Plan wykładu

- Wprowadzenie
- Kryptografia symetryczna
  - Podstawowe algorytmy symetryczne
  - Podstawy kryptoanalizy
  - Algorytmy DES i AES
- Kryptografia z kluczem publicznym
  - Elementy teorii liczb
  - Algorytm RSA
- Podpis cyfrowy
  - Definicja, własności
  - Algorytmy podpisu cyfrowego
  - Zastosowania
- Jednokierunkowe funkcje skrótu
  - Definicja, własności ogólne
  - Przykładowe funkcje skrótu
  - Zastosowania
- Podstawowe informacje na temat kodów detekcji i korekcji błędów.

Literatura

Literatura

[1] M. Karbowski, *Podstawy kryptografii*, Helion, Gliwice, 2014.

[2] N. Koblitz, *Wykład z teorii liczb i kryptografii*, Wydawnictwa Naukowo–Techniczne, Warszawa, 2 ed., 2006.

[3] W. Mao, *Modern Cryptography. Theory and Practice*, Pearson Education, 2004.

[4] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Kryptografia stosowana*, Wydawnictwa Naukowo–Techniczne, Warszawa, 2005. http://www.cacr.math.uwaterloo.ca/hac/.

[5] D. R. Stinson, *Kryptografia*, Wydawnictwa Naukowo–Techniczne, Warszawa, 2005.

[6] W. Trape, L. Washington, *Introduction to Cryptography with Coding Theory*, Pearson Prentice Hall, 2006.

Wprowadzenie

Główny cel zajęć to zapoznanie słuchaczy z metodami służącymi do:

- ochrony prywatności danych elektronicznych,
- autentyfikacji użytkowników systemów komputerowych,
- zabezpieczania przed nieuprawnionymi modyfikacjami danych
- podobnymi zastosowaniami opartymi na technikach kryptograficznych.

Omówione będą również metody zabezpieczania przed przypadkową modyfikacją danych w czasie przesyłania lub przechowywania (metody detekcji i korekcji błędów).

Podstawowe pojęcia

Kryptografia
Kryptografia zajmuje się zagadnieniami związanymi z

- poufnością informacji,
- integralnością danych,
- autentyfikacją danych,
- niezaprzeczalnością operacji wykonanych na danych.

Podstawowym zadaniem kryptografii jest projektowanie systemów zapewniających realizację powyższych zadań, tak zwanych systemów kryptograficznych.

Kryptoanaliza
Kryptoanaliza zajmuje się łamaniem systemów kryptograficznych.

Kryptologia
Kryptologia obejmuje całość zagadnień, którymi zajmuje się kryptografia i kryptoanaliza.

Podstawowe pojęcia

Krótkie spojrzenie na historię kryptografii:

- Początki kryptografii sięgają starożytności, pierwsze udokumentowane zastosowania kryptografii mają ok. 4 000 lat
- W starożytnej Grecji używano prostego "urządzenia szyfrującego" zwanego *Skytale*

- Juliusz Cezar używał do szyfrowania bardzo prostego szyfru podstawieniowego (zwanego obecnie szyfrem Cezara)
- Przez stulecia, w zasadzie do połowy XX wieku, kryptografia była stowana głownie przez wojsko, służby specjalne i dyplomację

Podstawowe pojęcia

Krótkie spojrzenie na historię kryptografii cd.:

- W latach 20-tych XX wieku wprowadzono elektryczne maszyny szyfrujące. Najbardziej znana maszyna tego rodzaju, Enigma, była używana przez armię niemiecką w czasie II wojny światowej.
- Pojawienie się komputerów zmieniło kryptografię, zarówno metody szyfrowania jak i kryptoanalizę
- W latach 70-tych XX pojawiła się kryptografia z kluczem publicznym
- Obecnie: powszechne zastosowanie metod kryptograficznych w działalności cywilnej: telekomunikacja, elektroniczny handel i bankowość, . . .

D. Kahn, *Łamacze kodów. Historia kryptografii*, WNT, Warszawa, 2004.

S. Levy, *Rewolucja w kryptografii*, WNT, Warszawa, 2002.

Podstawowe pojęcia

Osoby wymieniające informację nazywa się tradycyjnie Alicją i Bobem.

Osobę podsłuchującą nazywa się Ewą (*ang.* eavesdrop – podsłuchiwać).

Wiadomość, którą Alicja chce przesłać Bobowi nazywać będziemy tekstem jawnym.

Żeby zapewnić poufność, tekst jawny przed przesłaniem jest szyfrowany.

W ten sposób powstaje tekst zaszyfrowany (kryptogram).

Kryptogram jest przesyłany do Boba przez kanał komunikacyjny.

Po odebraniu kryptogramu Bob deszyfruje go i otrzymuje tekst jawny.

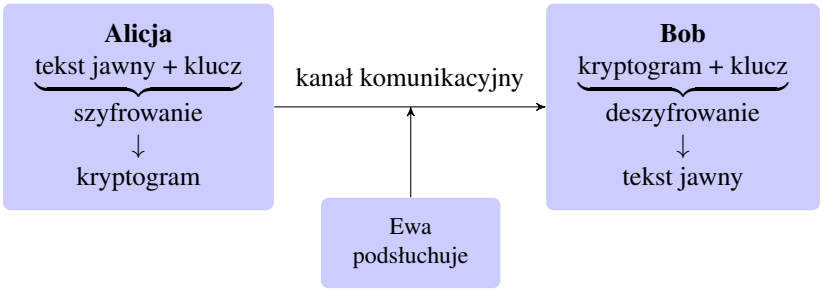
Podstawowe pojęcia

Szyfrowanie i deszyfrowanie odbywa się za pomocą ustalonych wcześniej procedur (stosowane są ustalone protokoły kryptograficzne).

