30 kwietnia 1928 r.

RZECZYPOSPOLITEJ POLSKIEJ

OPIS PATENTOWY

Nr 7329. Kl. 15 g 20.

Aktiebolaget Cryptograph
(Stockholm, Szwecja).

Sposób wytwarzania układów znaków szyfrowych, przeznaczonych szczególnie do ruchu telegraficznego, i przyrząd do wykonywania tego sposobu.

Zgłoszono 10 lutego 1921 r.
Udzielono 7 kwietnia 1927 r.
Pierwszeństwo: 10 października 1919 r. (Szwecja).

Wynalazek dotyczy sposobu wytwarzania układów znaków szyfrowych, przeznaczonych szczególnie do ruchu telegraficznego, i przyrządu służącego do wykonywania tego sposobu, składającego się z szybko szyfrującego, elektrycznego aparatu, zapomocą którego wytwarzane są dla nieobznajmionego teoretycznie i praktycznie z kluczem szyfrowym nieokreślone szyfry w formie druku czcionkowego lub znaków, jak np. telegraficzny alfabet.

Wynalazek dotyczy szczególnie umożliwienia szybkiego i nieprzerwanego szyfrowania i odszyfrowywania, np. drogą telegrafu bez drutu pewnych informacyj, które z jednej strony posiadają długość zabezpieczającą przed odczytaniem szyfru przez kogoś niepowołanego, co dotychczas udawało się przez przełożenie mechanizmów kluczowych aparatu szyfrującego, a z drugiej strony wytwarzane są one w takiej ilości, która przy użyciu jednego i tego samego urządzenia tego rodzaju mechanizmu nie zabezpiecza przed niepowołanem odczytaniem. Przy załatwianiu, np. korespondencyj prasowych przez radjotelegraf nadają się często teksty o wielu tysiącach słów, a ponieważ perjodyczność zmian, która dotychczas znanemi aparatami mogła być uskuteczniona bez każdorazowego przestawienia aparatu, w najlepszym wypadku wynosiła zaledwie po 1000 znaków, wyjaśnia to, że stopień pewności szyfru przy tego rodzaju długich koresponn-

dencjach albo zmniejszał się, albo te ostatnie musiały być podzielone na większą ilość szyfrów, przyczem klucz jednego szyfru był zupełnie lub częściowo niezależny od drugiego szyfru, co sprowadzało stratę czasu, nie zapewniało zachowania tajemnicy pomiędzy korespondentami i prowadziło łatwo do nieporozumień i omyłek w szyfrowaniu.

Wynalazek ułatwia następnie wprowadzenie znacznie szybszego postępowania, niż przy użyciu dotychczasowych aparatów do szyfrowania; zasada wynalazku dozwala zmniejszyć masy, które muszą być uruchomione przy szyfrowaniu każdego znaku i zastosować każdorazowe przymusowo elektryczne zwolnienie wszystkich mechanizmów, co powiększa niezawodność działania.

Według wynalazku stosuje się oprócz tego pewien rodzaj szeregów mutacji, które dotychczas nie były używane ani przy elektrycznych, ani przy mechanicznych aparatach szyfrujących, a które przedstawiają zalety bardzo ukrytego, zdawałoby się, nieregularnego zestawienia i dają możność wprowadzania licznych zestawień zapomocą niewielkiej zmiany aparatu.

Przy każdym rodzaju szyfrowania istnieje, w razie gdy wielka ilość słownych tekstów jest szyfrowana tym samym normalnym (alfabetycznym) szeregiem tego samego rodzaju mutacji przy odpowiedniem wzajemnem rozpoczęciu znaków, ta możliwość, że znaki szyfrowane mogą być uporządkowane według tego samego numeru porządkowego ze względu na rozmaitą częstotliwość rozmaitych rodzajów znaków. Powstała przez to lista częstotliwości może przez porównanie z przeciętnym porządkiem częstotliwości zgłosek znanej lub umówionej mowy tekstu dać wiadomość w większym lub mniejszym stopniu prawdopodobieństwa, które istnieje dla znaczenia znaków szyfrowanych, przez co rozwiązanie szyfru bez posiadania szeregu mutacji staje się bardzo ułatwione. To zachodzi naturalnie także w tym wypadku, czy szyfrowanie było wykonane zapomocą aparatu czy nie, dla tego dotychczas było zawsze koniecznem wymieniać bardzo często tego rodzaju części klucza aparatu, które w pewnym stopniu oznaczają zestawienie szeregu mutacji i przeważnie tak często aż każdy szyfr otrzyma swój specjalny szereg mutacji zapomocą rozmaitego urządzenia kluczy.

