

5 marca 1928 r.

2

URZĄD PATENTOWY



B 411' 3/02

RZECZYPOSPOLITEJ POLSKIEJ

OPIS PATENTOWY

Nr 6916.

Kl. 15 g 20.

Aktiebolaget Cryptograph
(Stockholm, Szwecja).

Przyrząd do pisma szyfrowego.

Zgłoszono 26 września 1924 r.

Udzielono 7 lutego 1927 r.

Pierwszeństwo: 28 września 1923 r. (Szwecja).

Wynalazek niniejszy dotyczy przyrządu do pisma szyfrowego, odznaczającego się uproszczoną budową poszczególnych części, wskutek czego koszt jego wykonania jest mniejszy, wymiary również mniejsze, a obchodzenie się z nim — łatwiejsze, chociaż umożliwia on stosowanie szyfrów bardziej złożonych i o dłuższym okresie mutacyjnym, niż dotychczas.

Możliwie największa różnorodność różnych przedstawień części szyfrowych, stanowiących podstawę szyfru umożliwiającą zamianę poszczególnych znaków podczas szyfrowania, które tak w danym przyrządzie, jak i we wszystkich przyrządach mechanicznych muszą być okresowe, jest rzeczą najważniejszą dla zabezpieczenia ta-

jemnicy szyfru, która zależy od stosunku długości okresu szeregu mutacyjnego do długości szyfru, względnie tekstu do szyfrowania.

(Szeregiem mutacyjnym nazywa się tu szereg liczbowy, którego wyrazy określają odstęp pewnego normalnego szeregu „alfabetycznego” dostosowane do odstępów między następującymi po sobie znakami tekstu i szyfru).

Oprócz wyżej wymienionego stosunku, wpływa również na bezpieczeństwo szyfru mniejsza lub większa regularność, z jaką powtarza się szereg mutacyjny w szyfrze. Ponieważ, przy zastosowaniu normalnego szeregu o n znakach, szereg mutacyjny może posiadać tylko n różnych wyrazów, mu-

szą niektóre z nich powtarzać się kilkakrotnie w szeregu o długości okresu równej np. $x \cdot n$. Ponieważ może się zdarzyć, a nawet przy dłuższem szyfrowaniu musi się zdarzyć, że powtórzenie zespołu znaków w tekście nastąpi jednocześnie z powtórzeniem zespołu znaków szeregu mutacyjnego, można na zasadzie praw kryptologii, przy pomocy stosunku czynników i odpowiedniości liczb wysnuć wnioski prawdopodobne co do matematycznego układu szeregu mutacyjnego i w ten sposób ułatwić odczytanie szyfru osobie niepowołanej.

Pożądanem jest więc w każdym przyrządzie do pisma szyfrowego, aby poza wydłużeniem szeregu mutacyjnego, nie powtarzały się odstępów tej samej długości i podobnie rozmieszczone w okresie mutacyjnym, lecz aby odstępów te odpowiadały raczej liczbom pierwszym, lub liczbom, których czynniki pierwsze różnią się od czynników pierwszych liczb określających okresy ruchu mechanicznych części przyrządu, lub poszczególne części klucza.

Głównym celem niniejszego wynalazku jest osiągnięcie wyżej wskazanego wyniku, i poza tem dostarcza wynalazek przyrządu o częściach łatwo i dogodnie zamiennych.

Załączony rysunek przedstawia przykład wykonania przyrządu do pisma szyfrowego danego wynalazku.

Fig. 1 przedstawia przekrój podłużny przyrządu, fig. 2 — rzut poziomy, częściowo w przekroju, fig. 3 — przekrój poprzeczny uwidoczniający mechanizm napędowy, fig. 4 — łańcuch odpowiadający dowolnemu szeregowi liczbowemu.

W skrzynce 1 o przekroju czworokątnym obraca się oś 2, na której umocowane są dwa krążki 3 połączone ze sobą prętami 4. Na obwodzie krążków 3 umieszczone są w kierunku osiowym sztabki 5 zaopatrzone od strony zewnętrznej w normalne szeregi znaków (alfabety). Część przyrządu ogra-

niczona krążkami 3 oraz sztabkami 5 tworzy rodzaj bębna.

