1. Szyfry monoalfabetyczne

1.1 Tablica Polibiusza

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

TABLICA POLIBIUSZA DLA AFABETU ŁACIŃSKIEGO

Tablica Polibiusza to tabela przypisująca każdą literę alfabetu parzę numerów; liczbie wiersza i kolumny. Została stworzona przez greckiego historyka Polibiusza w II w. p.n.e. Dzięki tablicy przedstawionej powyżej możemy przekształcić nazwę projektu "kody i szyfry" w 253414542443555421425 4.

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

TABLICA Z ROZWIDLENIEM

W tej tablicy część liter odpowiada jednej cyfrze, zaś inne dwóm. Jeśli litera odpowiada dwóm cyfrom, to pierwsza z nich to 1 lub 2. 1 i 2 same nie oznaczają żadnej litery. Tym sposobem "kody i szyfry" zmieniamy w 14185281020292871228.

1.2 Szyfr Cezara

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	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

SZYFR CEZARA

Szyfr Cezara polega na zastąpieniu każdej litery tekstu jawnego literą położoną o 3 miejsca dalej w alfabecie. Oczywiście szyfr można zmienić tak, by każda litera tekstu jawnego była zastępowana literą położoną o 1, 2, 4, 5 itd. miejsc w alfabecie. Z przekształceniem o 3 miejsca - jak w powyższej tablicy - "kody i szyfry" zmienia się w nrgblvcbiub.

1.3 Cykle

Szyfry przedstawione powyżej można też zapisać w postaci cykli np. szyfr cezara można przedstawić jako:

(adgjmpsvybehknqtwzcfilorux)

Każda litera zostaje zamieniona na literę znajdującą się po jej prawej stronie. W ten sposób przekształcenie zapętli się w nieskończoność. Nawiasy oddzielają poszczególne cykle od siebie.

1.4 Łamanie szyfrów monoalfabetycznych

Szyfr monoalfabetyczne można łatwo złamać, jeśli zna się ich działanie oraz ma się wystarczająco długą zaszyfrowaną wiadomość. Wystarczy użyć częstotliwości występowania liter. Spróbujmy z tekstem strony wikipedii na temat języka angielskigo (https://en.wikipedia.org/wiki/English_language).

Oryginał:

English is a West Germanic language that was first spoken in early medieval England and is now a global *lingua franca*. Named after the Angles, one of the Germanic tribes that migrated to England, it ultimately derives its name from the Anglia (Angeln) peninsula in the Baltic Sea. It is most closely related to the Frisian languages, although its vocabulary has been significantly influenced by other Germanic languages in the early medieval period, and later

by Romance languages, particularly French. English is either the official language or one of the official languages in almost 60 sovereign states. It is the most commonly spoken language in the United Kingdom, the United States, Canada, Australia, Ireland, and New Zealand, and is widely spoken in some areas of the Caribbean, Africa, and South Asia. It is the third most common native language in the world, after Mandarin and Spanish. It is the most widely learned second language and an official language of the United Nations, of the European Union, and of many other world and regional international organisations. It is the most widely spoken Germanic language, accounting for at least 70% of speakers of this Indo-European branch.

English has developed over the course of more than 1,400 years. The earliest forms of English, a set of Anglo-Frisian dialects brought to Great Britain by Anglo-Saxon settlers in the fifth century, are called Old English. Middle English began in the late 11th century with the Norman conquest of England, and was a period in which the language was influenced by French. Early Modern English began in the late 15th century with the introduction of the printing press to London and the King James Bible, and the start of the Great Vowel Shift. Through the worldwide influence of the British Empire, modern English spread around the world from the 17th to mid-20th centuries. Through all types of printed and electronic media, as well as the emergence of the United States as a global superpower, English has become the leading language of international discourse and the lingua franca in many regions and in professional contexts such as science, navigation, and law.

