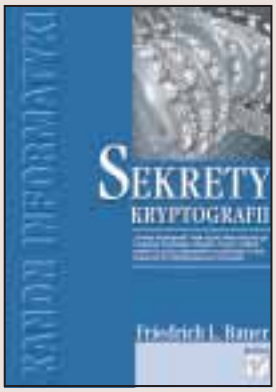
Sekrety kryptografii



Autor: John Paul Mueller
Tłumaczenie: Bartłomiej Garbacz
Tomasz Wasilewski
ISBN: 83-7197-960-6
Tytuł oryginału: Decrypted Secrets
Format: B5, stron: 536

Kryptologia, przez tysiąclecia nazywana „nauką tajemną", gwałtownie nabiera praktycznego znaczenia w systemach zabezpieczeń kanałów komunikacyjnych, baz danych i oprogramowania. Pełni ona ważną rolę w skomputeryzowanych systemach informacyjnych (systemy kluczy publicznych). W systemach komputerowych oraz sieciowych pojawia się coraz więcej możliwych zastosowań kryptologii związanych z prawami dostępu i ochroną plików źródłowych.

Pierwsza część niniejszej książki dotyczy kryptografii czyli tajnych kodów oraz sposobów ich. Część druga poświęcona jest kryptoanalizie, czyli procesowi deszyfrowania tajnych kodów; zawiera także porady dotyczące metod dostępu (assessing methods). Od czytelnika wymagana jest jedynie podstawowa wiedza z zakresu matematyki. Książka zawiera wiele ciekawych, zabawnych, a czasem osobistych opowieści z historii kryptologii, które sprawią, że zainteresuje ona także osoby nie zajmujące się kryptologią profesjonalnie.

„Sekrety kryptografii" to klasyka z dziedziny kryptologii. Niniejsze trzecie wydanie zostało poprawione i uzupełnione o wiele technicznych i bibliograficznych szczegółów.

„Najlepsza obecnie pozycja na temat kryptologii."
David Kahn, Cryptologia

„Książka niniejsza to niezbędna pozycja dla tych, którzy zajmują się kryptologią. Natomiast amatorom może posłużyć jako ważny leksykon, który w wielu przypadkach pokaże im, jak uczynić szyfry bezpieczniejszymi."
Arne Fransén, International Intelligence History Study Group

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 3.
Kroki szyfrowania: podstawienie proste

Wśród kroków szyfrowania wyróżnić można dwie duże klasy: *podstawienia* (*substitutions*) oraz *transpozycje* (*transpositions*). Są one szczególnymi przypadkami ogólnego kroku szyfrowania $V^{(n)} \longrightarrow W^{(m)}$. Rozpoczniemy od omówienia rodzajów podstawień, by następnie w rozdziale 6. zająć się transpozycjami.

Podstawienie proste (ang. *simple substitution*, niem. *Tauschverfahren* lub *Ersatzverfahren*) to podstawienie o monograficznych krokach szyfrowania $\chi_i \in M$:

$$\chi_i \colon V^{(1)} \longrightarrow W^{(m_i)}.$$

W przypadku monoalfabetycznym ustala się dowolny $\chi_s \in M$ i szyfrowanie przebiega według schematu $X = [\chi_s, \chi_s, \chi_s, \ldots]$. Zbiór M może wtedy być nawet jednoelementowy.

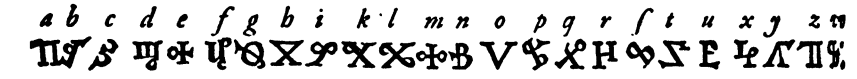
Zaczniemy od przypadku, w którym $m_i = 1$ dla wszystkich i.

3.1. Przypadek $V^{(1)} \longrightarrow W$ (jednodzielne podstawienia proste)

Przypadek $V^{(1)} \longrightarrow W$ związany jest z *jednodzielnym podstawieniem prostym*, zwanym w skrócie podstawieniem prostym (ang. *unipartite simple substitution*, franc. *substitution simple ordinaire*).

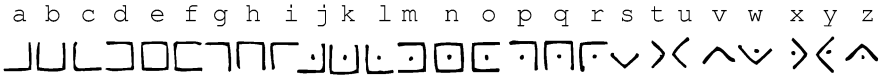
3.1.1. $V \longrightarrow W$**, heterogeniczne szyfrowanie bez homofonów i wartości zerowych.** Mamy tu do czynienia z przypadkiem podstawowym. Jako W często służy alfabet dziwnie wyglądających, niezwykłych grafemów; przykładów można szukać w Tajlandii, Persji, Etiopii koptyjskiej i innych miejscach. Znaków takich używał Giovanni Battista Porta (Giambattista Della Porta, 1535–1615) na swoim dysku szyfrującym (rysunek 23., patrz także rysunek 30.). Także Karol Wielki używał znaków tego typu (rysunek 24.), podobnie jak uczona i mistyczka Hildegarda von Bingen (1098–1179). W tym miejscu trzeba wspomnieć

Rysunek 23. Dysk szyfrujący Giovanniego Battisty Porty (1563)

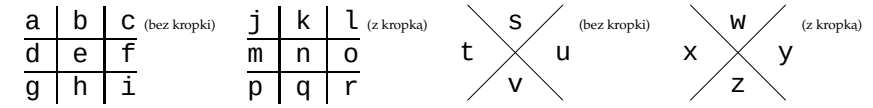


Rysunek 24. Tajemne znaki Karola Wielkiego

o szyfrze wolnomularzy (*Freemasons' cipher*). Jego źródeł szukać należy w starożytnym szyfrze *pigpen*. Współcześnie przyjmuje on następującą postać:



Szyfr ten można łatwo opanować dzięki diagramom:



Po złamaniu tego szyfru przez angielski wydział deszyfrowania w 1728 roku, car Piotr Wielki zaczął używać (oprócz nomenklatorów) heterogenicznego podstawienia $V \longrightarrow W$ o dziwacznym alfabecie tekstu zaszyfrowanego.

Znany pisarz Edgar Allan Poe wykorzystał w swoim opowiadaniu *Złoty żuk* banalny alfabet zwykłych czcionek drukarskich (podrozdział 15.10.1.).