Na osi 2 umocowane jest również koło zapadkowe 6, o które zazębiać się może zapadka 8 przyciskana do koła 6 sprężyną 7. Zapadka 8 umieszczona jest na jednym z ramion dwuramiennej dźwigni 9 umocowanej obrotowo na osi 2, o której drugie ramie opiera się sprężyna 10 dążąca do utrzymania dźwigni 9 w położeniu wskazanem na fig. 3. Koło zapadkowe 6 posiada ilość zębów równą ilości sztabek 5 bębna.

Poza tem, na osi 2 obracać się może drugie koło zapadkowe 11, do piasty którego umocowane jest koło 12 zaopatrzone na obwodzie w trzpienie 15. Koło 12 przymocowane jest zapomocą naśrubka 13 oraz przeciwnaśrubka 14 i może być sporządzone z dwóch krążków. Na obwodzie umieszczone są w równej odległości otwory, w które mogą być włożone trzpienie 15.

Koło 12 posiada również kołnierz 16, na którym umieszczone są znaki, po jednym na każdy otwór przeznaczony dla trzpieni 15, których położenie może być odczytywane przez okienko 17 (fig. 1) w osłonie przyrządu. Koło 11 niezależne od zapadki 8 posiada ilość zębów, odpowiadającą ilości otworów przeznaczonych do trzpieni koła 12, która to ilość jest mniejsza od ilości zębów koła zapadkowego 6. Ilości te są w pewnym do siebie stosunku i tak dobrane, że przy zupełnem przesunięciu dźwigni 9 z położenia fig. 3, koło zapadkowe 6 obraca się o dwa zęby, podczas gdy koło zapadkowe 11 tylko o jeden ząb. Ruch dźwigni 9 jest ograniczony przez zetknięcie się zapadki 8 z trzpieniem 18. Koła zapadkowe 6 i 11 utrzymywane są w swych położeniach zapomocą sprężyny zatraskowej 19.

Trzpienie 15 koła 12 mogą obracać koło zębate 20, umieszczone na czopie 22 w łożysku 21. Na piaście tego koła osadzona jest część ośmiokątna 23, przenosząca ruch koła na łańcuch utworzony z ogniw

24a i 24b różnych wysokości i uszeregowanych według jakiegokolwiek szeregu liczbowego. Łańcuch ten obejmuje koło prowadzące 25. Za każdym przesunięciem przez trzpień 15 koła 20, przesuwa się łańcuch o długość jednego ogniwa naprzód. Naprzeciwko części 23, po drugiej stronie łańcucha znajduje się rolka 26 umocowana obrotowo na czopie umieszczonym na końcu ramienia 27 osadzonego na końcu osi 28 przechodzącej przez wystającą część łożyska 21. Na drugim końcu osi 28 znajduje się, tworząc z ramieniem 27 kąt prosty, ramię 29 połączone zapomocą dźwigni 30 ze strzemieniem 31, obejmującym oś 2 i obciążonym sprężyną 32 w ten sposób, aby rolka 26 była przyciśnięta do łańcucha 24a, 24b. Gdy rolka 26 opiera się o niskie ogniwo 24a łańcucha, zajmuje strzemie 31 położenie, oznaczone na fig. 3 linią całkowitą podczas gdy, w razie podniesienia rolki 26 przez wysokie ogniwo 24b, strzemie 31 zajmuje położenie wskazane linią przerywaną. W górnej ścianie przyrządu umieszczone jest okienko podłużne 34 wielkości odpowiadającej szerokości dwóch sztabek bębna. Strzemie 31 umieszczone jest przed tem okienkiem w ten sposób, że stosownie do swego położenia chwilowego zakrywa jedną lub drugą sztabkę, znajdującą się przed okienkiem 34, przyczem zewnętrzna jego strona zaopatrzona jest w alfabet (fig. 2).

