Historia i podstawy kryptografii
Spotkanie 7
Rozwój szyfrów polialfabetycznych w XVI wieku

Jacek Rogowski

I Liceum Ogólnokształcące
w Łowiczu

Szyfry homofoniczne vs. polialfabetyczne

Szyfry homofoniczne i polialfabetyczne są tworzone w celu utrudnienia lub uniemożliwienia analizy częstotliwości przy ich łamaniu. Oba systemy mają swoje zalety (oznaczymy je znakiem $+$) i wady ($-$).

Szyfry homofoniczne

- Tajny alfabet z homofonami ma stały zestaw znaków dla każdej często powtarzającej się litery tekstu jawnego. $(-)$
- Klucz szyfru homofonicznego może mieć duże rozmiary (np. nomenklator) i jego dystrybucja jest kłopotliwa. $(-)$
- Szyfrowanie szyfrem homofonicznym nie wymaga wspomagania dodatkowymi rekwizytami. $(+)$
- Korzystanie z szyfru homofonicznego jest proste i dostępne dla osób niewykwalifikowanych. $(+)$
- Błąd popełniony przy szyfrowaniu jednego znaku nie wpływa negatywnie na poprawność reszty przekazu. $(+)$

Szyfry homofoniczne vs. polialfabetyczne

Szyfry homofoniczne i polialfabetyczne są tworzone w celu utrudnienia lub uniemożliwienia analizy częstotliwości przy ich łamaniu. Oba systemy mają swoje zalety (oznaczymy je znakiem $+$) i wady ($-$).

Szyfry polialfabetyczne

- Szyfr polialfabetyczny ma zmienny zestaw znaków dla każdej litery tekstu jawnego. $(+)$
- Klucz szyfru polialfabetycznego jest niewielki (np. pojedyncze słowo) i jego dystrybucja jest łatwa. $(+)$
- Szyfrowanie szyfrem polialfabetycznym na ogół wymaga wspomagania dodatkowymi rekwizytami. $(-)$
- Korzystanie z szyfru polialfabetycznego jest proste i dostępne dla osób niewykwalifikowanych. $(+)$
- Błąd popełniony przy szyfrowaniu jednego znaku może wpłynąć negatywnie na poprawność reszty przekazu. $(-)$

Johannes Trithemius (1462 – 1516)

J. Trithemius był opatem benedyktyńskim i jednym z najświetniejszych intelektualistów swoich czasów. Zajmował się wieloma dziedzinami, w tym magią.

Napisał traktat o kryptologii *Steganographia* (ok. 1499), w którym rozwinął ideę szyfrów polialfabetycznych wprowadzając nowe narzędzie do szyfrowania, tzw. *tabula recta*, zwaną później **tablicą Trithemiusa**.

Tablica Trithemiusa

Alfabet jawny																								
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tablica Trithemiusa

Algorytm szyfrowania

- Pierwszą literę wiadomości szyfruje się korzystając z alfabetu tajnego znajdującego się w wierszu A.
- Drugą literę wiadomości szyfruje się korzystając z alfabetu tajnego znajdującego się w wierszu B.

$$\vdots$$

- Dwudziestą szóstą literę wiadomości szyfruje się korzystając z alfabetu tajnego znajdującego się w wierszu Z.
- Dwudziesta siódma litera rozpoczyna od początku cykl przechodzenia przez kolejne alfabety.

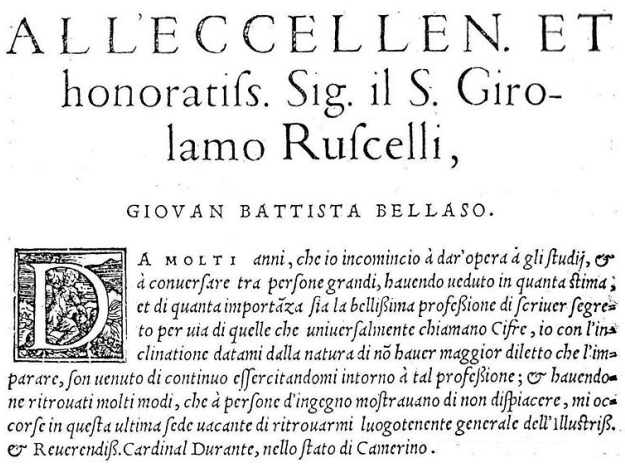
Szyfr Trithemiusa był pierwszym szyfrem polialfabetycznym, w którym zmiana alfabetu odbywa się dla każdej szyfrowanej litery.