Do klasy tej należy także szyfr księgarski przeznaczony do szyfrowania cen i dat, stanowiący różnowartościowe odwzorowanie $Z_{10} \longrightarrow Z_{26}$, tworzone na podstawie hasła (szyfr z frazą kluczową, *key-phrase cipher*). Jako przykład niech posłuży krok szyfrowania z hasłem `MILCHPROBE` ['próbka mleka'],

1	2	3	4	5	6	7	8	9	0
M	I	L	C	H	P	R	O	B	E,

przez wiele lat używany w Niemczech do znakowania daty pakowania masła. Podobnie w marynarce brytyjskiej, przy odczycie kodów ENIGMY, liczby były czasem reprezentowane za pomocą liter:

1	2	3	4	5	6	7	8	9	0
Q	W	E	R	T	Z	U	I	O	P .

3.1.2. $V^{(1)} \longrightarrow W$**, heterogeniczne szyfrowanie z homofonami i wartościami zerowymi.** Homofony znaleźć można w źródłach muzułmańskich, np. *al-Qalqashandi* z roku 1412, a także w szyfrze używanym przez Księstwo Mantui w 1401 roku w korespondencji z Simeonem de Crema. Samogłoski — zazwyczaj występujące najczęściej — opatrywano homofonami, co stanowiło pierwszy przejaw przywiązywania wagi do częstości występowania znaków. Dodatkowo zbiór W rozszerzano o cyfry. Wprowadzenie homofonów praktycznie wymusza dodanie wartości zerowych; w przeciwnym wypadku homofony można z łatwością rozpoznać na podstawie stałego wzorca liter, otaczających je w często występujących wyrazach.

Metoda korzystająca z homofonów, używana po dzień dzisiejszy, to tak zwany *szyfr książkowy*: z pewnej niewinnie wyglądającej książki, której identyczne egzemplarze posiadają zarówno nadawca, jak i odbiorca wiadomości, wybiera się kolejne litery tekstu jawnego; odpowiednie adresy postaci (strona x, wiersz y, znak z) tworzą grupę szyfru (x-y-z).

Wybierając za książkę niniejszy egzemplarz, słowo „ssak" można zaszyfrować jako: 25-6-3, 33-12-30, 30-1-9, 22-21-6.

3.2. Przypadek szczególny $V \longleftrightarrow V$ (permutacje)

W przypadku wzajemnie jednoznacznego odwzorowania $V \longleftrightarrow W$, jak w przykładach z podrozdziału 3.1.1., W jest nazywany N-znakowym *alfabetem nieuporządkowanym* tekstu zaszyfrowanego (ang. *mixed alphabet*; franc. *alphabet désordonné*, *alphabet incohérent*; niem. *umgeordnetes Geheimtextalphabet*), który odpowiada *alfabetowi standardowemu* tekstu jawnego (ang. *standard alphabet*; franc. *alphabet ordonné*; niem. *Standard-Klartextalphabet*) V, również składającemu się z N znaków.

W celu zdefiniowania podstawienia wystarczy utworzyć w pewien sposób listę odpowiadających sobie par znaków tekstu jawnego i kryptogramu, np. dla $V \doteq W = Z_{26}$ (zasady użycia w notacji małych liter oraz wersalików opisano w podrozdziale 2.5.4.):

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

Podczas szyfrowania dużo wygodniej jest oczywiście mieć znaki tekstu jawnego uporządkowane w alfabet standardowy (tekstu jawnego); daje to alfabet nieuporządkowany tekstu zaszyfrowanego:

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
R	A	W	E	N	Y	G	F	M	P	T	B	S	D	J	Q	V	K	O	U	H	I	C	Z	X	L

W matematyce zwyczajowo stosuję się taką notację podstawień. Jednak podczas deszyfrowania lepiej mieć znaki tekstu zaszyfrowanego uporządkowane w alfabet standardowy (tekstu zaszyfrowanego), co daje nieuporządkowany alfabet tekstu jawnego:

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

Z nową sytuacją mamy do czynienia w endomorficznym przypadku $V \triangleq W$. W szczególności wzajemnie jednoznaczne odwzorowanie $V \longleftrightarrow V$ jest wówczas permutacją V. Permutację $V \longleftrightarrow V$ można zrealizować w modelu elektrycznym poprzez wymianę (ang. *interchange*; niem. *Umstecken*) N przewodów w wiązce.

Do zapisu permutacji matematycy używają, oprócz notacji podstawień, także notacji cyklicznej:

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

w której trzeba zrezygnować z rozróżnienia pomiędzy małymi literami a wersalikami. Podczas szyfrowania przechodzimy cyklicznie od znalezionego znaku tekstu jawnego do następnego znaku; podczas deszyfrowania — cyklicznie do poprzedniego znaku. Cykle długości 1 (1-cykle) są często pomijane — my nie będziemy się do tego stosować.

3.2.1. Permutacje samoodwrotne. Najstarsze źródła (pomijając Egipt, do którego powrócimy przy omawianiu kodów) opisują samoodwrotną (inwolutywną) permutację V: indyjska *Kāma-sūtra*, napisana przez Vātsyāyanę, zawiera opis tajnego pisma traktowanego jako jedna z sześćdziesięciu czterech sztuk; *Mūladevīya* oznacza proces szyfrowania i deszyfrowania, który stanowi odbicie (*inwolucję*):

$$V \xleftrightarrow{2} V : \updownarrow \begin{matrix} \texttt{a kh gh c t ñ n r l y} \\ \texttt{k g n ṭ p ṇ m ṣ s ś} \end{matrix}.$$

Pozostałe znaki nie są zmieniane, więc permutacja nie jest *ściśle samoodwrotna, permutacja* (*properly self-reciprocal*). O alfabetach tekstu jawnego i tekstu zaszyfrowanego permutacji samoodwrotnej mówi się, że są względem siebie *wzajemnie odwrotne*.

W hebrajskim Starym Testamencie użyto podstawienia bustrofedonicznego (*boustrophedonic substitution*) zwanego *Athbash* — aczkolwiek nie w celu szyfrowania — które w łacińskim alfabecie $V = Z_{20}$ można odczytać jako

$$V \xleftrightarrow{2} V : \updownarrow \begin{matrix} \texttt{a b c d e f g h i l} \\ \texttt{z v t s r q p o n m} \end{matrix}.$$

Takie podstawienie korzysta z alfabetu odwróconego (inwersyjnego). W przypadku inwolucji

$$V \xleftrightarrow{2} V : \updownarrow \begin{matrix} \texttt{a b c d e f g h i l m} \\ \texttt{a z v t s r q p o n m} \end{matrix}$$

Charles Eyraud mówi o *alfabecie dopełniającym* (ang. *complementary alphabet*; franc. *alphabet complémentaire*) — patrz podrozdział 5.6. Permutacja ta nie jest jednak ściśle samoodwrotna: /a/ i /m/ pozostają niezmienione.