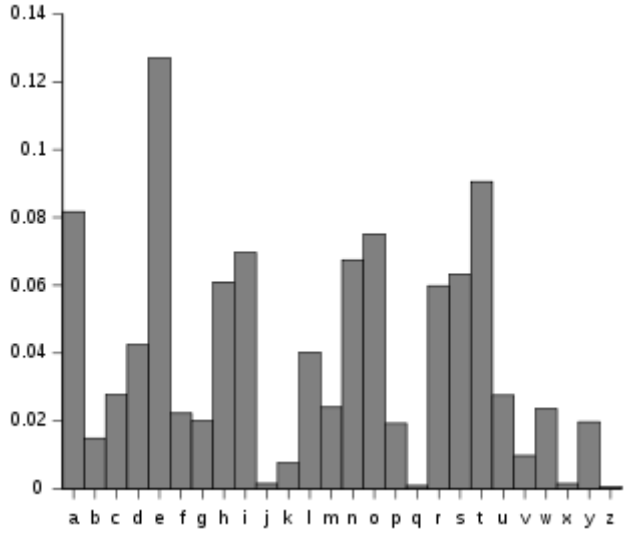
Modern English has little inflection compared with many other languages, and relies more on auxiliary verbs and word order for the expression of complex tenses, aspect and mood, as well as passive constructions, interrogatives and some negation. Despite noticeable variation among the accents and dialects of English used in different countries and regions – in terms of phonetics and phonology, and sometimes also vocabulary, grammar and spelling – English-speakers from around the world are able to communicate with one another with relative ease.

Tekst po zaszyfrowaniu:

hqjolvk lv d zhvw jhupdqlf odqjxdjh wkdw zdv iluvw vsrnhq lq hduob phglhydo hqjodqg dqg lv qrz d joredo olqjxd iudqfd qdphg diwhu wkh dqjohv rqh ri wkh jhupdqlf wulehv wkdw pljudwhg wr hqjodqg lw xowlpdwhob ghulyhv lwv qdph iurp wkh dqjold dqjhoq shqlqvxod lq wkh edowlf vhd lw lv prvw forvhob uhodwhg wr wkh iulvldq odqjxdjhv dowkrxjk lwv yrfdexodub kdv ehhq vljqlilfdqwob lqioxhqfhg eb rwkhu jhupdqlf odqjxdjhv lq wkh hduob phglhydo shulrg dqg odwhu eb urpdqfh odqjxdjhv sduwlfxoduob iuhqfk hqjolvk lv hlwkhu wkh riilfldo odqjxdjh ru rqh ri wkh riilfldo odqjxdjhv lq doprvw vryhuhljq vwdwhv lw lv wkh prvw frpprqob vsrnhq odqjxdjh lq wkh xqlwhg nlqjgrp wkh xqlwhg vwdwhv fdqdgd dxvwudold luhodqg dqg qhz chdodqg dqg lv zlghob vsrnhq lq vrph duhdv ri wkh fduleehdq diulfd dqg vrxwk dvld lw lv wkh wklug prvw frpprq qdwlyh odqjxdjh lq wkh zruog diwhu pdqgdulq dqg vsdqlvk lw lv wkh prvw zlghob ohduqhg vhfrqg odqjxdjh dqg dq riilfldo odqjxdjh ri wkh xqlwhg qdwlrqv ri wkh hxurshdq xqlrq dqg ri pdqb rwkhu zruog dqg uhjlrqdo lqwhuqdwlrqdo rujdqlvdwlrqv lw lv wkh prvw zlghob vsrnhq jhupdqlf odqjxdjh dffrxqwlqj iru dw ohdvw ri vshdnhuv ri wklv lqgr hxurshdq eudqfk hqjolvk kdv ghyhorshg ryhu wkh frxuvh ri pruh wkdq bhduv wkh hduolhvw irupv ri hqjolvk d vhw ri dqjor iulvldq gldohfwv eurxjkw wr juhdw eulwdlq eb dqjor vdarq vhwwohuv lq wkh iliwk fhqwxub duh fdoohg rog hqjolvk plggoh hqjolvk ehjdq lq wkh odwh wk fhqwxub zlwk wkh qrupdq frqtxhvw ri hqjodqg dqg zdv d shulrg lq zklfk wkh odqjxdjh zdv lqioxhqfhg eb iuhqfk hduob prghuq hqjolvk ehjdq lq wkh odwh wk fhqwxub zlwk wkh lqwurgxfwlrq ri wkh sulqwlqj suhvv wr orqgrq dqg wkh nlqj mdphv eleoh dqg wkh vwduw ri wkh juhdw yrzho vkliw wkurxjk wkh zruogzlgh lqioxhqfh ri wkh eulwlvk hpsluh prghuq hqjolvk vsuhdg durxqg wkh zruog iurp wkh wk wr plg wk fhqwxulhv wkurxjk doo wbshv ri sulqwhg dqg hohfwurqlf