Niniejszy wynalazek usuwa potrzebę ciągłego wymieniania kluczy przez to, że przez specjalny przyrząd cecha szyfrowanego tekstu sama wpływa na działanie stosowanych dla całego szeregu tekstów mechanizmów kluczowych, a tem samem także na zestawienie otrzymywanego szeregu ruchu, które ponieważ dwa teksty nigdy nie są równe głoska za głoską zmienia się dla każdego poszczególnego tekstu. To umożliwione zostaje zapomocą samoczynnie działającego przy szyfrowaniu jako też przy odszyfrowywaniu przyrządu, który każdorazowo działa, gdy każda wymówiona głoska np. a i oznaczający tę głoskę znak szyfrowy został odszyfrowany. Przez to osiąga się, że te same faktycznie podawane klucze liczbowe przy bieżącej, telegraficznej korespondencji mogą być stosowane podczas oznaczonego, poprzednio umówionego okresu czasu, a mianowicie całkiem niezależnie od ilości telegramów, które podczas tego czasu są wysyłane, nie wpływając na stopień pewności szyfru.

Ażeby wytłomaczyć właściwość wynalazku, należy przedewszystkiem dokładnie objaśnić zasadę teoretycznego szyfru, na którym wynalazek jest oparty.

Rozporządzając dwoma względem siebie przestawianemi narządami szyfrującemi, które zaopatrzone są cyklicznemi ze względu na porządek odwrotnie rozstawionemi alfabetami I i II, można przedstawić te ostatnie dla ułatwienia, jako dwa względ-

dem siebie przestawiane, powtarzające się szeregi znaków, jak np.

I. abcdefg abc defgab.....
II. gfedcbagfedcbagf.....

Jeśli następnie przyjąć, że każdy szereg może otrzymać wypośrodkowane przesunięcie o stałej wielkości i w stałym kierunku przeciwne do przesunięcia drugiego szeregu, np. szereg I jeden przesuw każdorazowo w prawo, a szereg II dwa przesuwy każdorazowo w lewo, to wtedy te szeregi naprzemian poruszające i zatrzymujące się mogą być oznaczone przez szeregi cyfr, naprzykład dla szeregu I: I 001010...., a dla szeregu II: 0200222020....., gdzie cyfra 0 oznacza, że w pewnej oznaczonej chwili nie odbywa się żaden ruch. Womawianych aparatach są wprawdzie te cyfry perjodyczne, lecz mogą one być zawsze tak obrane, że ilość członków okresów nie będzie posiadać żadnego wspólnego czynnika, np. dla szeregu I: (a) 11010 (11010), a dla drugiego szeregu II: (b) 2200 (2200).....

Tego rodzaju szeregi nazwane będą poniżej przez kluczowe lub „główne szeregi ruchu".

Przyjąwszy, że ruchy narządów szyfrujących odbywają się w przeciwnych kierunkach, podano naturalnie dodawanie obydwu szeregów ruchu (a) i (b) członek za członkiem względem przesunięcia obu narządów.

(a) 11010110101101011101011.....
(b) 22002200220022002200220022.....
(c) 33012310321123013210330123 1.....

Wynikły szereg ruchu (c) otrzymuje przytem ilość okresów równą wynikowi ilości okresów szeregów, złożonych w tym przykładzie 5 dla szeregu (a), a 4 dla szeregu (b) 4×5=20.

Złożone przesunięcie obydwu alfabetów w stosunku do siebie lub suma członów szeregu (c) jest tutaj 32, t. j. narządy szyfrujące, których alfabet pomyślany jest jako obejmujący siedem znaków, byłyby po całym okresie ruchu (32—4) : 7=4 stopnie od miejsca wyjściowego w stosunku do siebie przesunięte, a mianowicie:

I. abcdefgabcdefgabcd.....
II. cbagfedcbagfedcbag.....

Ponieważ 7 i 4 nie posiadają żadnego wspólnego dzielnika musi oczywiście 7 takich okresów ruchu nastąpić jeden po drugim, zanim narząd powróci do poprzedniego położenia wyjściowego na końcu całego okresu ruchu tak, że okres, który odnośnie do skuteczności narządów szyfrujących powstaje, będzie zawierał 4×5× = 140 członków.