Oczywista jest także samoodwrotność alfabetu przesuniętego, na przykład hebrajskiego *Albam*, użytego w 1589 roku przez Argentich, gdzie $V = Z_{20}$:

$$V \xleftrightarrow{2} V : \updownarrow \begin{matrix} \texttt{a b c d e f g h i l} \\ \texttt{m n o p q r s t v z'} \end{matrix}$$

czy też alfabetu Giovanniego Battisty Porty z 1563 roku (patrz rysunek 53.) przy $V = Z_{22}$:

$$V \overset{2}{\longleftrightarrow} V :\updownarrow \begin{matrix} \texttt{a b c d e f g h i l m} \\ \texttt{n o p q r s t v x y z} \end{matrix}.$$

Poniższy przykład przedstawia najogólniejszy przypadek bustrofedoniczy z użyciem hasła ($V = Z_{26}$):

$$V \overset{2}{\longleftrightarrow} V :\updownarrow \begin{matrix} \texttt{a n g e r s b c d f h i j} \\ \texttt{z y x w v u t q p o m l k} \end{matrix}.$$

Oprócz zalety zwięzłej notacji inwolucje posiadają cechę, którą niektórzy uważają za ogromnie ważną — pokrywanie się kroków szyfrowania i deszyfrowania.

Przy wykorzystaniu notacji cyklicznej, pięć ostatnich przykładów permutacji można zapisać jako:

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

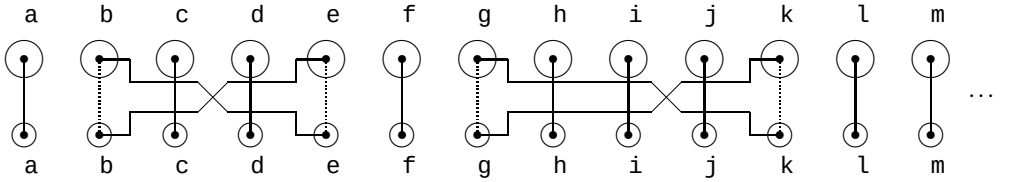
(Cykle uporządkowano w kolejności alfabetycznej ich pierwszych elementów).

Ściśle samoodwrotne permutacje nie posiadają 1-cykli, co oznacza występowanie w nich wyłącznie 2-cykli (zamiany, *swaps*). Stanowią one cel ataków kryptoanalitycznych (podrozdział 14.1.), które okazują się nieskuteczne, jeśli niektóre z cykli są 1-cyklami (cykle *female*).

W przypadku alfabetu binarnego $V = Z_2$ jedyną nietrywialną permutacją jest zamiana:

$$V \overset{2}{\longleftrightarrow} V :\updownarrow \begin{matrix} \texttt{O} \\ \texttt{L} \end{matrix}.$$

3.2.2. Komutator. W implementacjach elektrycznych inwolucje można zrealizować przez zamianę par przewodów, łatwą do wykonania przy zastosowaniu dwustronnych wtyków (rysunek 25.). W ten sposób zrealizowano inwolucje w centralce (ang. *plugboard*; niem. *Steckerbrett*) maszyny ENIGMA.



Rysunek 25. Permutacja samoodwrotna zrealizowana przy użyciu komutatora złożonego z par dwustronnych wtyków, przerywających bezpośrednie połączenia

Liczba inwolucji $d(k, N)$ zależy od N oraz od liczby k użytych koncentrycznych złącz wtykowych (*cinch plugs*):

$$d(k,N) = \frac{N!}{2^k \cdot (N-2k)! \cdot k!} = \binom{N}{2k} \cdot \frac{(2k)!}{2^k k!} = \binom{N}{2k} \cdot (2k-1)!!, \quad \text{gdzie}$$
$$(2k-1)!! = (2k-1) \cdot (2k-3) \cdot \cdots \cdot 5 \cdot 3 \cdot 1 = \frac{(2k)!}{2^k k!}.$$

Permutacje ściśle samoodwrotne („prawdziwe" inwolucje) istnieją tylko dla parzystych $N = 2\nu$. Liczba $d\left(\frac{N}{2}, N\right)$ wszystkich permutacji ściśle samoodwrotnych wynosi (przy błędzie względnym mniejszym niż 10^{-3} dla $N \geqslant 6$)

$$d\left(\frac{n}{2}, N\right) = (N-1)!! = (N-1) \cdot (N-3) \cdot \cdots \cdot 5 \cdot 3 \cdot 1 = \frac{(2\nu)!}{\nu! 2^\nu} \approx \frac{\sqrt{(2\nu)!}}{\sqrt[4]{\pi \cdot (\nu + \frac{1}{4})}}.$$

Przybliżenie to należy traktować jako dobre górne oszacowanie wartości $(N-1)!!$. Dla ustalonego N, wartość $d(k, N)$ osiąga maksimum przy $k = \left\lceil \nu - \sqrt{(\nu+1)/2} \right\rceil$:

$$d(5,26) \approx 5{,}02 \cdot 10^9, \quad d(6,26) \approx 1{,}00 \cdot 10^{11}, \quad d(7,26) \approx 1{,}31 \cdot 10^{12},$$
$$d(8,26) \approx 1{,}08 \cdot 10^{13}, \quad d(9,26) \approx 5{,}38 \cdot 10^{13}, \quad d(10,26) \approx 1{,}51 \cdot 10^{14},$$
$$d(11,26) \approx 2{,}06 \cdot 10^{14}, \quad d(12,26) \approx 1{,}03 \cdot 10^{14}, \quad d(13,26) \approx 7{,}91 \cdot 10^{12},$$
$$\text{zaś} \quad d(3,10) = 3\,150, \quad d(4,10) = 4\,725, \quad d(5,10) = 945.$$

Zauważmy, że $\log_2 d(10,26) \approx 47{,}10$ [bit], $\log_2 d(11,26) \approx 47{,}55$ [bit], $\log_2 d(12,26) \approx 46{,}55$ [bit], zaś dla wszystkich inwolucji $\log_2 \sum_{i=1}^{13} d(k,26) \approx \log_2 5{,}33 \cdot 10^{14} \asymp 48{,}92$ [bit].

