Kryptologia laboratorium 5.

Szyfry podstawieniowe polialfabetyczne

Tomasz Gzella
Instytut Matematyki Stosowanej

WYDZIAŁ FIZYKI TECHNICZNEJ
I MATEMATYKI STOSOWANEJ

POLITECHNIKA
GDAŃSKA

Szyfr Vigenère'a (polialfabetyczny)

Oparty na kluczu K o długości n. Klucz należy przedłużyć do długości tekstu jawnego przez powielenie.
Następnie należy przyporządkować literom (tekstu jawnego i klucza) pozycje liter w alfabecie. Oznaczy te liczby tekście jawnym jako $x = \{x_i\}_{i=1}^{m}$, a w przedłużonym kluczu $K = \{k_1, k_2, ..., k_n, k_{n+1}, ..., k_m\}$. Wystarczy dodać je wg wzoru

$$E_K(x) = x_i + k_i \ mod \ 26$$

otrzymując pozycje liter alfabetu w szyfrogramie $y = \{y_i\}_{i=1}^{m}$.

Szyfr Vigenère'a (polialfabetyczny)

Oparty na kluczu K o długości n. Klucz należy przedłużyć do długości tekstu jawnego przez powielenie.
Następnie należy przyporządkować literom (tekstu jawnego i klucza) pozycje liter w alfabecie. Oznaczy te liczby tekście jawnym jako $x = \{x_i\}_{i=1}^{m}$, a w przedłużonym kluczu $K = \{k_1, k_2, ..., k_n, k_{n+1}, ..., k_m\}$. Wystarczy dodać je wg wzoru

$$E_K(x) = x_i + k_i \ mod \ 26$$

otrzymując pozycje liter alfabetu w szyfrogramie $y = \{y_i\}_{i=1}^{m}$.
Deszyfrowanie przebiega według analogicznego wzoru:

$$D_K(x) = y_i - k_i \ mod \ 26$$

Szyfr Vigenère'a (polialfabetyczny)

Oparty na kluczu K o długości n. Klucz należy przedłużyć do długości tekstu jawnego przez powielenie.
Następnie należy przyporządkować literom (tekstu jawnego i klucza) pozycje liter w alfabecie. Oznaczy te liczby tekście jawnym jako $x = \{x_i\}_{i=1}^{m}$, a w przedłużonym kluczu $K = \{k_1, k_2, ..., k_n, k_{n+1}, ..., k_m\}$. Wystarczy dodać je wg wzoru

$$E_K(x) = x_i + k_i \ mod \ 26$$

otrzymując pozycje liter alfabetu w szyfrogramie $y = \{y_i\}_{i=1}^{m}$.
Deszyfrowanie przebiega według analogicznego wzoru:

$$D_K(x) = y_i - k_i \ mod \ 26$$

Przyjrzyjmy się przykładowi:

tekst jawny:	tajny tekst
klucz:	gdansk

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t
tekst jawny (num):	19	0	9	13	24	19	4	10	18	19

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t
tekst jawny (num):	19	0	9	13	24	19	4	10	18	19
klucz:	g	d	a	n	s	k	g	d	a	n

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t
tekst jawny (num):	19	0	9	13	24	19	4	10	18	19
klucz:	g	d	a	n	s	k	g	d	a	n
klucz (num):	6	3	0	13	18	10	6	3	0	13

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t
tekst jawny (num):	19	0	9	13	24	19	4	10	18	19
klucz:	g	d	a	n	s	k	g	d	a	n
klucz (num):	6	3	0	13	18	10	6	3	0	13
suma mod 26:	25	3	9	0	16	3	10	13	18	6

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t
tekst jawny (num):	19	0	9	13	24	19	4	10	18	19
klucz:	g	d	a	n	s	k	g	d	a	n
klucz (num):	6	3	0	13	18	10	6	3	0	13
suma mod 26:	25	3	9	0	16	3	10	13	18	6
szyfrogram:	Z	D	J	A	Q	D	K	N	S	G

Szyfr Vigenère'a (polialfabetyczny)

tekst jawny:	t	a	j	n	y	t	e	k	s	t
tekst jawny (num):	19	0	9	13	24	19	4	10	18	19
klucz:	g	d	a	n	s	k	g	d	a	n
klucz (num):	6	3	0	13	18	10	6	3	0	13
suma mod 26:	25	3	9	0	16	3	10	13	18	6
szyfrogram:	Z	D	J	A	Q	D	K	N	S	G

Szyfr z autokluczem:

tekst jawny:	t	a	j	n	y	t	e	k	s	t
klucz:	x	t	a	j	n	y	t	e	k	s

Pytanie: jak tutaj wygląda odszyfrowanie?