phgld dv zhoo dv wkh hphujhqfh ri wkh xqlwhg vwdwhv dv d joredo vxshusrzhu hqjolvk kdv ehfrph wkh ohdglqj odqjxdjh ri lqwhuqdwlrqdo glvfrxuvh dqg wkh olqjxd iudqfd lq pdqb uhjlrqv dqg lq surihvvlrqdo frqwhawv vxfk dv vflhqfh qdyljdwlrq dqg odz prghuq hqjolvk kdv olwwoh lqiohfwlrq frpsduhg zlwk pdqb rwkhu odqjxdjhv dqg uholhv pruh rq dxaloldub yhuev dqg zrug rughu iru wkh hasuhvvlrq ri frpsoha whqvhv dvshfw dqg prrg dv zhoo dv sdvvlyh frqvwuxfwlrqv lqwhuurjdwlyhv dqg vrph qhjdwlrq ghvslwh qrwlfhdeoh yduldwlrq dprqj wkh dffhqwv dqg gldohfwv ri hqjolvk xvhg lq gliihuhqw frxqwulhv dqg uhjlrqv lq whupv ri skrqhwlfv dqg skrqrorjb dqg vrphwlphv dovr yrfdexodub judppdu dqg vshoolqj hqjolvk vshdnhuv iurp durxqg wkh zruog duh deoh wr frppxqlfdwh zlwk rqh dqrwkhu zlwk uhodwlyh hdvh.

Teraz należy stworzyć tabelę ukazującą częstotliwość występowania poszczególnych znaków w języku angielskim oraz w pokazanym powyżej tekście zaszyfrowanym.
Częstotliwość występowania liter w języku angielskim:



(źródło: https://en.wikipedia.org/wiki/Frequency_analysis)

Częstotliwość występowania poszczególnych liter w tekście zaszyfrowanym:

Litery	a	b	c	D1	e	f	g	H1	i	j	k	L1	m
Ilość	5	27	1	219	25	63	88	262	54	84	96	170	1
Częstotliwość występowania	0.002	0.012	0	0.099	0.011	0.028	0.039	0.118	0.024	0.038	0.043	0.077	0

Litery	n	o	p	Q1	R1	s	t	u	V1	W1	x	y	z
Ilość	8	120	56	210	148	32	1	122	140	172	55	16	27
Częstotliwość występowania	0.003	0.054	0.025	0.095	0.067	0.014	0	0.055	0.063	0.078	0.024	0.007	0.012

W sumie w całym tekście jest 2202 liter. Częstotliwość występowania została zaokrąglona do 3 miejsc po przecinku. Jak widzimy najczęściej w tekście występuje litera "h". Najprawdopodobniej odpowiada więc ona literze "e". Jak widzimy w tekście często

występuje samotnie litera "d". Jedyną literą występującą samą w języku angielskim jest litera "a". Widzimy też często występujące w tekście pary liter "lv" i "lq". Zapewne odpowiadają angielskiemu "is" i "in". Oznacza to że litera "l" odpowiada literze "i". Spróbujmy więc rozszyfrować dzięki temu pierwsze sześć wyrazów:

eqjoivk iv a zevw jeupaqif oaqjxaje

hqjolvk lv d zhvw jhupdqlf odqjxdjh

Jak widzimy 2 słowem w zaszyfrowanym tekście jest "lv". Najczęściej 2 słowem w języku angielskim jest czasownik. "lv" oznacza więc pewnie wyraz "is". "lq" odpowiada więc zapewne słowu "in".