W ENIGMIE I *Reichswehry* z 1930 roku do połączenia komutatora realizowano początkowo za pomocą sześci dwustronnych wtyków dwuprzewodowych, zaś w ENIGMIE *Wehrmachtu* od początku, czyli od 1 października 1936 roku — za pomocą od pięciu do ośmiu wtyków; od 1 stycznia 1939 roku — od siedmiu do dziesięciu wtyków, zaś od 19 sierpnia 1939 roku — za pomocą dziesięciu wtyków.

3.2.3. Permutacje monocykliczne. Zwięzła notacja może także służyć do opisu permutacji monocyklicznej, której rząd wynosi N. Oto na przykład, dla $N = 20$, cykl standardowego alfabetu Z_{20}:

$$V \xleftrightarrow{N} V : (\mathtt{a\ b\ c\ d\ e\ f\ g\ h\ i\ l\ m\ n\ o\ p\ q\ r\ s\ t\ v\ x})$$

i jego trzeciej potęgi

$$V \xleftrightarrow{N} V : (\mathtt{a\ d\ g\ l\ o\ r\ v\ b\ e\ h\ m\ p\ s\ x\ c\ f\ i\ n\ q\ t}).$$

W notacji podstawień przyjmą one postać:

$$V \xleftrightarrow{N} V : \begin{matrix} \mathtt{a\ b\ c\ d\ e\ f\ g\ h\ i\ l\ m\ n\ o\ p\ q\ r\ s\ t\ v\ x} \\ \mathtt{B\ C\ D\ E\ F\ G\ H\ I\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ V\ X\ A} \end{matrix}$$

oraz

$$V \xleftrightarrow{N} V : \begin{matrix} \mathtt{a\ b\ c\ d\ e\ f\ g\ h\ i\ l\ m\ n\ o\ p\ q\ r\ s\ t\ v\ x} \\ \mathtt{D\ E\ F\ G\ H\ I\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ V\ X\ A\ B\ C} \end{matrix}.$$

Z tego drugiego kroku szyfrowania korzystał według Swetoniusza Juliusz Cezar, który szukając potrzebnej litery przesuwał się po prostu w alfabecie o trzy pozycje do przodu. Jego następca August, pod wieloma względami podrzędny w stosunku do Cezara, używał pierwszego z podanych kroków szyfrowania (być może dlatego, że niekoniecznie umiał liczyć do trzech); Swetoniusz twierdził także, że zastępował on /x/ przez AA.

Każda potęga cyklu alfabetu standardowego daje w wyniku alfabet CAESAR. Powrócimy do tej kwestii w rozdziale 5. (dodawanie CAESAR). Należy jednak zauważyć, że choć oba powyższe kroki szyfrowania są rzędu dwadzieścia, to ich drugie potęgi są już tylko rzędu dziesięć, a potęgi dziesiąte — rzędu dwa (są to więc opisane wcześniej inwolucje). $(N-1)$-ta potęga jest odwrotnością potęgi pierwszej i stanowi krok deszyfrowania.

Monoalfabetyczne podstawienie kroku szyfrowania CAESAR wprowadzono w 1915 roku w armii rosyjskiej po tym, jak okazało się nierealne oczekiwanie, że sztaby będą w stanie używać czegoś bardziej skomplikowanego. Dla szefów służb kryptoanalitycznych, pruskiego (Ludwig Deubner) i austriackiego (Hermann Pokorny), mile prostą sprawą było deszyfrowanie tych wiadomości.

Ze swej natury ścieżka na dysku, obręcz płuczki lub pasek materiału zamknięty w kształt pierścienia mogą służyć jako reprezentacja pełnego cyklu. Narzędzia takie były szeroko stosowane. W sposób szczególny wykorzystali je (podrozdział 7.5.3.) Thomas Jefferson i Étienne Bazeries. q-tą potęgę permutacji monocyklicznej otrzymuje się przez cykliczne liczenie krokami co q znaków.

3.2.4. Alfabety nieuporządkowane. Do przedstawiania niesamoodwrotnych i niecyklicznych permutacji $V \longleftrightarrow V$ w najogólniejszym przypadku alfabetu nieuporządkowanego (ang. *mixed alphabet*; franc. *alphabet désordonné*; niem. *permutieres Alphabet*) zazwyczaj stosuje się notację podstawień:

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

Zwięzła notacja cykliczna także jest przydatna. Ukazuje ona rozkład powyższej permutacji

$$V \longleftrightarrow V: \texttt{(a s n h y x w v q l f i)(b e r m g t o j)(c)(d u p k)(z)}$$

na jeden 12-cykl, jeden 8-cykl, jeden 4-cykl oraz dwa 1-cykle (podział cykliczny $12+8+4+1+1$).

3.2.4.1. Dodatkowe alfabety nieuporządkowane otrzymuje się przez cykliczne przesunięcie jednego z dwóch wierszy w notacji podstawień (przesunięty alfabet nieuporządkowany; ang. *shifted mixed alphabet*; franc. *alphabet désordonné paralléle*; niem. *verschobenes permutieres Alphabet*):

$$V \longleftrightarrow V: \begin{matrix} \texttt{a b c d e f g h i j k l m n o p q r s t u v w x y z} \\ \texttt{E C U R I T Y A B D F G H J K L M N O P Q V W X Z S} \end{matrix}'$$

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

W notacji cyklicznej mają one postać:

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

3.2.4.2. Iterowanie podstawień, zwane także podnoszeniem do wyższej potęgi, tworzy potęgi alfabetu nieuporządkowanego, np. druga potęga przedstawionego wyżej podstawienia *SECURITY…* daje podstawienie

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

o wszystkich cyklach długości parzystej rozdzielonych na pół; w notacji podstawień:

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

Przesuwanie z jednej strony, a podnoszenie do potęgi z drugiej, w ogólnym przypadku nie dają tego samego rezultatu; są to dwie krańcowo różne metody tworzenia rodziny co najwyżej N (a czasem mniejszej liczby) alfabetów towarzyszących (rozdział 7.).