Oparty na kluczu o długości n^2. Najpierw należy przyporządkować literom (tekstu jawnego i klucza) liczby wg kolejności alfabetu. Tekst jawny dzielimy na bloki długości n (braki uzupełniamy losowo). Klucz długości n^2 zapisujemy w formacie macierzy o wymiarach $n \times n$, którą mnożymy przez bloki tekstu jawnego $(mod 26)$. Otrzymane wyniki zamieniamy na litery.

Przykładowe szyfrowanie dla $n = 2$ przebiega następująco:
tekst jawny:
laborki $=$

Szyfr Hilla

Oparty na kluczu o długości n^2. Najpierw należy przyporządkować literom (tekstu jawnego i klucza) liczby wg kolejności alfabetu. Tekst jawny dzielimy na bloki długości n (braki uzupełniamy losowo). Klucz długości n^2 zapisujemy w formacie macierzy o wymiarach $n \times n$, którą mnożymy przez bloki tekstu jawnego $(mod 26)$. Otrzymane wyniki zamieniamy na litery.

Przykładowe szyfrowanie dla $n = 2$ przebiega następująco:
tekst jawny:
laborki $= \begin{bmatrix} 11 & 0 & 1 & 14 & 17 & 10 & 8 \end{bmatrix}$
tekst dzielimy na fragmenty o długości $n = 2$:
la $= \begin{bmatrix} 11 & 0 \end{bmatrix}$, bo $= \begin{bmatrix} 1 & 14 \end{bmatrix}$, rk $= \begin{bmatrix} 17 & 10 \end{bmatrix}$, i $= \begin{bmatrix} 8 & 14 \end{bmatrix}$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $=$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix}$

Szyfr Hilla - wybór klucza

Przykładowy klucz: $\text{list} = \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \left[\begin{array}{cccc} 11 & 8 & 18 & 19 \end{array}\right] \rightarrow \left[\begin{array}{cc} 11 & 8 \\ 18 & 19 \end{array}\right]$

$$det(list) = det\left[\begin{array}{cc} 11 & 8 \\ 18 & 19 \end{array}\right] =$$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

$$det(list) = det \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix} = 65 \ mod \ 26 = 13$$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \left[\begin{array}{cccc} 11 & 8 & 18 & 19 \end{array}\right] \rightarrow \left[\begin{array}{cc} 11 & 8 \\ 18 & 19 \end{array}\right]$

$$det(list) = det\left[\begin{array}{cc} 11 & 8 \\ 18 & 19 \end{array}\right] = 65 \ mod \ 26 = 13$$

Macierz klucza musi być odwracalna, by odszyfrować wiadomość.
Jakie są warunki na odwracalność macierzy?

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

$$det(list) = det \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix} = 65 \ mod \ 26 = 13$$

Macierz klucza musi być odwracalna, by odszyfrować wiadomość. Jakie są warunki na odwracalność macierzy?

- $A \in M_{n \times n}$
- istnieje $|A|^{-1}$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

$$det(list) = det \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix} = 65 \ mod \ 26 = 13$$

Macierz klucza musi być odwracalna, by odszyfrować wiadomość.
Jakie są warunki na odwracalność macierzy?

- $A \in M_{n \times n}$
- istnieje $|A|^{-1}$

$\begin{bmatrix} 1^{-1} & 3^{-1} & 5^{-1} & 7^{-1} & 9^{-1} & 11^{-1} & 15^{-1} & 17^{-1} & 19^{-1} & 21^{-1} & 23^{-1} & 25^{-1} \end{bmatrix} =$

$\begin{bmatrix} 1 & 9 & 21 & 15 & 3 & 19 & 7 & 23 & 11 & 5 & 17 & 25 \end{bmatrix}$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

$$det(list) = det \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix} = 65 \ mod \ 26 = 13$$

Macierz klucza musi być odwracalna, by odszyfrować wiadomość. Jakie są warunki na odwracalność macierzy?