enjoisk is a zesw jeupanf oanxaje

hqjolvk lv d zhvw jhupdqlf odqjxdjh

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	x
d				h				l					q	r				v	w						

Najczęściej występujące w języku angielskim wciąż nieodszyfrowane litery to "t" oraz "o". Po podobnej częstotliwości występowania widzimy że "t" jest zaszyfrowane jako "w" zaś "o" jako "r".

enjoisk is a zest jeupanf oanxaje tkat zas ilust vsonen in eauob pegieydo enjoang ang

hqjolvk lv d zhvw jhupdqlf odqjxdjh wkdw zdv iluvw vsrnhq lq hduob phglhydo hqjodqg dqg

Mamy prawie rozszyfrowany wyraz "wkdw", który zapewne oznacza wyraz "that". Litera "k" odpowiada więc zapewne literze "h".
enjoish is a zest jeupanf oanxaje that zas ilust vsonen in eauob pegieydo enjoang ang
hqjolvk lv d zhvw jhupdqlf odqjxdjh wkdw zdv iluvw vsrnhq lq hduob phglhydo hqjodqg dqg

Trójka znaków "zdv" w tym kontekście oznacza was lub has. Jako że to "k" odpowiada "h", to "z" odpowiada "w".
enjoish is a west jeupanf oanxaje that was ilust ssonen in eauob pegieyao enjoang ang
hqjolvk lv d zhvw jhupdqlf odqjxdjh wkdw zdv iluvw vsrnhq lq hduob phglhydo hqjodqg dqg

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			g	h		d	k	l					q	r				v	w			z			

Mamy trzyliterowe słowo zaczynające się na "an". Zapewne jest to słowo "and". Oznacza to że "g" odpowiada literze "d".
Reszta liter jest łatwo rozszyfrowana podobną metodą. Inną ciekawą metodą rozszyfrowania szyfru cezara jest sprawdzenie wszystkich 26 możliwości przekształcenia liter.

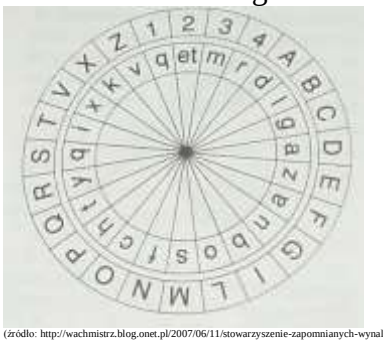
2. Homofony

Homofony to dodatkowe znaki szyfrogramu odpowiadające znakom tekstu jawnego. Mają uniemożliwić atak na szyfr używając częstotliwości występowania liter w tekście. Pewnymi znakami można zastąpić też spacje. Dla utrudnienia odszyfrowania tekstu można też wstawić do tekstu nic nieznaczące znaki puste. W praktyce jednak, można domyślić się które znaki szyfrogramu odpowiadają którym znakom tekstu jawnego dzięki powtarzającym się słowom.

3. Szyfry polialfabetyczne

Szyfry polialfabetyczne to szyfry posiadające więcej niż jeden alfabet tajny. Szyfry te są o wiele trudniejsze do złamania niż szyfry monoalfabetyczne.