3.2.5. Alfabety uzyskiwane z haseł. Przedstawione wyżej przykłady ukazały już sposób konstruowania (endomorficznego) podstawienia prostego $V \longleftrightarrow V$ za pomocą hasła (ang. *password*; franc. *mot-clef*; niem. *Kennwort*, *Losung*): zazwyczaj mnemonicznego klucza lub wyrażenia kluczowego. W klasycznej metodzie używa się słowa z V, zapisuje się jego znaki bez powtórzeń i uzupełnia w kolejności alfabetycznej znakami niewystępującymi w haśle. Metodę tę datuje się na okolice roku 1580, kiedy to użył jej Giovanni Battista Argenti. Był to standard kryptologiczny jeszcze w XX wieku[1].

Jednakże konstrukcja taka nie jest bezpieczna: prostą sprawą może okazać się odgadnięcie brakującego fragmentu hasła (wszakże najczęściej występujące samogłoski /e/ oraz /a/ są zawsze zastępowane literami z hasła, jeśli ma ono długość 5 lub więcej znaków). Małym pocieszeniem jest fakt, że hasło nie będzie wymagać istotnego uzupełnienia.

Z tego względu bardziej wymyślne metody korzystają z przestawienia hasła, na przykład przez zapisanie go w wierszach i odczytywanie w kolumnach (metoda Charlesa Wheatstone'a z 1854 roku, transpozycja opisana szczegółowo w podrozdziale 6.2.):

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

Otrzymany tym sposobem alfabet

```
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
S A L X E B M Z C D N U F O R G P I H Q T J V Y K W
```

w notacji cyklicznej przedstawia się jako

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

z 1-cyklem (e).

W kolejnej metodzie także kolumny po stronie tekstu jawnego wypełniane są w alfabetycznej kolejności liter hasła; w bieżącym przykładzie jest to kolejność:

[1] Dopuszczenie powtórzeń jest rzeczą złą, gdyż prowadzi do polifonów, jak np. w szyfrze z frazą kluczową

```
a b c d e f g h i j l m n o p q r s t u v x y z
L E G O U V E R N E M E N T P R O V I S O I R E
```

oraz zmniejsza liczbę elementów zbioru znaków tekstu zaszyfrowanego (w naszym przypadku do 13 znaków; np. $\{\texttt{b}, \texttt{g}, \texttt{j}, \texttt{m}, \texttt{z}\} \longmapsto \texttt{E}$).

trzecia, druga, szósta, piąta, pierwsza, siódma, czwarta, ósma kolumna,

co daje w rezultacie:

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

Ostatecznie otrzymujemy alfabet:

```
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
C D N E B M Z I H Q R G P S A L X T J V U F O Y K W
```

który w notacji cyklicznej będzie miał postać

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

Metoda ta może być także wykorzystana do konstruowania cykli. Zdanie *„évitez les courants d'air"* [„unikaj przeciągów"] (Bazeries, podrozdział 7.5.3.) tworzy cykl:

$$V \xleftrightarrow{\mathrm{N}} V: \quad (\mathtt{e\ v\ i\ t\ e\ z\ l\ s\ c\ o\ u\ r\ a\ n\ d\ b\ f\ g\ h\ j\ k\ m\ p\ q\ x\ y}).$$

3.2.6. Liczba odwzorowań. Poniższa tabela przedstawia liczbę $Z(N)$ możliwych alfabetów $V \longleftrightarrow V$ dla $N = 26$, $N = 10$ i $N = 2$:

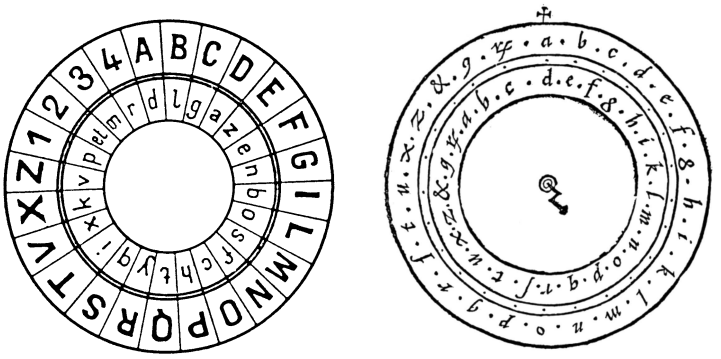
Liczba permutacji	$Z(N)$	$Z(26)$	$Z(10)$	$Z(2)$
razem	$N!$	$4{,}03 \cdot 10^{26}$	3 628 800	2
monocykliczne	$(N-1)!$	$1{,}55 \cdot 10^{25}$	362 880	1
inwolucje razem	$\approx N \cdot (N!)^{\frac{1}{2}}$	$5{,}33 \cdot 10^{14}$	9 496	2
ścisłe inwolucje	$\approx (N!)^{\frac{1}{2}}$	$7{,}91 \cdot 10^{12}$	945	1
uzyskane z sensownych haseł (wyrazy mnemoniczne)		$10^4 \ldots 10^6$		

3.2.7. Dyski szyfrujące i paski szyfrujące. Przy mechanizacji procesu podstawiania, ustalony związek znaków tekstu jawnego i znaków tekstu zaszyfrowanego, podobnie jak w notacji podstawień, można osiągnąć dzięki użyciu cylindra lub paska materiału. Dwa okienka pozwalają w danej chwili widzieć tylko dwa odpowiadające sobie znaki. Okienka można ustawić tak, że główny szyfrant widzi jedynie tekst jawny, zaś operator — tylko okienko z bieżącym znakiem kryptogramu, przy czym nie może zrozumieć treści szyfrowanego komunikatu (podrozdział 7.5.2., maszyna Gripenstierny, rysunek 54.).

Wyboru jednego z N przesuniętych alfabetów towarzyszących dokonać można, jeśli jedno z okienek jest ruchome. Inna możliwość to przesuwanie alfabetu tekstu jawnego względem alfabetu tekstu zaszyfrowanego. Prowadzi to do użycia dwóch dysków (rysunek 26.) lub dwóch pasków (rysunek 27.). W tym drugim przypadku konieczne jest powtórzenie jednego z alfabetów (duplikacja).