- $A \in M_{n \times n}$
- istnieje $|A|^{-1}$

$\begin{bmatrix} 1^{-1} & 3^{-1} & 5^{-1} & 7^{-1} & 9^{-1} & 11^{-1} & 15^{-1} & 17^{-1} & 19^{-1} & 21^{-1} & 23^{-1} & 25^{-1} \end{bmatrix} =$

$\begin{bmatrix} 1 & 9 & 21 & 15 & 3 & 19 & 7 & 23 & 11 & 5 & 17 & 25 \end{bmatrix}$

Klucz **list** jest nieodpowiedni! Zaszyfrowanej wiadomości nie da się odszyfrować! Musimy wybrać inny klucz:

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

$$det(list) = det \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix} = 65 \ mod \ 26 = 13$$

Macierz klucza musi być odwracalna, by odszyfrować wiadomość. Jakie są warunki na odwracalność macierzy?

- $A \in M_{n \times n}$
- istnieje $|A|^{-1}$

$\begin{bmatrix} 1^{-1} & 3^{-1} & 5^{-1} & 7^{-1} & 9^{-1} & 11^{-1} & 15^{-1} & 17^{-1} & 19^{-1} & 21^{-1} & 23^{-1} & 25^{-1} \end{bmatrix} =$

$\begin{bmatrix} 1 & 9 & 21 & 15 & 3 & 19 & 7 & 23 & 11 & 5 & 17 & 25 \end{bmatrix}$

Klucz **list** jest nieodpowiedni! Zaszyfrowanej wiadomości nie da się odszyfrować! Musimy wybrać inny klucz:

$$\text{text} = \begin{bmatrix} 19 & 4 & 23 & 19 \end{bmatrix}$$

Szyfr Hilla - wybór klucza

Przykładowy klucz: list $= \begin{bmatrix} 11 & 8 & 18 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix}$

$$det(list) = det \begin{bmatrix} 11 & 8 \\ 18 & 19 \end{bmatrix} = 65 \ mod \ 26 = 13$$

Macierz klucza musi być odwracalna, by odszyfrować wiadomość. Jakie są warunki na odwracalność macierzy?

- $A \in M_{n \times n}$
- istnieje $|A|^{-1}$

$\begin{bmatrix} 1^{-1} & 3^{-1} & 5^{-1} & 7^{-1} & 9^{-1} & 11^{-1} & 15^{-1} & 17^{-1} & 19^{-1} & 21^{-1} & 23^{-1} & 25^{-1} \end{bmatrix} =$

$\begin{bmatrix} 1 & 9 & 21 & 15 & 3 & 19 & 7 & 23 & 11 & 5 & 17 & 25 \end{bmatrix}$

Klucz **list** jest nieodpowiedni! Zaszyfrowanej wiadomości nie da się odszyfrować! Musimy wybrać inny klucz:

$$\text{text} = \begin{bmatrix} 19 & 4 & 23 & 19 \end{bmatrix} \rightarrow \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}$$

Następnie wykonujemy mnożenia macierzy modulo 26:

$$text \cdot la = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 11 & 0 \end{bmatrix}^T =$$

Szyfr Hilla - szyfrowanie

Następnie wykonujemy mnożenia macierzy modulo 26:

$$text \cdot la = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 11 & 0 \end{bmatrix}^T = \begin{bmatrix} 209 \\ 253 \end{bmatrix} mod\ 26 = \begin{bmatrix} 1 \\ 19 \end{bmatrix} = BT$$

Szyfr Hilla - szyfrowanie

Następnie wykonujemy mnożenia macierzy modulo 26:

$$text \cdot la = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 11 & 0 \end{bmatrix}^T = \begin{bmatrix} 209 \\ 253 \end{bmatrix} mod\ 26 = \begin{bmatrix} 1 \\ 19 \end{bmatrix} = BT$$

$$text \cdot bo = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 1 & 14 \end{bmatrix}^T = \begin{bmatrix} 75 \\ 289 \end{bmatrix} mod\ 26 = \begin{bmatrix} 23 \\ 3 \end{bmatrix} = XD$$

$$text \cdot rk = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 17 & 10 \end{bmatrix}^T = \begin{bmatrix} 363 \\ 581 \end{bmatrix} mod\ 26 = \begin{bmatrix} 25 \\ 9 \end{bmatrix} = ZJ$$

$$text \cdot i = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 8 & 14 \end{bmatrix}^T = \begin{bmatrix} 208 \\ 450 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 8 \end{bmatrix} = AI$$