Dla użycia przyrządu do szyfrowania, nastawia się bęben 3, 5 przy pomocy krążka 33 umieszczonego zewnątrz w pewne umówione położenie. Stosownie do umowy wyszukuje się na strzemieniu 31 literę odpowiadającą pierwszej literze tekstu oryginalnego przez naciskanie kilkakrotnie dźwigni 9. Litera znajdująca się naprzeciwko tej litery, na alfabecie bębna w okienku 34 będzie pierwszym znakiem szyfru. Następnie naciska się znów dźwignię 9 i wyzyskuje litery strzemienia odpowiadające drugiej literze tekstu, drugim zna-

kiem szyfru będzie litera alfabetu bębna, znajdująca się naprzeciwko tej litery w okienku 34. Czynność tę powtarza się następnie dla każdej litery tekstu oryginalnego.

Odszyfrowanie szyfru odbywa się w sposób odwrotny, gdyż poszczególne alfabety zajmują podczas tej czynności to samo położenie co podczas szyfrowania.

Porządek umieszczenia alfabetów na strzemieniu i na bębnie nie gra tu żadnej roli. Mogą być te alfabety umieszczone w przeciwnym porządku lub parami w porządku odwrotnym lub jak poniżej:

I. — 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.

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

lub

I. — 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

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

I — oznacza alfabet strzemienia, a II — bębna.

Zamiana znaków może nastąpić tak podczas szyfrowania jak i podczas odszyfrowania.

Jeżeli natomiast, alfabety strzemienia i bębna rozmieszczane są bez żadnego określonego porządku, należy zwrócić uwagę przy zamianie znaków na porządek tej zamiany. I tak, jeżeli podczas szyfrowania zamieniono znaki zaczynając od strzemienia, należy podczas odszyfrowywania rozpocząć zamianę od bębna, i odwrotnie.

Dla wyjaśnienia działania przyrządu w zależności od szeregu mutacyjnego służącego za podstawę do szyfrowania, przypuszcza się, dla uproszczenia, że alfabety bębna oraz strzemienia umieszczone są w przeciwnym porządku i przesunięte są

względem siebie o jedno miejsce w kierunku przeciwnym do obrotu bębna.

W powyżej opisanym przyrządzie może być oczywiście użyta dowolna ilość sztabek alfabetycznych, lecz z powodów łatwo zrozumiałych należy wybrać ilość nieparzystą. Można nie umieszczać niektórych sztabek, lub umieszczać sztabki bez alfabetu. W tym wypadku może się zdarzyć, że w okienku 34 nie ukazuje się żadna sztabka bębna, należy wtedy naciskać dźwignię 9 kilkakrotnie przed dokonaniem zamiany znaków.

W przytoczonym przykładzie przyjmuje się, że bęben zaopatrzony jest w 29 sztabek i że alfabety 7 i 12 są opuszczone tak, że przy nieruchomym strzemienu 31 i każdorazowym obrocie bębna o dwa przesunięcia, alfabety będą ukazywały się w okienku 34 w następującym porządku:

1, 3, 5, 9, 11, 13, 15, 17, 21, 23, 25, 27, 29, 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 24, 26, 28, 1, 3, 5, 9.

Co daje szereg mutacyjny równy temu szeregowi liczbowemu.

Jeżeli jednak strzemię 31, którego położenie wyjściowe może być np. to, które jest oznaczone linią ciągłą na fig. 2, zmieni swe położenie przy pierwszym ruchu bębna, to zamiast alfabetu 3 będzie widoczny w okienku 34 alfabet 4. Jeżeli przy dalszym przesunięciu bębna strzemię 31 pozostanie nieruchomym, alfabet 6 ukaże się w okienku, podczas gdy w razie przesunięcia się strzemięcia ukazałby się alfabet 5. Przesunięcia strzemięcia powodują więc ten sam skutek w stosunku do względnego ruchu strzemięcia i bębna, co obrót bębna naprzemian o dwa, trzy lub jedno przesunięcie. Ponieważ jednak nieobecność niektórych sztabek bębna może spowodować konieczność kilku dodatkowych przesunięć takowego, a działanie to nie jest stałe, lecz zależne od przypadkowego położenia łańcucha 24a, 24b, które to położenie z kolei zależne jest od przypadkowego położenia

i układu koła 16, więc przy wyzyskaniu tych warunków otrzymać można nadzwyczaj złożony szereg alfabetyczny zmienny, którego utworzenie nie da się ująć wzorem analitycznym, gdyż te same wyniki mogą być osiągnięte przez różne działania.

