divisate fie-care în 38 părțĭ egale.

In divisiunile bandeĭ întâia sunt înscrise de la drépta la stânga 26 litere ale alfabetuluĭ, urmate de alte 12 prime litere ale alfabetuluĭ.

In a III-a bandă sunt înscrise de la drépta la stânga cele 13 litere din urmă, urmate de 25 litere de la începutul alfabetuluĭ pe banda intermediară se găsesc 26 litere ale alfabetuluĭ; cea d'âmtâiŭ literă corespunțênd la a 7-a divisiune din prima bandă, pe cursar sunt menajate douĕ deschidĕturĭ rectangulare, corespunțênd la prima și la a III-a bandă, și lăsând a vedea 13 litere din fie-care din aceste bande. Afară de acésta o


l k j i h g f e d c
a b c d
j x w v n t s r q p
0 1 2 3 4 5 6 7 8 9
a z y x w v u t s r q p o
A B C D E F G H I J K L M
L
N O P Q R S T U V W X Y Z
n m l k j i h g f l d e b
m l k j i h g f e d c b a
t u v w x y z
z y x w v u t s r q p o u
A 26 p
B 25 l
C 24 o
D 23 e
E 22 s c r
F 21 t o e
G 20 i n q
H 19 p c u
I 18 l e w t h
J 17 o n k r g
K 16 e t o u n
L 15 s m h r c p e i l
M 14 t u z a s e o c q
N 13 i l s r m l s o s
O 12 p t d z x e s o i
P 11 l o m ă a a a r j a a s i
Q 10 o s f î p v c s f i p f s a x
R 9 e d n u h i z n n l w n u
S 8 s d q s b i l v y m h a t a t i l
T 7 t e o a s n y a s k a s m g d p
U 6 i r m t k t r c b t k t k i v e z
V 5 p e s u c a w o i e s i o c n j n
W 4 l p l b z r j o m s i u g u g a a
X 3 o r g r g z y p i p n d l m l m
Y 2 e e d d i z r q t o e d s p a h
Z 1 s a t a t a t o f u z a t e p m h

mică deschidătură corespunḑênd la banda centrală, nu lasă a vedea de cât o literă din acéstă bandă, cele două bande ale cursoruluï care se afla în intervalul bandelor rectanguluï primesc 26 litere ale alfabetuluï 13 sus, și 13 jos.

Pe mica bandă superióră se află 10 cifre corespunḑênd cu 10 litere ale cursoruluï. Transformatorul se așéză în capul tablouluï.

Acest tablou are 26 colóne verticale și se fixéză pe dênsul prin mijloc a 4 cuișóre o fóie de hârtie în lungul căreia putem vedea colónele. — Acésta pusă pentru a scri cryptogramul unuï text clar, se întrebuințéză o cheiă alésă dupe voe. Să luăm un exemplu, să 'l cifrăm și cu modul acesta ne putem da maï bine socotéla de întrebuințarea acestuï aparat; pentru acésta luăm drept cheiă cuvêntul *Ploești*, și să cifrăm textul următor; *exemplu:* **o ședere prea multă în satul Breda, va întârzia concentrarea și va compromite situațiunea trupelor, inamicul se află deja la Micloșanï.**

l k j i h g f e d c b a z	0 1 2 3 4 5 6 7 8 9	j i h g f e d c b a
	x w v u t s y q p o n m l	
A B C D E F G	A B C D E F G H I J K L M	W X Y Z
	O	
y x w v u t s r q p o n m	N O P Q R S T U V W X Y Z	w v u t s r q p o n
	k j l h g f e d c b a z y	

Dupe ce am așezat transformatorul în capul tablouluï, pe care am fixat o cólă de hârtie, dupe cum am spus maï sus, scrim cuvêntul care forméză cheia pe tablou, începênd de la prima literă din colóna verticală, scriind câte o literă în fie-care colónă și repetând acéstă cheiă de atâtea orï, până se va ocupa cele 26 litere ale colóneï. Dupe acésta scrim textul clar al de-

peşeĭ, începênd cu scrierea din colóna care corespunde primeĭ litere a depeşeĭ, ast-fel prima literă a depeşeĭ este p, începem şi scrim de la colóna unde se află p, a doua literă este l, continuăm cu scrierea depeşeĭ începând de la colóna care o indică litera l, şi aşa maĭ încolo până terminăm cu scrierea; dacă am terminat cu literile depeşeĭ, începem iar cu prima literă până terminăm depeşa.

Transformatorul fiind aşezat în capul tablouluĭ, facem să alunece cursorul de o manieră ast-fel ca în deschizătura centrală să apară litera L şi dupe acésta cryptographiăm tóte literile aflate în colónele unde se află litera L — adică în colónele 25, 18, 11 şi 4.

Pentru a face cifrarea uneĭ litere se ia acéstă literă pe banda cursoruluĭ şi o înlocuim prin litera care corespunde pe banda dreptunghiuluĭ fix al transformatoruluĭ, adică litera e o înlocuim cu w, pe t cu h în colóna 11, înlocuim pe o cu m, pe a cu a, pe r cu j şi aşa maĭ încolo.

Dupe ce am terminat cu L scrim cursorul de o manieră ast-fel ca în deschizătura centrală să apară litera o şi atuncĭ crytographiăm literile din colónele 24, 17, 10 şi 3; dupe ce am terminat cu acésta mişcăm din nou cursorul până când în deschizătura centrală apare litera e şi începem operaţia ca maĭ sus, şi cu modul acesta terminăm cifrarea şi în locul depeşeĭ enunţată maĭ sus, vom avea cryptogramul m f d q o m s l g d t z y s d a p u b s k c z g d t x a c h l y r w j y z t r e q u w k o c s m s a f z y s b i m i q f h k k s i p o z s k o g d d t h g n e o s i j p n t g v n g m p p a s w t p z n a m h h l q s i i x u l.

Din descripţia acestuĭ aparat se póte vedea clar că putem obţine nu numaĭ o indiscifrabilitate matematică

dar chiar o indiscifrabilitate materială asigurată, când nu cunóscem cheia.

Acest aparat este simplu și ușor de transportat, și se póte înlocui tabloul prin o hârtie ale căreĭ colóne să fie trase dinainte, și va fi suficientă de a avea cifrorul cu sine numaĭ transformator independent ceea ce va simplifica metóda.