3.1 Tarcza Albertiego



(źródło: http://wachmistrz.blog.onet.pl/2007/06/11/stowarzyszenie-zapomnianych-wynalazcow-xix/)

Tarcza Albertiego została stworzona przez włoskiego kryptografa Leona Battiste Albertiego. Składa się z dwóch krążków większego (stałego) na którym znajdują się litery w kolejności alfabetycznej oraz mniejszego (ruchomego) na którym znajdują się litery wypisane w kolejności losowej. Żeby komunikacja za pomocą tarczy Albertiego zachodziła poprawnie, zarówno wysyłający, jak i adresat muszą mieć takie same tarczę. Następnie wybieramy *wskaźnik* czyli jeden znak z mniejszego koła. Musi być on znany zarówno wysyłającemu, jak i adresatowi. Gdy chcemy wysłać jakiś komunikat, zaczynamy go napisaniem dowolnego znaku z większego krążka, który piszemy dużą literą. Następnie obracamy krążek ruchomy tak, by litera którą właśnie napisaliśmy znajdowała się nad *wskaźnikiem*. Szyfrujemy parę słów, zamieniając znaki tekstu jawnego na odpowiadające im znaki na dużego krążka, a następnie znowu wybieramy losowy znak z większego okręgu, zapisujemy go w wiadomości wielką literą i obracamy mniejszy krążek tak, by litera którą właśnie napisaliśmy znajdowała się nad *wskaźnikiem*. Szyfrujemy parę słów, i powtarzamy cały proces, aż do zakończenia szyfrowania. Adresat wiadomości bierze swoją tablicę, ustawia ją tak by wcześniej ustalony wskaźnik znajdował się pod pierwszą dużą literą, następnie deszyfruje wiadomość aż do następnej dużej litery poprzez zmienienie każdej litery kryptogramu na odpowiadającą jej literę na małym krążku. Proces powtarzamy aż do zakończenia szyfrowania. Tarcza Albertiego została stworzona do alfabetu włoskiego.

3.2 Szyfr Vigenere' 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
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	Y

(źródło: http://krystianpiwowarczyk.pl/content/article/show/historia-kryptologii-cz-pierwsza)

Szyfr Vigenere'a polega na szyfrowaniu tekstu jawnego za pomocą klucza oraz tablicy Vigenere'a. Tekst jawny szyfrujemy w następujący sposób: bierzemy pierwszą literę tekstu jawnego i pierwszą literę klucza, znajdujemy literę odpowiadającą tym dwom literom na tablicy Vigenere'a. Będzie to pierwsza litera kryptogramu. Następnie bierzemy drugą literę klucza i drugą literę tekstu jawnego itd. Jeśli klucz jest krótszy od tekstu jawnego, to powtarzamy go w koło aż osiągnie odpowiednią długość. Adresat odszyfrowuje wiadomość biorąc najpierw pierwszą literę klucza i kryptogramu. Wybieramy kolumnę odpowiadającą literze klucza, a następnie szukamy w niej litery kryptogramu. Wiersz w której się ona znajduje odpowiada literze tekstu jawnego. Cały proces powtarzamy aż do odszyfrowania wiadomości.

Klucz musi zostać ustalony wcześniej przez adresata i nadawcę. Jako klucza można użyć dowolnego słowa. Można też użyć tak zwanego *autoklucza*. Autoklucz polega na wybraniu losowej litery, z której pomocą zostanie zaszyfrowana pierwsza litera tekstu jawnego. Jako klucza do zaszyfrowania następnych liter tekstu jawnego używamy poprzednich znaków tekstu jawnego.

Zaszyfrujmy zdanie "Attack will begin on four o'clock" kluczem "secret" oraz autokluczem rozpoczętym literą "s".

Attack will begin on four o'clock
Sxvrgd omnc fxymp fr ygyt f'geggm - zdanie zaszyfrowane kluczem "secret"

Attack will begin on four o'clock
Stmtcm getw mfkov bb stil f'qnzqm - zdanie zaszyfrowane autokluczem

3.3 Algorytm della Porty

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

W algorytmie della Porty używamy tzw. tablicy della Porty. W każdym wierszu tabeli mamy alfabet podzielony na pół; jedna połowa zapisana nad drugą. By zaszyfrować wiadomość, najpierw musimy wybrać klucz. Następnie bierzemy pierwszą literę klucza i tekstu jawnego. Litera klucza wskazuje na wiersz tabeli którego użyjemy do zaszyfrowania wiadomości. Jeśli dana litera tekstu znajduję się w górnej połowie alfabetu, to zaszyfrowujemy ją jako literę bezpośrednio pod nią; jeśli w dolnej, nad nią. Następne litery tekstu jawnego szyfrujemy kolejnymi literami klucza.

