Szyfr Vigenere'a

Przykładem podstawienia polialfabetycznego jest szyfr Vigenere'a.[1mm]W przypadku szyfru Vigenere'a kolejne alfabety użyte do szyfrowania otrzymujemy stosując szyfr Cezara o różnej długości klucza.[1mm]Zatem kluczem jest wektor $(k_1, k_2, \ldots, k_n)$ określający kolejne przesunięcia alfabetów.[1mm]Dla ułatwienia zapamiętania ciąg $(k_1, k_2, \ldots, k_n)$ możemy zastąpić słowem kluczowym o literach odpowiadających $k_1, k_2, \ldots, k_n$.

Słowo kluczowe: PEN $\rightarrow (15, 4, 13)$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
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
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

Szyfrowanie:

CAFFE LATTE $\rightarrow$ CAF $\vert$ FEL $\vert$ ATT $\vert$ E $\rightarrow$ RES$\vert$UIY$\vert$PXG$\vert$T

Szyfr Vigenere'a

Przestrzeń klucza

Na każdej pozycji w słowie kluczowym mamy 26 możliwości wyboru.

Zatem jeżeli słowo kluczowe ma długość n to rozmiar przestrzeni klucza wynosi:

$$26^n.$$

Dla $n = 10$:

$$26^{10} \approx 1{,}4 \times 10^{15} \approx 2^{47}.$$

Dla $n = 20$:

$$26^{20} \approx 2 \times 10^{28} \approx 2^{94}.$$

Ogólne podstawienie polialfabetyczne

W szyfrach tego rodzaju kolejne litery tekstu jawnego są zastępowane w kryptogramie literami z kolejnych dowolnie przepermutowanych alfabetów.

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

Szyfrowanie:

CAFFE LATTE $\rightarrow$ CAFF $\vert$ ELAT $\vert$ TE $\rightarrow$ BEMZ $\vert$ XFXA $\vert$ CD

Ogólne podstawienie polialfabetyczne

Przestrzeń klucza

Mamy 26! możliwości wyboru każdej z permutacji.

Zatem jeżeli kluczem jest n permutacji to rozmiar przestrzeni klucza wynosi:

$$(26!)^n.$$

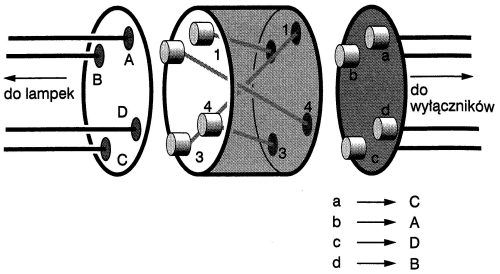
Dla $n = 10$:

$$(26!)^{10} \approx 1{,}1 \times 10^{266} \approx 2^{884}.$$

Dla $n = 20$:

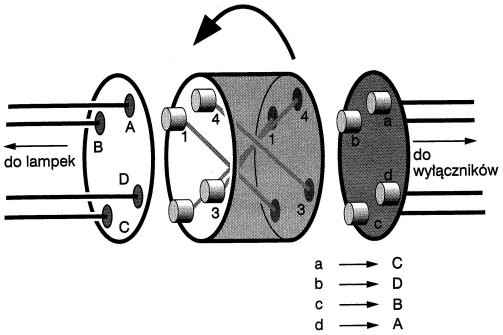
$$(26!)^{20} \approx 1{,}3 \times 10^{532} \approx 2^{1768}.$$

Realizacja szyfrów polialfabetycznych
Cylindry szyfrujące



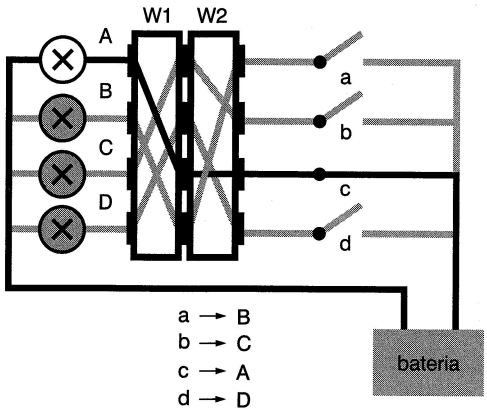
Zastosowanie stałego cylindra szyfrującego pozwala zrealizować podstawienie monoalfabetyczne.