Dyski szyfrujące (ang. *cipher disk*; franc. *cadran*; niem. *Chiffrierscheibe*), mechaniczne urządzenia służące do ogólnego podstawiania przy użyciu przesuniętych alfabetów nieuporządkowanych, zostały opisane już w 1466 roku przez Leona Battistę Albertiego[2] (patrz rycina B). Suwaki szyfrujące (ang. *cipher slide*; franc. *reglette*; niem. *Chiffrierschieber*) były

[2] Na ilustracji Albertiego, w odróżnieniu od współczesnej konwencji, wielkie litery oznaczają tekst jawny, zaś



Rysunek 26. Dysk szyfrujący Leona Battisty Albertiego (według Langego i Soudarta, 1935)

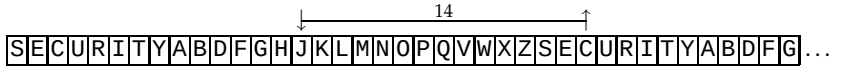
używane w Anglii czasów elżbietańskich około roku 1600. W wieku XIX nazywano je suwakami *Saint-Cyr* (od nazwy słynnej francuskiej akademii wojskowej). Takie samo przeznaczenie mają pręty szyfrujące (ang. *cipher rods*; franc. *bâtons*; niem. *Chiffrierstäbchen*).

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	d	c	e	f	g	h	i	j	k	l	m	...
S	E	C	U	R	I	T	Y	A	B	D	F	G	H	J	K	L	M	N	O	P	Q	V	W	X	Z															

Rysunek 27. Suwak szyfrujący z podwojonym alfabetem tekstu jawnego

3.2.8. Realizacja cykli za pomocą okienek. Mechanizacja permutacji monocyklicznej może bazować także na notacji cyklicznej. Cykl znaków umieszcza się na cylindrze lub suwaku (w tym drugim przypadku pierwszy znak trzeba powtórzyć na końcu). Sąsiadujące okienka pozwalają widzieć w danej chwili tylko dwa znaki, z których lewy jest znakiem tekstu jawnego, zaś prawy odpowiednim znakiem kryptogramu.

Wyboru spośród (maksymalnie N) towarzyszących potęg alfabetu nieuporządkowanego można dokonywać, o ile odległość między okienkami da się zmieniać. W przypadku suwaka konieczne jest powtórzenie całego cyklu. q-tą potęgę permutacji monocyklicznej otrzymuje się, kiedy okienka dzieli odległość q znaków (rysunek 28. dla $q = 14$).



Rysunek 28. Suwak szyfrujący z okienkami do generowania potęg alfabetu

3.3. Przypadek $V^{(1)} \longrightarrow W^m$ (wielodzielne podstawienia proste)

3.3.1. $m = 2$**, dwudzielne podstawienie proste** $V^{(1)} \longrightarrow W^2$**.** Podstawienia korzystające z bigramów (*bigram substitutions*, podstawienia dwudzielne) były znane już w starożytności. Polibiusz opisał piątkowe ($|W| = 5$) podstawienie dwudzielne dla liter greckich. We współczesnej formie dwudzielnego podstawienia prostego alfabet Z_{25} wpisuje się w tabelę o wymiarach 5×5:

małe litery — kryptogram. Znak /et/ najprawdopodobniej oznacza symbol &. Początkową pozycję dysku wyznacza się ustawiając obok siebie literę klucza, na przykład D i znak tekstu jawnego, na przykład /a/.

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

lub

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

Odszyfrowanie semagramu tekstowego

3 3 5 1 5 1 4 1 2 3 4 3 3 3 5 1 4 5 1 2 4 3 2 4 1 1 3 4 3 4 1 1 3 4 3 4 4 2 3 3 1 1 4 4 4 2 4 3 3 3

z podrozdziału 1.2., rysunek 3., przeprowadzone za pomocą prawego kwadratu Polibiusza, prowadzi do następującego tekstu jawnego:

`needmoneyforassassination`
[potrzebne pieniądze na zabójstwo].

Choć Polibiusz opisał sposób reprezentowania liczb 1–5 za pomocą pochodni, to w bardziej współczesnych czasach używano sygnałów stukania. szczególny szyfr $Z_{25} \longrightarrow Z_5 \times Z_5$ przedstawiony powyżej jest powszechnie znanym, prawdziwie międzynarodowym szyfrem stukania, używanym w więzieniach od Alcatraz po Ploetzensee zarówno przez przestępców, jak i więźniów politycznych. Zwykła szybkość transmisji wynosi od 8 do 15 słów na minutę.

W carskiej Rosji taki szyfr stukania (z rosyjskim alfabetem wpisanym w kwadrat 6×6) również był powszechnie znany i wraz z anarchistami rosyjskimi przywędrował do Europy Zachodniej jako część szyfru nihilistów (podrozdział 9.4.5.); używano go także w sensie steganograficznym (podrozdział 1.2.). Arthur Koestler w *Sonnenfinsternis*, a także Aleksander Sołżenicyn w *Archipelagu Gułag*, opisali jego użycie w Związku Sowieckim.

Konstrukcja alfabetu zazwyczaj korzysta z hasła, które zostaje wpisane wiersz po wierszu, a całość uzupełnia się pozostałymi znakami. Hrabia Honoré de Mirabeau, francuski rewolucjonista z XVIII wieku, używał tej metody w swojej korespondencji z markizą Sophie de Monnier — używał jej również steganograficznie, dodając jako wartości zerowe znaki: `6`, `7`, `8`, `9`, `0`.

System ADFGVX, opracowany przez Fritza Nebela (1891–1967) i stosowany w 1918 roku w transmisji radiowej na niemieckim froncie zachodnim dowodzonym przez generała kwatermistrza Ericha Ludendorffa, pracował przy $|W| = 6$ (alfabet tekstu zaszyfrowanego Z_6 — patrz podrozdział 2.5.2.), w oparciu o tabelę

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

Korzysta się także z tabel prostokątnych. Giovanni Battista Argenti około roku 1580 zastosował następujący schemat (przy $W = Z_{10}$):

	0	1	2	3	4	5	6	7	8	9
1	p	i	e	t	r	o	a	b	c	d
2	f	g	h	l	m	n	q	s	u	z

w którym po raz pierwszy użyte zostało hasło.

Podstawienie dwudzielne pozostawia na ogół dużo miejsca dla homofonów:

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

W przykładzie tym znak /0/ może służyć jako wartość *null*. Znak zera, początkowo nazywany *nulla ziffra*, wciąż nie wszędzie jest poważnie brany pod uwagę.