Zaszyfrujemy zdanie "Attack will begin on four o'clock" kluczem "secret".

Attack will begin on four o'clock
rihsno ftxq zvxtb jc wkjf j'npknw

3.4 Cylinder Jeffersona

(źródło: https://commons.wikimedia.org/wiki/File:Jefferson_cylinder_cipher_(replica)_-_National_Cryptologic_Museum_-_DSC07717.JPG)

Cylinder Jeffersona składa się z ponumerowanych krążków, na których krawędzi napisano alfabet w losowej kolejności. Krążki te można nałożyć w dowolnej kolejności na wspólnej osi. Nadawca i adresat ustalają najpierw kolejność nakładania krążków na oś (klucz). Gdy nadawca chce wysłać wiadomość, układa krążki za pomocą ustalonego klucza, a następnie obraca je tak by pokazały część wiadomości (dla n krążków będzie to n liter wiadomości). Spisuje on następnie litery z innej strony krążków. Jest to szyfrogram. Nadawca powtarza proces aż do zaszyfrowania całej wiadomości. Adresat po otrzymaniu wiadomości układa swoje krążki w kolejności ustalonej w kluczu, następnie zaś obraca je tak, by pokazywały pierwszą część szyfrogramu. Następnie zaś szuka spośród pozostałych rzędów liter sensownej wiadomości. Jest to tekst jawny.

3.5 Szyfr Playfair'a

Szyfrowanie wiadomości w oparciu o szyfr Playfair'a polega na ustaleniu klucza przez adresata i nadawcę który następnie wpisujemy do tabeli o wymiarach 5x5, ignorując powtarzające się litery. Następnie, resztę liter wpisujemy zgodnie z kolejnością alfabetyczną.

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

Przykładowa tablica Playfair'a oparta o klucz "szyfr"

W szyfrze Playfair'a "i" i "j" traktowano jako jeden znak. By zaszyfrować wiadomość, najpierw należy podzielić ją na pary liter. Dwie takie same litery należy rozdzielić literą "x".
Jeśli para liter znajdowała się w tym samym rzędzie ustalonej tablicy Playfair'a, to zaszyfrowywano je jako litery znajdujące się po ich prawej stronie w tablicy Playfair'a. Jeśli znajdowały się w tej samej kolumnie, to zaszyfrowywano je jako litery znajdujące się pod nimi. Jeśli litery znajdowały się w różnych kolumnach i wierszach, to szyfrowano je jako litery znajdujące się w tym samym wierszu, ale w kolumnie drugiej szyfrowanej przez nas litery.
Zaszyfrujmy zdanie "Attack will begin on four o'clock" za pomocą klucza "szyfr"

Attack will begin on four o'clock
AT TA CK WI LX LB EG IN ON FO UR OC LO CK

GS SG DI VK QR HE AL HO PO YP XZ VI IQ DI

3.6 Szyfry ADFGX i ADFVGX

Szyfry te były używane przez niemiecką armię podczas I wojny światowej. Oba zostały złamane przez francuskiego porucznika Georges Painvin'a.

By użyć szyfru ADFGX, najpierw należy ustalić klucz oraz stworzyć tabelę o wymiarach 5x5 wypełnioną losowo ułożonymi znakami alfabetu. "I" oraz "j" traktujemy jako tą samą literę.