Szyfry polialfabetyczne weszły do gry

- Szyfry Albertiego i Trithemiusa są pierwszymi szyframi polialfabetycznymi w historii.
- Oba szyfry są *de facto* zmodyfikowanym szyfrem Cezara, w którym następuje cykliczna wymiana klucza (czyli tajnego alfabetu).
- Przewagą szyfru Albertiego nad szyfrem Trithemiusa jest możliwość wymiany klucza (złożonego z jednej litery i dwóch liczb).
- Zaletą szyfru Trithemiusa jest wprowadzenie zasady szyfrowania każdej litery nowym tajnym alfabetem (co w szyfrze Albertiego jest tylko możliwością), ale ustalona lista kolejnych alfabetów powoduje, że w istocie jest to szyfr „bez klucza".
- Po opublikowaniu algorytmów szyfrów Albertiego i Trithemiusa pojawiło się zapotrzebowanie na kryptosystem łączący zalety obu tych szyfrów, ale pozbawiony ich wad.

Giovan Battista Bellaso (1505 – ?)

O G. B. Bellaso zachowało się bardzo niewiele informacji. ZNie wiadomo nawet, w którym roku zmarł.



ALL'ECCELLEN. ET
honoratiſs. Sig. il S. Giro-
lamo Ruſcelli,

GIOVAN BATTISTA BELLASO.

DA MOLTI anni, che io incomincio à dar'opera à gli ſtudij, & à conuerſare tra perſone grandi, hauendo ueduto in quanta ſtima, et di quanta importãza ſia la belliſſima profeſſione di ſcriuer ſegreto per uia di quelle che uniuerſalmente chiamano Cifre, io con l'inclinatione datami dalla natura di nõ hauer maggior diletto che l'imparare, ſon uenuto di continuo eſſercitandomi intorno à tal profeſſione; & hauendone ritrouati molti modi, che à perſone d'ingegno moſtrauano di non diſpiacere, mi occorſe in queſta ultima ſede uacante di ritrouarmi luogotenente generale dell'Illuſtriſs. & Reuerendiſs. Cardinal Durante, nello ſtato di Camerino.

Bellaso wydał w roku 1553 książkę *La Cifra del Sig. Giovan Battista Bel[l]aso*, w której opisał sposób ustalania tajnego alfabetu dla każdej szyfrowanej litery na podstawie wymiennego klucza. Niestety, jego szyfr znany jest jako **szyfr Vigenere'a**, od nazwiska francuskiego kryptografa, który opisał inny sposób korzystania z klucza w tym szyfrze.

Szyfr Vigenere'a (autor: G. B. Bellaso)

Algorytm szyfrowania

- Kluczem jest dowolny ustalony ciąg liter; na ogół jest to słowo lub zdanie.
- Pierwszą literę wiadomości szyfruje się korzystając z alfabetu tajnego znajdującego się w wierszu, który rozpoczyna się od pierwszej litery klucza.
- Drugą literę wiadomości szyfruje się korzystając z alfabetu tajnego znajdującego się w wierszu, który rozpoczyna się od drugiej litery klucza.

$$\vdots$$

- Po wyczerpaniu liter klucza procedurę zaczyna się od początku używając dla kolejnej litery wiadomości ponownie pierwszej litery klucza itd.

Szyfr Vigenere'a — przykład 1

Klucz: *tajemnica*

Fragment tablicy Trithemiusa:

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

Szyfrowanie:

tekst jawny:	*k*	*r*	*y*	*p*	*t*	*o*	*g*	*r*	*a*	*f*	*i*	*a*
klucz:	**t**	**a**	**j**	**e**	**m**	**n**	**i**	**c**	**a**	**t**	**a**	**j**
tekst tajny:	D	R	H	T	F	B	O	T	A	Y	I	J

Szyfr Vigenere'a — przykład 2

Klucz: *projekt*

Fragment tablicy Trithemiusa:

	Alfabet jawny																								
	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
	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
	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	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
	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	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
	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
	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

Szyfrowanie:

tekst jawny:	*a*	*b*	*r*	*a*	*k*	*a*	*d*	*a*	*b*	*r*	*a*
klucz:	**p**	**r**	**o**	**j**	**e**	**k**	**t**	**p**	**r**	**o**	**j**
tekst tajny:	P	S	F	J	O	K	W	P	S	F	J

Szyfr Vigenere'a – zalety i wady

Zalety szyfru Vigenere'a:

- Polialfabetyczność.
- Łatwość wymiany i uzgodnienia klucza.
- Prostota algorytmu szyfrowania.

Wady szyfru Vigenere'a:

- Litery leżące w odległości równej długości klucza są szyfrowane tym samym szyfrem Cezara.
- Bezpieczeństwo zależne od długości klucza.
- Możliwość stosowania analizy częstotliwości pod warunkiem znajomości długości klucza.
- Możliwość odgadnięcia długości klucza.