Najlepiej jest, kiedy homofony wyrównują częstość występowania znaków w kryptogramie. Skoro w języku angielskim litery /e/, /t/, /a/, /o/, /n/, /i/, /r/, /s/, /h/ występują z łączną częstością około 70%, równomierny rozkład osiąga się przy

	1	2	3	4	5	6	7	8	9	
4, 5, 6, 7, 8, 9, 0	e	t	a	o	n	i	r	s	h	71,09%
2, 3	b	c	d	f	g	j	k	l	m	19,46%
1	p	q	u	v	w	x	y	z		9,45%.

W innej metodzie używa się 4-literowego hasła, które decyduje o początkach cykli: (**00**...24), (**25**...49), (**50**...74), (**75**...99) przy definiowaniu szyfru homofonicznego (dla $V = Z_{25}$ i $W = Z_{10}^2$), np. z hasłem *KILO*:

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
K	16	17	18	19	20	21	22	23	24	**00**	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
I	42	43	44	45	46	47	48	49	**25**	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
L	65	66	67	68	69	70	71	72	73	74	**50**	51	52	53	54	55	56	57	58	59	60	61	62	63	64
O	87	88	89	90	91	92	93	94	95	96	97	98	99	**75**	76	77	78	79	80	81	82	83	84	85	86

Dziesiętny ($|W| = 10$) szyfr dwudzielny nie musi posiadać homofonów: podstawienie może nie być surjektywne, a części par można nie wykorzystać. Szyfru takiego używał szwedzki baronet Fridric Gripenstierna — prawdopodobnie w oparciu o propozycję Christophera Polheima. Zabawnej formy dwudzielnego szyfru z homofonami w czasie prac nad bombą atomową w Los Alamos używali: generał brygady Leslie R. Groves oraz podpułkownik Peer da Silva (rysunek 29.) podczas rozmów telefonicznych w celu ukrycia specjalnych nazw i miejsc. Chodzi o to, że odszukanie w diagramie potrzebnej litery zabiera nieco czasu, homofony są więc wybierane z większą losowością niż w normalnej sytuacji, kiedy szyfrant jest w pewien sposób stronniczy.

3.3.2. $m = 3$**, trójdzielne podstawienie proste** $V^{(1)} \longrightarrow W^3$**.** Podstawianie za pomocą trójznaków (*tripartite substitution*, podstawienie trójdzielne) zaproponował w swoim dziele *Polygraphiæ* Trithemius, przy $|W| = 3$ (warto zauważyć, że $3^3 = 27 > 26$) dla celów steganograficznych. W innych sytuacjach podobne trójdzielne podstawienia spotyka się rzadko.

3.3.3. $m = 5$**, pięciodzielne podstawienie proste** $V^{(1)} \longrightarrow W^5$**.** Podstawienie grupami po pięć znaków kryptogramu (podstawienie pięciodzielne) przy $|W| = 2$ zostało użyte przez Francisa Bacona razem z technikami steganograficznymi (warto zauważyć, że

1	2	3	4	5	6	7	8	9	0	
i	p	i		o	u	o		p	n	1
w	e	u	t	e	k		l	o		2
e	u	g	n	b	t	n		s	t	3
t	a	z	m	d		i	o	e		4
s	v	t	j		e		y		h	5
n	a	o	l	n	s	u	g	o	e	6
	c	b	a	f	r	s		i	r	7
i	c	w	y	r	u	a	m		n	8
m	v	t		h	p	d	i	x	q	9
l	s	r	e	t	d	e	a	h	e	0

Rysunek 29. Szyfr dwudzielny używany w Los Alamos w 1944 roku podczas rozmów telefonicznych

$2^5 = 32 > 26$). Pięciodzielne szyfrowanie binarne zostało wskrzeszone w maszynie szyfrującej Vernama w 1918 roku (podrozdział 8.3.2.), a podczas drugiej wojny światowej w szyfrujących maszynach dalekopisowych Siemens T 52 (*Geheimschreiber*) oraz Lorenz SZ 40/42 (*Schlüsselzusatz*), patrz podrozdziały: 9.1.3. oraz 9.1.4.

3.3.4. $m = 8$ **ośmiodzielne podstawienie proste** $V^{(1)} \longrightarrow\!\!\!\!\!\rightarrow W^8$**.** Dla $|W| = 2$ (kod 8-bitowy, binarny kod EBCDIC, kod ASCII z bitem parzystości) ośmiodzielne podstawienie proste pokrywa się z jednodzielnym podstawieniem bajtów (Z_{256}) znanym ze współczesnych komputerów.

3.4. Przypadek ogólny $V^{(1)} \longrightarrow\!\!\!\!\!\rightarrow W^{(m)}$ (rozstawianie)

W przypadku ogólnym $V^{(1)} \longrightarrow\!\!\!\!\!\rightarrow W^{(m)}$ mogą wystąpić wartości zerowe i homofony.

Simeone de Crema z Mantui (1401) korzystał z samych homofonów (przy $m = 1$). Przy $m = 2$ oprócz homofonów i wartości zerowych pojawia się nowe ważne pojęcie: *rozstawianie* (ang. *straddling*; niem. *Spreizen*) alfabetu, będące odwzorowaniem V na $W^1 \cup W^2$. Szyfr używany na dworze papieskim, opracowany przez Matteo Argentiego po 1590 roku wykorzystuje homofony, wartości zerowe oraz rozstawianie. Dla alfabetu Z_{24} rozszerzonego o `/et/`, `/con/`, `/non/`, `/che/`, oraz `5` i `7` służące jako wartości zerowe, krok szyfrowania $Z_{24}^{(1)} \longrightarrow\!\!\!\!\!\rightarrow Z_{10}^1 \cup Z_{10}^2$ wygląda następująco:

a	b	c	d	e	f	g	h	i	l	m	n	o
1	86	02	20	62 82	22	06	60	3	24	26	84	9

p	q	r	s	t	v	z	et	con	non	che	ϵ
66	68	28	42	80 40	04	88	08	64	00	44	5 7

3.4.1. Zastrzeżenia. Kroki szyfrowania z rozstawianiem podlegają ograniczeniu nakazującemu, by indukowane przez nie szyfrowanie było lewostronnie jednoznaczne (*left-unique*) — to znaczy, że granice (hiatusy) między elementami szyfru jedno- i dwuliterowego, a przez to odpowiednie dekompozycje, są dobrze określone. Jak stwierdzono w podrozdziale 2.4., Giovanni Battista oraz Matteo Argenti byli świadomi tego faktu. Ich szyfry spełniają następujący warunek: W dzieli się na znaki używane jako elementy szyfru jednoznakowego, $W' = \{1, 3, 5, 7, 9\}$ oraz szyfru dwuznakowego, $W'' = \{0, 2, 4, 6, 8\}$. Argenti popełnili błąd przyjmując, że także drugi znak szyfru musi być elementem W'', co prowadzi do rozstawiania. Udzielili oni także bardziej praktycznych porad: należy pomijać /u/ występujące po /q/ oraz pomijać podwojone litery.