Realizacja szyfrów polialfabetycznych
Cylindry szyfrujące



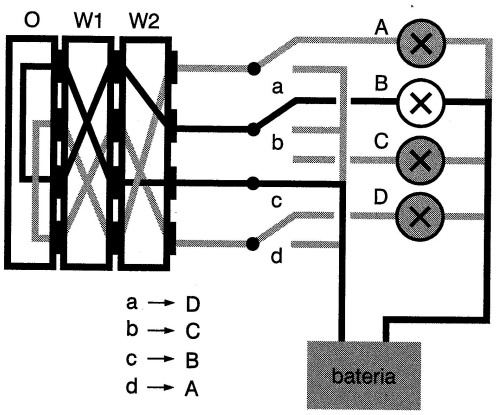
Po wpisaniu każdej litery cylinder obraca się o jedną pozycję.Ten obrót cylindra pozwala zrealizować szyfr Vigenere'a o długości klucza równej 26.

Realizacja szyfrów polialfabetycznych
Cylindry szyfrujące



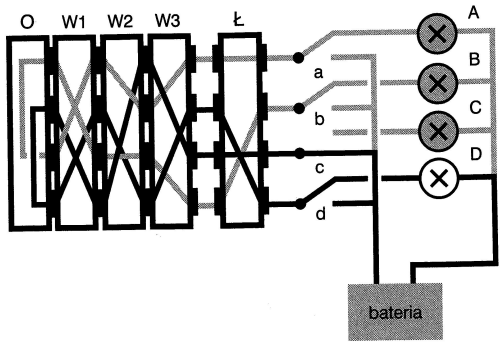
Gdy mamy kilka cylindrów, to po wpisaniu każdej litery pierwszy cylinder obraca się o jedną pozycję.
Gdy pierwszy cylinder wykona pełen obrót (po wpisaniu 26 liter) to drugi cylinder obraca się o jedną pozycję.
Gdy drugi cylinder wykona pełen obrót (po wpisaniu $26 \cdot 26$ liter) to trzeci cylinder obraca się o jedną pozycję i tak dalej.
Zwiększenie liczby cylindrów pozwala zwiększyć długość klucza.

Realizacja szyfrów polialfabetycznych
Cylindry szyfrujące



Działanie cylindra odwracającego.

Realizacja szyfrów polialfabetycznych
Enigma



O – cylinder odwracający, W1, W2, W3 – cylindry szyfrujące, Ł – łącznica.

Schemat maszyny szyfrującej Enigma.

Realizacja szyfrów polialfabetycznych
Enigma

Niemiecka maszyna szyfrująca Enigma.

Realizacja szyfrów polialfabetycznych

Enigma

Teoretycznie przestrzeń kluczy Enigmy liczyła około

$$2^{366}$$

elementów.[2mm]Ze względu na pewne ograniczenia praktyczne stosowane przez Niemców w czasie wojny w rzeczywistości dostępne było około

$$2^{77}$$

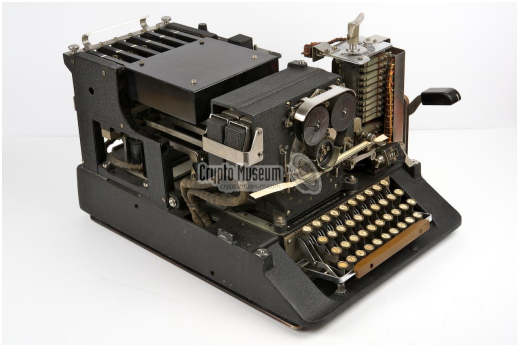
kluczy.[2mm]Konstrukcja Enigmy miała pewne słabości, które zostały wykorzystane do przeprowadzenia efektywnego ataku, innego niż wyczerpujące przeszukanie przestrzeni kluczy.

Szyfr Enigmy został złamany przez polskich matematyków:

Marian Rejewski Jerzy Różycki Henryk Zygalski

Inne maszyny szyfrujące

W czasie II Wojny Światowej maszyny szyfrujzace były w powszechnym użyciu, np. Amerykanie używali maszyny szyfrującej Sigaba.
Sigaba wykorzystywała cylindry szyfrujące (5 szyfrujących i 10 kontrolujących ustawienia szyfrujących), nie posiadała łącznicy oraz cylindra odwracającego.
Według dostępnych danych, w czasie, gdy Sigaba była używana, jej szyfr nie został złamany.



Amerykańska maszyna szyfrująca Sigaba.

Inne maszyny szyfrujące

Po II Wojnie Światowej jeszcze przez wiele lat używano elektromechanicznych maszyn szyfrujących.
Np. szwajcarska maszyna Hagelin CX-52, skonstruowana w roku 1952 była używana w ponad 50 krajach.
W wielu krajach CX-52 jako rezerwowa maszyna szyfrująca była w użyciu jeszcze w latach 80-tych a w niektórych jeszcze w 90-tych.