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

Przykładowa tablica ADFGX

	A	D	F	V	G	X
A	P	8	Y	X	0	T
D	H	Q	4	G	N	3
F	M	1	A	K	Z	V
V	9	D	U	B	5	S
G	L	C	W	2	J	R
X	I	7	F	E	O	6

Przykładowa tablica ADFVGX

Gdy chcemy zaszyfrować wiadomość, najpierw szyfrujemy ją za pomocą powyższej tabeli jak w szyfrze Polibiusza. Następnie zaś, bierzemy nasze słowo klucz, pomijając powtarzające się litery i układamy zaszyfrowaną wiadomość pod nim tak, by tworzyła ona tabelę. Wiadomość piszemy od prawej do lewej. Pod każdą literą klucza znajduję się teraz kolumna. Kolumny te zamieniamy miejscami, układając litery klucza w kolejności alfabetycznej. Następnie wiadomość piszemy od góry do dołu.

Szyfr ADFVGX działa tak samo jak szyfr ADFGX, jednakże zamiast tabeli o wymiarach 5x5 używa się tabeli o wymiarach 6x6, w której wpisujemy wszystkie cyfry oraz cały alfabet. "I" oraz "j" traktujemy jako dwie różne litery.

Zaszyfrujmy zdanie "Attack will begin on four o'clock" szyframi ADFGX i ADFVGX kluczem "secret".

ADFGX:

Attack will begin on four o'clock

DA FF FF AD GX.XF AG DF GA GA.GF XA DG DF GG.DX GG AX DX DD.XG DX GX GA DX.GX XF

S	E	C	R	T
D	A	F	F	F
F	A	D	G	X
X	F	A	G	D
F	G	A	G	A
G	F	X	A	D
G	D	F	G	G
D	X	G	G	A
X	D	X	D	D
X	G	D	X	X
G	G	A	D	X
G	X	X	F	X

C	E	R	S	T
F	A	F	D	F
D	A	G	F	X
A	F	G	X	D
A	G	G	F	A
X	F	A	G	D
F	D	G	G	G
G	X	G	D	A
X	D	D	X	D
D	G	X	X	X
A	G	D	G	X
X	X	F	G	X

Szyfrogram:
FDAAXFGXDAXAAFGFDXDGGXFGGGAGGDXDFDFXFGGDXXGGFXDADGADXX
X

3.7 Szyfr z jednorazowym kluczem szyfrującym

Szyfr z jednorazowym kluczem szyfrującym to szyfr Vigenere'a, w którym klucz jest tak samo długi jak tekst jawny, losowy i używa się go tylko raz. Takiego szyfru nie da się złamać, ale klucze trzeba ciągle generować i przesyłać do adresatów co sprawia problemy, ponieważ takie klucze wróg może przejąć.

4. Deszyfracja

4.1 Miara koincydencji.

Bardzo wartościową informacją na temat szyfrów polialfabetycznych jest długość klucza. Jeśli znamy długość klucza, możemy podzielić tekst na części zaszyfrowane tą samą literą klucza i odszyfrować go jak szyfr monoalfabetyczny. Długość klucza możemy znaleźć dzięki

powtarzającym się słowom. Możemy też użyć metody Friedmana i miary koincydencji liter. Jeśli podzielimy tekst na pół i ustawimy te połówki pod sobą to wystąpią pary liter znajdujące się pod sobą. Miara koincydencji liter to szansa wystąpienia takiej pary liter nazywaną kappa. Każdy język ma różną miarę kappa oznaczaną k_p. Zaś jako k_r oznaczamy miarę koincydencji w tekście losowym, dla alfabetu łacińskiego wynosi ona 0,0385.
Friedman stworzył metodę określania długości klucza dzięki mierze koincydencji liter.
Najpierw piszemy kryptogram dwa razy, pod sobą. Następnie obliczamy parametr k i przesuwamy fazowo dolny kryptogram. Powtarzamy ten proces w kółko. Jeśli przesunięcie fazowe jest równe długości klucza, to parametr k zmieni się skokowo i będzie bliski k_p, zaś jeśli nie, to będzie ona bliska k_r.