O ile w tym objaśnionym przykładzie wyszłoby się z poprzednio wskazanego względnego położenia szeregów I i II, gdzie głoska tekstu *a* przy odczytywaniu w szeregu I odpowiadałyby szyfrowanej głosce g w szeregu II, to oczywiście powszechne szyfrowanie jednej i tej samej głoski tekstu dałoby szyfr z okresem 140, jak wskazano na poniższej tabliczce:

głoska tekstu.	poczynająca szereg ruchu głoska szyfrowa 33012310 32 11 23013210 znaki cyfrowe:
a	gdaagebaaecbafccbfdcc
b	fcggfdaggdbagebbaecbb
c	ebffecgffcagfdaagdbaa
d	daeedbfeebgfecggfcagg
e	cgddcaeddafedbffebgff
f	bfccbgdccgedcaeedafee
g	aebbafcbbfdcbgddcgedd
a	gddcaeddafedbffebgff
b	fccbgdccgedcaeedafee
c	ebbafcbbfdcbgddcgedd
d	daagebaaecbafccbfdcc
e	cggfdaggdbagebbaecbb
f	bffecgffcagfdaagdbaa
g	aeedbfecbgfecggfcagg

głoska tekstu poczynająca szereg ruchu
głoska szyfrowa 33012310 32 11 23013210
znaki cyfrowe:

a	cggfdaggdbagebbaecbb
b	bffecgffcagfdaagdbaa
c	aeedbfeebgfecggfcagg
d	gddcaeddafedbffebgff
e	fccbgdccgedcaeedafee
f	ebbafcbbfdcgbddcgedd
g	daagebaaecbafccbfdcc
a	fccbgdccdegcaeedafee
b	ebbafcbbfdebgddcgedd
c	daagebaaecbafccbfdcc
d	cggfdaggdbagebbaecbb
e	bffecgffcadfdaagdbaa
f	aeedbfeebgfecggfcagg
g	gddcaeddafedbffebgff
a	bffecgffcagfdaagdbaa
b	aeedbfeebgfecggfcagg
c	gddcaeddafedbffebgff
d	fccbgdccgedcaeedafee
e	ebbafcbbfdcbgddcgedd
f	daagebaaecbafccbfdcc
g	cggfdaggdbagebbaecbb
a	ebbafcbbfdcbgddcgadd
b	daagebaaecbafccbfdcc
c	cggfdaggdbagebbaecbb
d	bffecgffcagfdaagdbaa

głoska tekstu poczynająca szereg ruchu
głoska szyfrowa 33012310 32 11 23013210
znaki cyfrowe:

e	aeedbfeebgfecggfcagg
f	gddcaeddafedbffebgff
g	fccbgdccgedcaeedafee
a	aeedbfeebgfecggfcagg
b	gddcaeddafedbffebgff
c	fccbgdccgedcaeedafee
d	ebbafcbbfdcbgddcgedd
e	daagebaaecbafccbfdcc
f	cggfdaggdbagebbaecbb
g	bffecgffcagfdaagdbaa

Ażeby wykonane mutacje zastąpić dozwalającemi na porównanie wartościami liczb, przyjęto, że zamiany znaków przy przesunięciach pewnego szeregu alfabetu w stosunku do siebie powstają same, przyczem wielkość odnośnych przesunięć przy rozmaitych zamianach może podawać wartość liczb mutacji. W razie przyjęcia wyżej wspomnianego szeregu I do alfabetycznego lub normalnego szeregu, wykonane według tabliczki każdorazowo dla jednej i tej samej głoski tekstu mutacje mogą być podane przez szeregi cyfr $\alpha, \beta, \gamma, \delta, \varepsilon, \rho, \eta$).

Stosownie do tego otrzymuje się, włącznie z mutacją położenia wyjściowego:

dla głoski	a	szereg	mutacji	α :	4 15542655206530063400 411..
„	„	b	„	„	β :	4 1554265520653063400 411..
„	„	c	„	„	γ :	2 63320433054315541255 266..
„	„	d	„	„	δ :	0 411052115321633260 33 044..
„	„	e	„	„	ε :	5 266530663106411045 11 522..
„	„	f	„	„	ρ :	3 044315441654266523 66 300..
„	„	g	„	„	η :	1 522163226432044301 44 155..

Przy badaniu tych szeregów mutacji można łatwo zauważyć, że posiadają one pewną analogję pomiędzy sobą i że także w dalszym ciągu składają się z tych samych szeregów cyfr z 20 członkami w rozmaitym wzajemnym porządku następstwa.

Według tego co wyżej wspomniano daje np. tekst: abacgdfdbeeacdfebbgea następujący szyfr: gcafabdegafbfcefaeefc z sze-

regiem mutacji: 610315515311361163112 i przyjęto, że gdyby 20 ostatnich znaków tekstu powtarzało się 7 razy, to otrzymałoby się następujący szyfr, który naturalnie posiadałby wyżej wspomnianą analogję pomiędzy różnemi, każda 20 znaków zawierającemi częściami:

gcafabdegafbfcgfaeafc
fdbdegacdbebfabdaabf
bgegacdfgeaebdegddeb
ecacdfgbcadaegacggae
afdfbgcefdgdacdfceda
dbgbcefabgegdfgbffgd
gecefabdecfcgbcebbcg