Maszyna Hagelin CX-52

Tabliczka jednokrotna (szyfr Vernama)

Szyfr zaproponowany w roku 1918 przez G. Vernama i J. Mauborgne'a.

Klucz jest losowym ciągiem znaków.

Klucz musi być takiej samej długości jak wiadomość:

$$k_1 k_2 k_3 k_4 \dots k_n$$

Tekst jawny: $a_1 a_2 a_3 a_4 \dots a_n$

Szyfrowanie:

$$\begin{aligned} c_1 &= a_1 + k_1 \mod 26 \\ c_2 &= a_2 + k_2 \mod 26 \\ &\dots \\ c_n &= a_n + k_n \mod 26 \end{aligned}$$

Kryptogram: $c_1 c_2 c_3 c_4 \dots c_n$

Deszyfrowanie:

$$a_i = c_i - k_i = c_i + (26 - k_i) \mod 26, i = 1, 2, \dots, n$$

Tabliczka jednokrotna (szyfr Vernama)

Własności:

+ Jeżeli klucz jest dobrze wybrany (czyli jest całkowicie losowy), to tabliczka jednokrotna jest szyfrem niemożliwym do złamania.
  Atak przez wyczerpujące przeszukanie przestrzeni kluczy jest bezcelowy – sprawdzając wszystkie klucze otrzymamy wszystkie możliwe teksty o określonej długości.
  Atak przy pomocy znanego tekstu jawnego pozwala wyznaczyć tylko część klucza odpowiadającą znanemu tekstowi, nic nie mówi o pozostałej części klucza.

– Klucz musi być takiej samej długości jak wiadomość.

– Klucz musi być całkowicie losowy, co nie jest proste do uzyskania, gdy ma być odpowiednio długi.

Tabliczka jednokrotna (szyfr Vernama)

Przykład

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Niech szyfrogram będzie postaci: AGX $\rightarrow$ (0,6,23)

Zastosujmy wyczerpujące przeszukanie przestrzeni kluczy.

W czasie przeszukania między innymi sprawdzimy klucze: CCF i NSE

Deszyfrowanie z kluczem CCF:

CCF $\rightarrow$ (2,2,5)

$(0, 6, 23) + (26 - 2, 26 - 2, 26 - 5) = (0, 6, 23) + (24, 24, 21) = (24, 30, 44) = (24, 4, 18) \mod 26$

(24,4,18) $\rightarrow$ YES

Deszyfrowanie z kluczem NSE:

NSE $\rightarrow$ (13,18,4)

$(0, 6, 23) + (26 - 13, 26 - 18, 26 - 4) = (0, 6, 23) + (13, 8, 22) = (13, 14, 45) = (13, 14, 19) \mod 26$

(13,14,19) $\rightarrow$ NOT

Tabliczka jednokrotna (szyfr Vernama)

Wersja binarna

Tekst jawny zamieniamy na ciąg bitów (0 i 1), korzystając np. z kodu ASCII:

$$A \rightarrow 1000001, \quad B \rightarrow 1000010, \quad C \rightarrow 1000011, \ldots$$

W rezultacie otrzymujemy ciąg bitów:

$$a_1 a_2 a_3 a_4 \ldots a_n$$

Klucz jest losowym ciągiem bitów.

Klucz musi być takiej samej długości jak wiadomość:

$$k_1 k_2 k_3 k_4 \ldots k_n$$

Tabliczka jednokrotna (szyfr Vernama)

Wersja binarna

Szyfrowanie:

$$c_1 = a_1 \oplus k_1, \quad c_2 = a_2 \oplus k_2, \quad \ldots \quad c_n = a_n \oplus k_n$$

gdzie $\oplus$ oznacza dodawanie $\mod 2$.

Gdy operujemy tylko w zbiorze bitów to stosujemy równoważne oznaczenia:

$$a \oplus b \equiv a\, XOR\, b \equiv a + b \mod 2.$$

Deszyfrowanie:

$$a_1 = c_1 \oplus k_1, \quad a_n = c_n \oplus k_n, \quad \ldots \quad a_n = c_n \oplus k_n$$

ponieważ

$c_1 \oplus k_1 = (a_1 \oplus k_1) \oplus k_1 = a_1 \oplus (k_1 \oplus k_1) = a_1 \oplus 0 = a_1$.

$k_1 \oplus k_1 = 0$ gdyż $0 + 0 = 0$ oraz $1 + 1 = 2 = 0 \mod 2$.