Szyfr Hilla - szyfrowanie

Następnie wykonujemy mnożenia macierzy modulo 26:

$$text \cdot la = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 11 & 0 \end{bmatrix}^T = \begin{bmatrix} 209 \\ 253 \end{bmatrix} mod\ 26 = \begin{bmatrix} 1 \\ 19 \end{bmatrix} = BT$$

$$text \cdot bo = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 1 & 14 \end{bmatrix}^T = \begin{bmatrix} 75 \\ 289 \end{bmatrix} mod\ 26 = \begin{bmatrix} 23 \\ 3 \end{bmatrix} = XD$$

$$text \cdot rk = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 17 & 10 \end{bmatrix}^T = \begin{bmatrix} 363 \\ 581 \end{bmatrix} mod\ 26 = \begin{bmatrix} 25 \\ 9 \end{bmatrix} = ZJ$$

$$text \cdot i = \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} \cdot \begin{bmatrix} 8 & 14 \end{bmatrix}^T = \begin{bmatrix} 208 \\ 450 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 8 \end{bmatrix} = AI$$

szyfrogram: BTXDZJAI

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} =$$

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} =$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \; mod \; 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1} \begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \; mod \; 26 =$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1}\begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \ mod \ 26 =$$

$$3\begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \ mod \ 26 =$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1} \begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \ mod \ 26 =$$

$$3 \begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \ mod \ 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1} \begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \ mod \ 26 =$$

$$3 \begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \ mod \ 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Pytanie: w jaki sposób odszyfrować wiadomość zapisaną przy pomocy tego szyfru?

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \; mod \; 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1} \begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \; mod \; 26 =$$

$$3 \begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \; mod \; 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Pytanie: w jaki sposób odszyfrować wiadomość zapisaną przy pomocy tego szyfru?

$$\begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} BT =$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1}\begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \ mod \ 26 =$$

$$3\begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \ mod \ 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Pytanie: w jaki sposób odszyfrować wiadomość zapisaną przy pomocy tego szyfru?

$$\begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} BT = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 19 \end{bmatrix} =$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \; mod \; 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1} \begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \; mod \; 26 =$$

$$3 \begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \; mod \; 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Pytanie: w jaki sposób odszyfrować wiadomość zapisaną przy pomocy tego szyfru?

$$\begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} BT = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 19 \end{bmatrix} =$$

$$= \begin{bmatrix} 271 \\ 104 \end{bmatrix} \; mod \; 26$$

Szyfr Hilla - deszyfrowanie

$$det(text) = det\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod\ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1}\begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \ mod\ 26 =$$

$$3\begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Pytanie: w jaki sposób odszyfrować wiadomość zapisaną przy pomocy tego szyfru?

$$\begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} BT = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 19 \end{bmatrix} =$$

$$= \begin{bmatrix} 271 \\ 104 \end{bmatrix} \ mod\ 26 = \begin{bmatrix} 11 \\ 0 \end{bmatrix}$$

$$det(text) = det \begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix} = 269 \ mod \ 26 = 9,$$

$$\begin{bmatrix} 19 & 4 \\ 23 & 19 \end{bmatrix}^{-1} = 9^{-1} \begin{bmatrix} 19 & -4 \\ -23 & 19 \end{bmatrix} \ mod \ 26 =$$

$$3 \begin{bmatrix} 19 & 22 \\ 3 & 19 \end{bmatrix} \ mod \ 26 = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix}.$$

Pytanie: w jaki sposób odszyfrować wiadomość zapisaną przy pomocy tego szyfru?

$$\begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} BT = \begin{bmatrix} 5 & 14 \\ 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 19 \end{bmatrix} =$$

$$= \begin{bmatrix} 271 \\ 104 \end{bmatrix} \ mod \ 26 = \begin{bmatrix} 11 \\ 0 \end{bmatrix} = la \quad itd.$$