Podany przyrząd, który zestawione szeregi ruchu *(c)* uzależnia od znajdowania się i ułożenia pewnej głoski (głoski influencyjnej) w tekście, np. w tym wypadku głoski *a* przeprowadzanoby więc przy przyjętym w przykładzie szeregu kluczowym (a, b) i przy wyżej wspomnianym tekście i przy początkowo odpowiadających sobie znakach szeregów alfabetycznych I i II takie działanie, że szósta, ósma i dziesiąta liczba przesunięcia zestawionego szeregu ruchu (c) zastąpiona byłaby przez 0. Tem samem otrzymałoby się zamiast szeregu (c): 33012310321123013210 następujący szereg (c1): 33012010321120013 210, a przyjęty tekst dałby wtedy następujący szyfr gcafabgaedbebfdegddfb z szeregiem mutacji: 6103151416446250524111.

Gdyby więc inny tekst np. adacgdfdbe eacafebbgea, który wyróżnia się jedynie ze względu na drugą głoskę od poprzednio użytej, był szyfrowany temi samemi czynnikami szyfrowania, otrzymałoby się zamiast niego następujący rezultat:

szereg ruchu (c2): 30012010321120013 210

szyfr: gadbdecdfgeaebgacggae

szereg mutacji: 643641404200051315 034.

Jasnem jest, że przy rzeczywistych wymawianych tekstach znajdowanie się i położenie głoski influencyjnej nietylko, jak w przykładzie, w jednem jedynem miejscu na początku szyfru, lecz wskutek całkiem przypadkowych okoliczności zmieniałoby się od początku do końca, dlatego przy dowolnym wymawianym tekście działanie głoski influencyjnej wyżej wspomnianą analogją, która istnieje bez użycia niniejszego przyrządu pomiędzy szeregami częściowemi złożonego szeregu ruchu i wskutek tego także ta sama analogja odnośnie do szeregu mutacji (α, β, γ....) dla każdej powtarzanej głoski tekstu musi być zaniechana. Z tego wynika, że szereg mutacji szyfru otrzymuje dowolne zestawienie, które z matematycznego punktu widzenia zmienia się w regularnym sposobie dla rozmaitych szyfrowanych temi samemi czynnikami szyfrowania tekstów, wynik nieosiągnięty dotychczas przez żaden ze znanych dotychczas elektrycznych lub mechanicznych aparatów szyfrujących.

Stosownie do tego, co wyżej wspomniano, polega sposób na tem, że przypadkowy wybór odpowiedającego znakowi tekstu znaku szyfrowego odbywa się w zgodności z wzajemnem położeniem dwóch dowolnie obranych, symetrycznie urządzonych szeregów znaków, z których każdy stosownie do dowolnie obranego szeregu cyfr (szeregu kluczowego) każdorazowo zostaje przestawiony, przyczem każdorazowo gdy pewien znak tekstu zostaje szyfrowany, wspomniane szeregi znaków podczas następnego przebiegu szyfrowania albo nie zostają przestawione, albo przed ostatnim bez względu na wspomniane szeregi cyfr zostają przestawione o dowolnie obrany kawałek.

Na rysunku podaje fig. 1 schematyczne urządzenie całkowitego aparatu do szyfrowania według wynalazku, fig. 2 przedstawia kolektory aparatu częściowo w przekroju, a częściowo w widoku bocznym, fig. 3 jest widokiem końcowym przyrządu napędowego kolektora, fig. 4 jest przekrojem

sam magnes *M* włącza się w przewód 7 tego solenoidu S_3, który uruchomia klawisz T_2 maszyny do pisania lub dziurkowania dla głoski *a*, wówczas oczywiście ma miejsce stan spoczynku i nieprawidłowości za każdym razem, gdy zostanie odbity odpowiadający głosce *a* znak szyfrowy zapomocą któregokolwiek klawisza wyjściowego. Poza powyższem szyfrowanie uskutecznia się w ten sposób, że deska klawiszowa *T* zostanie uruchomiona w zgodności z otrzymanym szyfrem, przyczem pierwotny tekst otrzymuje się w maszynie do pisania T_2.

W razie gdy przy rozwiązywaniu szyfru zastosowano więcej niż jedną głoskę influencyjną, to odpowiadające tym głoskom influencyjnym solenoidy S_2 muszą być połączone poszczególnie z każdym elektromagnesem *M*, ponieważ inaczej wszystkie odpowiadające głoskom influencyjnym solenoidy S_2 byłyby wzbudzane każdorazowo, gdy odszyfrowywany zostaje znak, odpowiadający jednej z tych głosek.