Tak zwane szyfry szpiegowskie, używane przez sowiecki NKWD i jego kontynuatorów, to szyfry z rozstawianiem. Zostały one ujawnione przez schwytanych szpiegów. Przez analogię z kwadratem Polibiusza można je opisać za pomocą tablicy prostokątnej, np.:

(∗)

	0	1	2	3	4	5	6	7	8	9
	s	i	o	e	r	a	t	n		
8	c	x	u	d	j	p	z	b	k	q
9	.	w	f	l	/	g	m	y	h	v

której pierwszy wiersz zawiera jednoliterowe elementy szyfru.

Przy $W = Z_{10}$ otrzymać można 28 elementów szyfru, co wystarczy dla Z_{26} i dwóch znaków specjalnych: . znaczącego 'stop' oraz /, służącego do zmiany trybu litera–liczba. Z uwagi na fakt, że szyfr ten podlegał dalszemu szyfrowaniu (szyfrowanie zamykające, *closing*, podrozdział 9.2.1.), był przydatny do szyfrowania liczb (po przesłaniu znaku przejścia litera–liczba umożliwiał powtórną transmisję liczby), będącą dodatkowym zabezpieczeniem przed błędami transmisji.

Przy konstrukcji tej tablicy także korzystano z hasła. Dr Per Meurling, szwedzki podróżnik, zrobił to w 1937 roku w sposób następujący: zapisał 8-literowe hasło (M. Delvayo był hiszpańskim komunistą), a pod nim pozostałą część alfabetu; kolumny zostały ponumerowane od końca:

	0	9	8	7	6	5	4	3	2	1
	m	d	e	l	v	a	y	o		
1	b	c	f	g	h	i	j	k	n	p
2	q	r	s	t	u	w	x	z	.	/

Procedura taka ma tę wadę, że nie wszystkie najczęściej występujące litery otrzymują jednocyfrowe kody. Wadą tą charakteryzowała się także metoda szwedzkiego szpiega Bertila Erikssona, której używał w 1941 roku: ponumerował on kolumny zgodnie z alfabetyczną kolejnością liter znajdujących się w haśle (podrozdział 3.2.5.):

	6	0	8	7	5	4	9	1	2	3
3	p	a	u	s	o	m	v	e	j	k
9	b	c	d	f	g	h	i	l	n	q
	r	t	w	x	y	z				

Hasło pochodziło ze szwedzkiego tłumaczenia powieści Jaroslava Haška *Paus, som Svejk själv avbröt*.... Z uwagi na fakt, że szyfrowanie najczęściej występujących liter za pomocą kodów jednocyfrowych, nie zaś wielocyfrowych, skraca również czas transmisji telegraficznej, w 1940 roku NKWD opracował metodę, która brała to pod uwagę.

Max Clausen, radiooperator rosyjskiego szpiega w Tokio dra Richarda Sorge, musiał zapamiętać zdanie: *„a sin to err"* (to bardzo dobra rada dla każdego szpiega), zawierające osiem najczęściej występujących liter w języku angielskim, w sumie w 65,2% przypadków. Do tablicy wstawiono hasło *subway* i uzupełniono je pozostałymi literami. Następnie, przechodząc kolumny od strony lewej do prawej, najpierw literom ze zbioru $\{\mathtt{a},\mathtt{s},\mathtt{i},\mathtt{n},\mathtt{t},\mathtt{o},\mathtt{e},\mathtt{r}\}$ przypisano liczby od 0 do 7; potem, pozostałym literom przypisano liczby od 80 do 99:

s	u	b	w	a	y
0	82	87	91	5	97
c	d	e	f	g	h
80	83	3	92	95	98
i	j	k	l	m	n
1	84	88	93	96	7
o	p	q	r	t	v
2	85	89	4	6	99
x	z	.	/		
81	86	90	94		

W ten sposób kwadrat Polibiusza oznaczony na stronie 72 znakiem $(*)$ otrzymano w bardziej zwięzłej notacji.

W przypadku cyrylicy odpowiedni jest podział na siedem kodów jednocyfrowych oraz trzydzieści kodów dwucyfrowych, co w sumie daje 37 kodów i pozwala na użycie 5 znaków specjalnych. W metodzie, którą zdradził agent Reino Hayhanen, pomocnik wysoko postawionego szpiega rosyjskiego Rudolfa Abla, korzystano z rosyjskiego słowa „снегопад" ['opady śniegu'], którego pierwszych siedem liter występuje z łączną częstością 44,3%. Tablicę utworzoną jak zwykle:

с	н	е	г	о	п	а	.	.	.
б	в	д	ж	з	и	j	к	л	м
р	т	у	ф	х	ц	ч	ш	щ	ъ
ы	ь	э	ю	я	.	.	.	.	.

przekształcano za pomocą klucza, który był zmieniany od komunikatu do komunikatu, a który można było znaleźć w z góry ustalonym miejscu zaszyfrowanej wiadomości. Ostatecznie dokonywano szyfrowania zamykającego (*closing encryption* — podrozdział 9.2.1.).

3.4.2. Rosyjskie łączenie. Przy tej okazji trzeba wyjaśnić używaną przez Rosjan metodę, zwaną „rosyjskim łączeniem": wiadomość dzieli się w niej na dwie części mniej więcej tej samej długości, po czym łączy się je w odwrotnej kolejności, ukrywając w ten sposób gdzieś pośrodku rzucające się w oczy wyrażenia, standardowo występujące na początku i na końcu wiadomości.

Winston Churchill nazwał Rosję *„a riddle wrapped in a mystery inside an enigma"* [„zagadka otoczona tajemnicą niewiadomego"]. To samo powiedzieć można o rosyjskiej kryptologii.