Tak np. odczytanie bezpośrednie jednego po drugim alfabetów 1 i 5 może być uskutecznione jednym z następujących sposobów:

a) obrót bębna z alfabetu 1 do alfabetu 3, puste miejsce w alfabecie 3, dalszy obrót bębna do alfabetu 5, przyczem łańcuch może być bądź nieruchomy, bądź zaopatrzony w dwa równe następujące po sobie ogniwa;

b) obrót bębna z alfabetu 1 do alfabetu 3, lecz łańcuch przesuwany z ogniwa wysokiego na niskie, co powoduje położenie odczytujące alfabetu 4, puste miejsce w alfabecie 4, dalszy obrót bębna do alfabetu 5, który zostaje odczytany, gdyż łańcuch przesuwany znów z ogniwa niskiego na wysokie;

c) obrót bębna z alfabetu 1 do alfabetu 3 z odczytaniem położenia alfabetu 2 wskutek przesunięcia się łańcucha z niskiego na wysokie ogniwo, puste miejsce w alfabecie 2, dalszy obrót bębna do alfabetu 5, które to położenie zostaje odczytane wskutek ponownego przesunięcia się łańcucha z wysokiego na niskie ogniwo.

Oczywiście, w szeregu mutacyjnym, w ten sposób otrzymanym, mogą powstać przerwy odpowiadające liczbom pierwszym, lecz nie koniecznie odpowiadające porządkowi odczytywania alfabetów, gdyż zależne są one nie tylko od dowolnych przesunięć alfabetów bębna względem siebie, lecz również i od rozmaitego układu tychże.

Przypuszczając, że bęben posiada nieparzystą ilość $2N + 1$ sztabek, że koło trzpieniowe 12 posiada S trzpieni, a łańcuch K ogniw, i że liczby te nie mają wspólnego dzielnika, długość okresu $P =$

$(2N + 1)$ S. K przesunąć, a jeżeli w bębnie znajduje się T miejsc pustych, wtedy $P = (2N + 1 - T)$ S. K zmian znaków, gdyż okresowość może powstać dopiero wtedy, gdy wszystkie części szyfrowe znajdą się znów względem siebie w swem położeniu wyjściowem.

Części, od których uzależniony jest układ szyfru, są w opisanym przyrządzie łatwo dostępne. W tym celu ścianki 34 i 36 skrzynki mogą być odejmowane, a część ścianki przy łańcuchu 24a, 24b jest umieszczona na zawiasach 37. Dla zmiany porządku sztabek alfabetycznych bębna, zdejmuje się krążek 33 i usuwa się ściankę 34, następnie wyjmuje się trzpień 35, za pomocą którego bęben umocowany jest na osi 2, można wtedy wyjąć z łatwością bęben. Dla zmiany trzpieni 15 koła 12, odkręca się nasrębki 14 i 13, wyjmuje ściankę 36 oraz koło 12.

Zastrzeżenie patentowe.

Przyrząd do pisma szyfrowego, posiadający kilka części regulujących wzajemnie swe położenie, z których jedna zaopa-

trzona jest w zespół normalnych szeregów znaków i obraca się o pewien określony kąt przy każdej czynności szyfrowania, znamienny szczególnem połączeniem czterech części, a mianowicie jednej części (31) wahającej się tam i zpowrotem, zaopatrzonej w normalny szereg znaków i umieszczonej w stosunku do drugiej części, w kształcie bębna (3, 5) zaopatrzonego w szeregi znaków, przed okienkiem do odczytywania tych znaków w ten sposób, że pozwala odczytywać jeden lub drugi szereg znaków bębna z jednej lub drugiej strony tej części (31) wahającej się, przyczem każdorazowe położenie tej części (31) zależne jest od trzeciej części (24a, 24b) odpowiadającej dowolnemu szeregowi liczbowemu i przesuwanej każdorazowo o pewną długość przez czwartą część (12, 15), odpowiadającą również pewnemu szeregowi liczbowemu i obracającą się przy każdej czynności szyfrowania o pewien kąt.

Aktiebolaget Cryptograph.

Zastępca: M. Skrzypkowski,
rzecznik patentowy.