O ile zamiast wprowadzania w stan spoczynkowy narządów szyfrujących C_1, C_2 przy każdorazowem szyfrowaniu głoski influencyjnej, pożądane byłoby wprowadzanie w ruch tych narządów niezależnie od ruchu wywołanego stykami k_5, k_6, to wtedy należy tylko włączyć przełącznik *d*, d_1 w obwód prądu solenoidów S_4, S_5, a tem samem włączyć pomiędzy przewody *13* i *12* względnie *14* i *12a* i urządzić przełącznik tak, że normalnie będzie on otwarty, przejściowo jednak będzie zamknięty elektromagnesem *M*, podczas szyfrowania głoski influencyjnej.

Skoro ogólny przebieg działań rozmaitych narządów został powyżej schematycznie objaśniony, więc rzeczywiste formy wykonania tych narządów będą poniżej opisane stosownie do fig. 2—7.

Obydwa przedstawione na fig. 2 narządy szyfrujące C_1, C_2 urządzone są każdy na jednym wale *21*, *22*; wały te są umieszczone współosiowo i mogą się obracać w łożyskach *26*, *27*, *28*, które przepuszczone są przez ściany zewnętrzne *68*, *68a* aparatu i przez stałą część pośrednią *36*. Każdy narząd składa się z otaczającej koncentrycznie wał w pewnem oddaleniu rury metalowej *23*, *23a*, która przytrzymywana jest zapomocą dwóch na wale umocowanych części *29*, *30* względnie *29a*, *30a*. Części *29*, *29a* wykonane są jako koła przełączające lub zaporowe, zaś części *30*, *30a* jako tarcze okrągłe każda z cylindrycznym kołnierzem. Na rury nasadzone są pierścienie *25*, *25a*, izolowane jeden od drugiego i od rur. Oba narządy szyfrujące zaopatrzone są we wskazane pierścienie *25*, *25a* w takiej ilości, która równa się ilości klawiszy wyjściowych *T* aparatu (fig. 1). Na wałach urządzone są dalej tarcze okrągłe *34*, *34a* z izolującego materjału z urządzonemi w równych odstępach trzpieniami stykowemi *35*, *35a*, których ilość przy każdej tarczy okrągłej jest równa ilości pierścieni metalowych *25* względnie *25a* narządu. Każdy trzpień stykowy *35*, *35a* połączony jest elektrycznie izolowanym przewodem *67a* z jednym ze wspomnianych pierścieni metalowych *25*, *25a* w dowolnej kolejności. Dowolny porządek wspomnianych połączeń posiada przy obydwu narządach szyfrujących odwrotny przebieg tak, że gdyby one były umieszczone z jednej strony obok siebie z kołami zaporowemi *29*, *29a*, wówczas wskazane narządy byłyby identyczne. W stałej części pośredniej *36* są założone trzpienie stykowe *38*, *38a* w metalowych tulejach *37* z obu stron, przyczem trzpienie te wsparte są nazewnątrz sprężynami śrubowemi *39* i mieszczą się na kole w równych odstępach, jak wyżej wspomniane trzpienie *35*, *35a* tak, że pierścienie metalowe narządów szyfrujących C_1, C_2 przez odpowiednie ustawienie tych narządów mogą wchodzić parami w elektryczne połączenie ze sobą.

Do każdego pierścienia metalowego przylega sprężyna stykowa *66*, przymocowana do stałej części *69* względnie *39a* z izolującego materjału. Te sprężyny odpowiadają wskazanym na fig. 1 sprężynom stykowym k_3 względnie k_4.

Umieszczone na zewnętrznych końcach narządów szyfrujących C_1, C_2 koła przełączające i zaporowe *29*, *29a* zaopatrzone są obok swych zębów zębami zaporowemi *41*, *41a* w liczbie odpowiadającej wyżej wspomnianym trzpieniom stykowym *35*, *35a* (fig. 3). Każde koło zaporowe obracane jest zapomocą zapadki *42*, poruszanej zapomocą obracającej się około czopa *44* dźwigni *43*. Dźwignie *43* przyciskane są sprężynami *46* do stałych oporków *45*, jednak przy wzbudzeniu elektromagnesu *47* mogą być przez niego przyciągane. Koła zaporowe *29* są przełączane o jeden ząb i przytrzymywane zapomocą znajdujących się na dźwigniach *43* występów *48*, które przy końcu ruchu podchodzą pod zęby zaporowe i hamują ich dalszy ruch wskutek bezwładności.