Blaise de Vigenère (1523 – 1596)

B. de Vigenère był francuskim dyplomatą, tłumaczem, alchemikiem i kryptografem. Błędnie przypisano mu autorstwo szyfru stworzonego przez Bellasco.

Napisał książkę o kryptografii *Traicté des Chiffres* (1585), w której zawarł obraz wiedzy kryptologicznej swoich czasów oraz rozwinął ideę szyfru z **autokluczem.**

Szyfr z autokluczem – wariant 1 (autor: B. de Vigenère)

Algorytm szyfrowania

- **Kluczem pierwotnym** jest dowolny ustalony ciąg liter; na ogół jest to słowo lub zdanie, choć Vigenère proponował pojedynczą literę.
- Za kluczem pierwotnym dopisuje się tekst jawny otrzymując **pełny klucz** szyfru.
- Korzystając z kolejnych liter klucza pełnego szyfruje się kolejne litery tekstu jawnego w taki sam sposób, jak w szyfrze Vigenera.
- Nie ma potrzeby powtarzania klucza podczas procedury szyfrowania, ponieważ klucz pełny ma długość większą niż tekst jawny.

Szyfr z autokluczem (wariant 1) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**
Klucz pełny: **ctajemnica**

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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**t**	**a**	**j**	**e**	**m**	**n**	**i**	**c**
tekst tajny:	V	T	J	N	Q	Z	V	K	C

Szyfr z autokluczem – wariant 2 (autor: B. de Vigenère)

Algorytm szyfrowania

- **Kluczem pierwotnym** jest dowolny ustalony ciąg liter; na ogół jest to słowo lub zdanie, choć Vigenère proponował pojedynczą literę.
- Za kluczem pierwotnym dopisuje się sukcesywnie kolejne litery tworzonego kryptogramu otrzymując **pełny klucz** szyfru.
- Korzystając z kolejno dopisywanych liter klucza pełnego szyfruje się dalsze litery tekstu jawnego w taki sam sposób, jak w szyfrze Vigenera.
- Nie ma potrzeby powtarzania klucza podczas procedury szyfrowania, ponieważ klucz pełny ma długość większą niż tekst jawny.

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 1

Klucz pełny: **c**

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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**								
tekst tajny:	V								

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 2

Klucz pełny: **cv**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**							
tekst tajny:	V	V							

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 3

Klucz pełny: **cvv**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**						
tekst tajny:	V	V	E						

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 4

Klucz pełny: **cvve**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**	**e**					
tekst tajny:	V	V	E	I					

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 5

Klucz pełny: **cvvei**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**	**e**	**i**				
tekst tajny:	V	V	E	I	U				

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 6

Klucz pełny: **cvveiu**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**	**e**	**i**	**u**			
tekst tajny:	V	V	E	I	U	H			

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 7

Klucz pełny: **cvveiuh**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**	**e**	**i**	**u**	**h**		
tekst tajny:	V	V	E	I	U	H	P		

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 8

Klucz pełny: **cvveiuhp**

Alfabet jawny																								
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
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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**	**e**	**i**	**u**	**h**	**p**	
tekst tajny:	V	V	E	I	U	H	P	R	

Szyfr z autokluczem (wariant 2) — przykład

Tekst jawny: *tajemnica*
Klucz pierwotny: **c**

Krok 9

Klucz pełny: **cvveiuhpr**

Alfabet jawny																								
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	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

Szyfrowanie:

tekst jawny:	*t*	*a*	*j*	*e*	*m*	*n*	*i*	*c*	*a*
klucz:	**c**	**v**	**v**	**e**	**i**	**u**	**h**	**p**	**r**
tekst tajny:	V	V	E	I	U	H	P	R	R

Szyfr z autokluczem – zalety i wady

Zalety szyfru z autokluczem:

- Polialfabetyczność.
- Łatwość wymiany i uzgodnienia klucza pierwotnego.
- Prostota algorytmu szyfrowania.
- Brak okresowości pełnego klucza szyfru.
- Nieprzydatność analizy częstotliwości do łamania szyfru.
- Długość pełnego klucza większa od długości tekstu jawnego.

Wady szyfru z autokluczem:

- Bezpieczeństwo zależne od długości klucza pierwotnego.
- Odgadnięcie fragmentu tekstu jawnego pozwala na odczytanie dalszej części tekstu jawnego.
- W wariancie 1: odgadnięcie długości klucza pierwotnego ułatwia złamanie szyfru.
- W wariancie 2: tekst tajny odsłania dużą część klucza pełnego.
- Błędny wybór alfabetu tajnego uniemożliwia odczytanie wiadomości lub znacznej jej części.