4.2 Metoda słów prawdopodobnych
W wiadomościach często można przewidzieć, gdzie będą pewne słowa. Np. Polacy odszyfrowujący Enigmę szukali słów heilhitler.

4.3 Symetria pozycji Kerckhoffsa
Auguste Kerckhoffs, holenderski kryptolog z XIX w. , stworzył metodę łamania szyfru Vigenere' a. Zauważył on, że w alfabecie podstawowym szyfru Vigenere'a litery zawsze mają taką odległość pomiędzy sobą, nieważne jak został on przesunięty. Znając długość klucza, możemy dzięki temu łatwo odszyfrować dowolną wiadomość.
Kerckhoffs jako przykład podał wiadomość
RBNBJ JHGTS PTABG JXZBG JICEM QAMUW
IVGAG NEIMW REZKZ SUABR RBPBJ CGYBG
JJMHE NPMUZ CHGWO UDCKO JKKBC PVPMJ
NPGKW PWADW CPBVM RBZBH JWZDN MEUAO
JFBMN KEXHZ AWMWK AQMTG LVGHC QBMWE
Kerckhoffs podzielił tekst na części po pięć znaków, ponieważ w jego przykładzie klucz ma pięć znaków. Kerckhoffs założył że wiadomość zaczyna się od legeneralwolseleytelegraphie. Podpiszmy prawdopodobną frazę pod pierwsze znaki kryptogramu.
RBNBJ JHGTS PTABG JXZBG JICEM QAM
legen eralw olsel eytel egrap hie
Stwórzmy tabelę z dopasowanymi znakami.

	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
1					J			q				R			p											
2					B		I		a			T						H							x	
3	G				M		n											c	a	z						
4	E				B							T														
5					z							g		j		M							S			

Jak widać w tabeli 2 i 4 litera klucza są takie same.

	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
1					J			q				R			p											
2	e				B		I		a			T						H							x	
3	G				M		n											c	a	z						
5					z							g		j		M							S			

Uzupełnijmy tabelę o litery wynikające z relacji wiążące wiersze.

	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
1			g	h	j		m	q	n		x	r	e	s	p		b		i	c	a	z		t		
2	e	s	p		b		I	c	a	z		t					g	h	j		m	q	n		x	r
3	g	h	j		m	q	n		x	r	e	s	p		b		I	c	a	z		t				
5		i	c	a	z		t					g	h	j		M	q	n		x	r	e	S	p		b

Odszyfrujmy dzięki przedstawionym wyżej literom resztę wiadomości:

RBNBJ JHGTS PTABG JXZBG JICEM QAMUW

legen eralw olsel eytel egrap hie__

IVGAG NEIMW REZKZ SUABR RBPBJ CGYBG

s_ail iaqu_ latte n_seu lemen tq_el

JJMHE NPMUZ CHGWO UDCKO JKKBC PVPMJ

eserv ice_e tra__ __r__ e__ec ommun

Kerckhoffs domyślił się, że w drugim wierszu jest fraza attend seulement que.

	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
1			g	h	j	k	m	q	n		x	r	e	s	p		b		i	c	a	z		t		
2	e	s	p		b		I	c	a	z		t					g	h	j	k	m	q	n		x	r
3	g	h	j	k	m	q	n		x	r	e	s	p		b		I	c	a	z		t				
5		I	c	a	z		t					g	h	j	k	M	q	n		x	r	e	S	p		b

Jak widać w alfabecie podstawowym znajduje się słowo RESPUBLICA

	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
1			g	h	j	k	m	q	n		x	r	e	s	p	u	b	l	i	c	a	z		t		
2	e	s	p	u	b	l	I	c	a	z		t					g	h	j	k	m	q	n		x	r
3	g	h	j	k	m	q	n		x	r	e	s	p	u	b	l	I	c	a	z		t				
5	l	I	c	a	z		t					g	h	j	k	M	q	n		x	r	e	S	p	u	b

Teraz odszyfrowanie reszty wiadomości jest bardzo łatwe.