Wzbudzanie obu lub jednego ze wspomnianych magnesów *47* uskutecznia się zapomocą następujących urządzeń. Około czopa *49*, przymocowanego do ramy aparatu, obraca się koło przełączające, czyli zaporowe *51* tego rodzaju, co wyżej wspomniane koła *29*, *29a*. W ten sam sposób co koła *29*, *29a* mogą być one pokręcane naprzód zapomocą zapadki 55, poruszającego się około czopa *59* ramienia *56*, które może być podnoszone elektromagnesem *76*; ramię to jest również zaopatrzone w ząb zaporowy *57*, który służy do tego, ażeby przeszkodzić dalszemu poruszaniu się koła *51* wskutek bezwładności. Na kole zaporowem *51* umocowane jest koło zębate *52* z taką ilością zębów, jak i koło zaporowe. Zaczepia ono obracające się około czopa *48* koło zębate *53*, które styka się z kołem zębatem *54* obracającem się około czopa *50*. Zboku każdego koła zębatego *52*, *54* obraca się około tego samego czopa cylindryczna część *60* względnie *61*, która jest pociągana zapomocą zabieracza *62* względnie *63*, obracając się wraz z kołem zębatem (fig. 4). Jak wynika z fig. 5, złożone są obydwie części *60*, *61* z tarcz okrągłych *60a*, *60b* względnie *61a*, *61b*, z których tarcze oznaczone literą *a* posiadają na obwodzie kołnierz z pewną ilością wykrojów i z tą samą ilością wykonanych koncentrycznie wewnątrz kołnierza otworów *60c* względnie *61c*. W tych wykrojach mogą być osadzone luźne części *60d*, które przytrzymywane są zapomocą umieszczonych w nich, wchodzących w otwory *60c*, *61c* trzpieni *60e*, tak, że skoro tarcze *60b*, *61b* przez wśrubowanie wyżej wspomnianych zabieraczy *62*, *63* zostaną połączone z częściami *60a*, *61a*, to one nie mogą być uwolnione.

Części *60d*, które jak zęby wystają nad obwodem tarcz *60a*, *61a*, służą do tego, ażeby przy stopniowem przełączaniu obrotowych części zamykać jeden lub obydwa przyrządy stykowe *64*, *65*. Gdy ząb *60d* przechodzi pod przyrządem stykowym *64*, który odpowiada stykowi k_6 na fig. 1, zostaje, jak wyżej opisano, zamknięty obwód prądu, który wzbudza elektromagnes z jednej strony aparatu. W razie gdy ząb *60d* przechodzi pod przyrządem stykowym *65*, odpowiadającym stykowi k_3 na fig. 1, to elektromagnes zostaje wzbudzony na drugiej stronie aparatu.

Przy wskazanej na fig. 2, 3, 4 i 5 formie wykonania są stosunki części, względnie przekładnie kół zapadkowych *29*, *29a*, *51* kół zębatych *52*, *53*, *54* i tarcz *60a*, *61a*, które poniżej będą nazywane „kołami kluczowemi" tego rodzaju, że ustanowione na wstępie w teoretycznem wyjaśnieniu warunki zostają wypełnione dla osiągnięcia szeregu mutacji największej długości, gdy koła *29*, *29a* posiadają np. 29 zębów, koło *51* — 13 zębów, koło kluczowe *60a* — 13 zębów, a koło kluczowe *61a* —

11 wykrojów dla umieszczenia dowolnie osadzonych zębów *60d*. Przy wskazanej formie wykonania odpowiada więc cały okres ruchu narządów szyfrujących 13.11.29 = 4147 uderzeniom klawiszy.

W opisanym przyrządzie są pokręcane oba narządy szyfrujące C_1, C_2 przy ruchu o jeden i ten sam kąt; aparat może być jednak w ten sposób zmieniony, że te narządy przez zamianę części napędowych mogą być pokręcane o różny kąt względem siebie. Dalej, może obrót koła kluczowego *61a* przez stosowne urządzenie części napędowych otrzymać dowolną wielkość w stosunku do obrotu koła kluczowego *60a* i również może być podziałka kół kluczowych zmieniona zapomocą wykrojów na umieszczenie zębów *60d*. Fig. 6 przedstawia przyrząd do wykonywania dowolnego obrotu narządu szyfrującego. Zamiast wału *70*, który podtrzymuje narząd szyfrujący *71*, zastosowano czop obrotowy *74*, na którym jest umocowane koło przełączające *75* oraz koło zębate *73*. Koło *73* zaczepia umocowane na wale 70 narządu szyfrującego koło zębate *72* tak, że pokręcanie narządu *71* dla każdego następnego przełączenia koła zapadkowego *75* zapomocą jednej z zapadek *42*, *42a* ramion *43*, *43a* zależne będzie od stosunku pomiędzy średnicami kół zębatych *72*, *73*, które można wymieniać. Ilość zębów koła przełączającego *75* jest natomiast zawsze równa ilości klawiszy aparatu. Przez odpowiedni dobór przekładni można np. osiągnąć, że jeden narząd szyfrujący, w razie gdy ilość klawiszy jest 29, będzie się pokręcał o 2/29 części obrotu, a drugi narząd szyfrujący o 4/29 części jednego obrotu.

Przez zmianę ilości zębów kół *51*, *52*, *54* (fig. 2 i 4) i odpowiednią zmianę ilości wykrojów do osadzania zębów *60d* w kołach *60a*, *61a* mogą być, naturalnie, osiągnięte dowolne stosunki pomiędzy ruchami obrotowemi obu kół kluczowych dla każdego uderzenia klawisza, i również rozmaite ustawienia zębów *60d* oddają rozmaite szeregi działania. Kąty pokręcania kół kluczowych muszą zawsze odpowiadać takiej części jednego obrotu, jaką wyznaczono zależnie od ilości wykrojów kół *60a*, *61a* przy następujących ilościach:

17 zębów na kole *51*,
34 zęby na kole *52*,
46 zębów na kole *54*.

17 względnie 23 wykroje dla zębów w kołach kluczowych *60*, *61* potrzebny byłby okres zawierający 17.23 = 391 uderzeń klawiszów, ażeby mechanizmy kluczowe sprowadzić całkiem niezależnie od ilości włączonych zębów do położenia wyjściowego.

Zastrzeżenia patentowe.

1. Sposób sporządzania przeznaczonych szczególnie do ruchu telegraficznego układów znaków szyfrowych w formie drukowanych czcionkami lub dziurkowanych pasków, kawałków z papieru lub z podobnego materjału, znamienny tem, że przypadkowy wybór odpowiadającego znakowi tekstu znaku szyfrowego odbywa się w zgodności z wzajemnem położeniem dwóch dowolnie obranych, symetrycznie ułożonych szeregów znaków, z których każdy stosownie do dowolnie obranego szeregu cyfr (szeregu kluczowego) zostaje przestawiony, przyczem każdorazowo, gdy szyfrowany zostaje pewien znak tekstu, wspomniane szeregi znaków albo podczas następnego przebiegu szyfrowania nie zostają przestawione, albo przed nim bez względu na wspomniane szeregi cyfr zostają przestawione o dowolnie obrany kawałek.

2. Przyrząd do wykonania sposobu według zastrz. 1 z deską klawiszową, która zostaje uruchomiona stosownie do szyfrowanego tekstu, i z regulowaną zapomocą deski klawiszowej, elektrycznie napędzaną maszyną do sporządzania szyfru,

znamienny dwoma w stosunku do siebie czasowo zatrzymywanemi, symetrycznie urządzonemi podobnemi do komutatora narządami (C_1, C_2), które ze służącą do sporządzania szyfru maszyną są połączone elektrycznie i jej ruchy regulują, następnie dwoma mechanizmami stykowemi (N_1, k_6 i N_2, k_5), które regulują ruchy czasowo zatrzymywanych narządów (C_1, C_2) stosownie do dwóch dowolnych szeregów cyfr, oraz wreszcie wyłącznikiem (d, d_1) który uruchomiany jest dowolnie obranym klawiszem deski klawiszowej (T) i w ten sposób jest urządzony, że przy naciśnięciu tego klawisza albo dowolnie przerywa, albo przy następnym naciśnięciu innego klawisza deski klawiszowej zamyka lub dowolnie sprowadza niezależny od mechanizmów stykowych ruch obu podobnych do komutatora narządów (C_1, C_2).

3. Przykład według zastrz. 2, znamienny przyrządami stykowemi (S, k_1, k_2), które mogą być uruchomiane, każdy jednym klawiszem deski klawiszowej (T), i w ten sposób są wykonane, że przy naciśnięciu tych klawiszy zostaje uruchomiony odpowiedni narząd sporządzającej szyfry maszyny, podczas gdy przy ruchu wgórę klawisza odbywają się ruchy rozmaitych przestawianych narządów.

Aktiebolaget Cryptograph.
Zastępca: Dr. inż. M. Kryzan,
rzecznik patentowy.

Fig.1

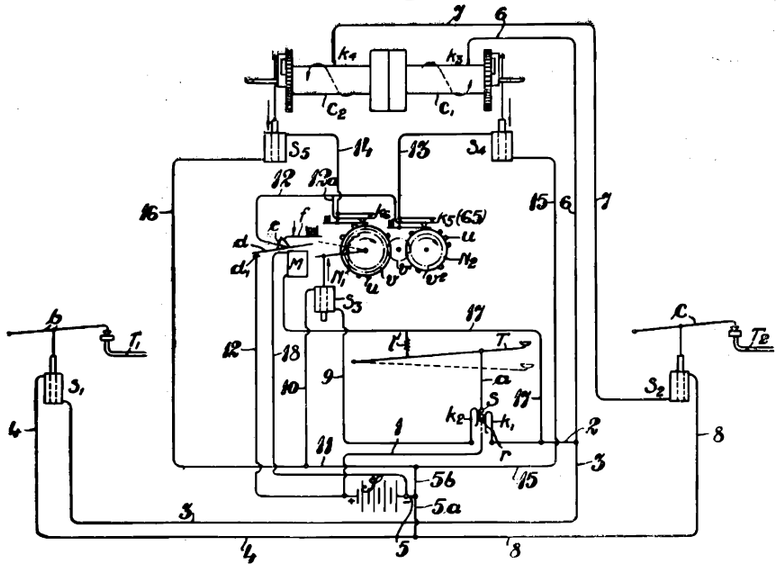


Fig.2

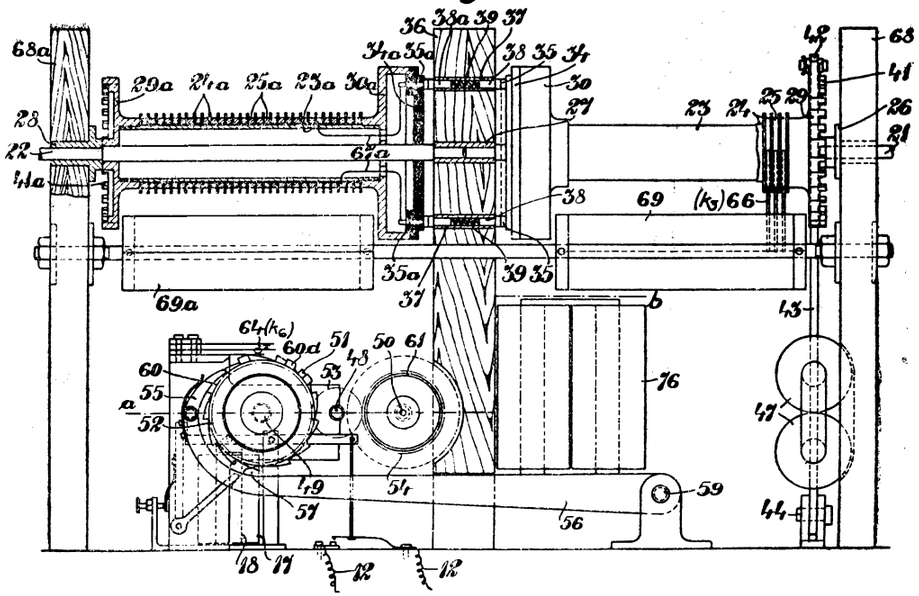


Fig. 3

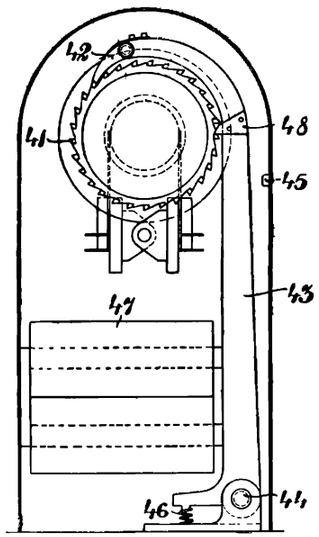
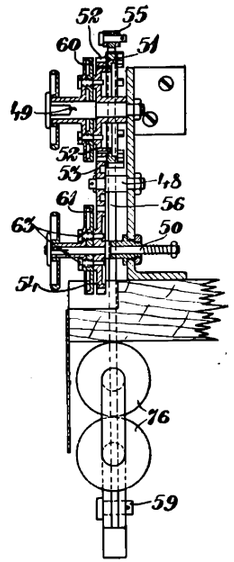


Fig. 4



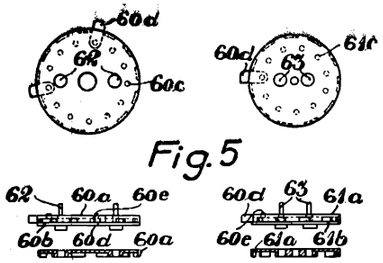


Fig. 5

Fig. 7

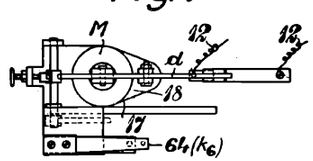
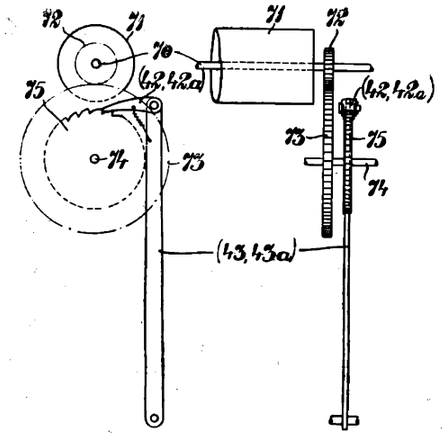


Fig. 6



Druk L. Bogusławskiego, Warszawa.