Procedury te zależą zazwyczaj od pewnego, ustalonego wcześniej między Alicją i Bobem ciągu znaków, zwanego kluczem.

Klucz przynajmniej w części jest tajny, zatem jeżeli nawet Ewa przechwyci kryptogram to nie jest w stanie otrzymać tekstu jawnego.

Podstawowe pojęcia



System kryptograficzny nazywamy

- symetrycznym, gdy do szyfrowania i deszyfrowania jest wykorzystywany ten sam klucz;
- asymetrycznym, gdy do szyfrowania i deszyfrowania wykorzystywane są różne klucze.

Podstawowe pojęcia

Przykład – szyfr Cezara
Każdej literze przyporządkowujemy literę stojącą w alfabecie o 3 pozycje dalej.

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

Tekst jawny: TO JEST TEKST PROBNY
Kryptogram: WR MHVW WHNVW SUREQB

Kluczem jest liczba 3 - ilość pozycji, o którą należy przesunąć alfabet.

Możemy oczywiście przesunąć alfabet o inną liczbę pozycji co odpowiada wyborowi innego klucza spośród zbioru $\{1, \ldots, 25\}$.

Deszyfrowanie jest równie proste jak szyfrowanie: każdej literze kryptogramu przyporządkowujemy literę stojącą odpowiednią liczbę pozycji w lewo.

Podstawowe pojęcia

Działania modulo n

...

Podstawowe pojęcia

Szyfr Cezara możemy też opisać bardziej matematycznie. Każdej literze alfabetu przyporządkowujemy liczbę całkowitą od 0 do 25:

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

Jeżeli klucz ma wartość k to szyfrowanie polega na dodawaniu do każdego znaku liczby k modulo 26. Np. $k = 7$:

$$\mathrm{F} = 5 \to 5 + 7 = 13 \mod 26 \to \mathrm{N}$$
$$\mathrm{w} = 22 \to 22 + 7 = 3 \mod 26 \to \mathrm{D}$$

Podstawowe pojęcia

Symetryczny system kryptograficzny

$\mathcal{A}$ – alfabet (zbiór symboli mogących wystąpić w tekście jawnym).

$\mathcal{P}$ – zbiór wszystkich dopuszczalnych tekstów jawnych (elementy $\mathcal{P}$ to ciągi elementów z $\mathcal{A}$).$\mathcal{C}$ – zbiór wszystkich kryptogramów.

$\mathcal{K}$ – przestrzeń kluczy (zbiór wszystkich możliwych kluczy).

Niech dla każdego klucza $k \in \mathcal{K}$ określona będzie funkcja $e_k \colon \mathcal{P} \to \mathcal{C}$ (reguła szyfrowania) oraz funkcja $d_k \colon \mathcal{C} \to \mathcal{P}$ (reguła deszyfrowania) oraz niech funkcje te spełniają warunek:

$$\forall x \in \mathcal{P} \qquad d_k\big(e_k(x)\big) = x.$$

Wtedy uporządkowaną piątkę $\big(\mathcal{P}, \mathcal{C}, \mathcal{K}, \{e_k \colon k \in \mathcal{K}\}, \{d_k \colon k \in \mathcal{K}\}\big)$ nazywamy symetrycznym systemem kryptograficznym (szyfrem symetrycznym).

Podstawowe pojęcia

Przykład – szyfr Cezara

W przypadku szyfru Cezara zachodzi:

$\mathcal{A} = \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$ $\mathcal{K} = \mathbb{Z}_{26}$

$$\forall x \in \mathbb{Z}_{26} \qquad e_k(x) = x + k \mod 26$$
$$\forall y \in \mathbb{Z}_{26} \qquad d_k(x) = x - k \mod 26$$

Podstawowe szyfry symetryczne

Szyfr Cezara jest przykładem ogólnej grupy szyfrów, tak zwanych monoalfabetycznych szyfrów podstawieniowych. W szyfrach tych każdy znak alfabetu jest zastępowany innym znakiem.

Aby takie podstawienie było jednoznaczne, to różnym znakom alfabetu muszą odpowiadać różne znaki po podstawieniu.

Zatem takie podstawienie jest po prostu pewną permutacją symboli alfabetu.

Zatem w przypadku monoalfabetycznego szyfru podstawieniowego kluczem jest wybrana permutacja π.

Jeżeli alfabetem jest $\mathcal{A} = \mathbb{Z}_{26}$, to możliwych jednoparametrowych podstawień jest tyle ile permutacji zbioru 26 elementowego, czyli 26!.

Podstawowe szyfry symetryczne

Przykład – dowolne podstawienie monoalfabetyczne
Rozważmy szyfr w którym kluczem jest następująca permutacja:

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
10	11	12	13	14	15	16	17	18	19	25	24	23	22	21	20	9	8	7	6	5	4	3	2	1	0
K	L	M	N	O	P	Q	R	S	T	Z	Y	X	W	V	U	J	I	H	G	F	E	D	C	B	A

Tekst jawny: TEKST PROBNY
Kryptogram: GOZHG UIVLWB

Zatem w przypadku szyfru podstawieniowego kluczem jest wybrana permutacja π:

$$\forall x \in \mathcal{A} \qquad e_\pi(x) = \pi(x) = y$$
$$d_\pi(y) = \pi^{-1}(y) = x$$

Szyfr Cezara jest szczególnym przypadkiem monoalfabetycznego szyfru podstawieniowego, w którym z wszystkich 26! permutacji jako klucze wykorzystuje się tylko 26 permutacji (przestawienia cykliczne).

Podstawowe szyfry symetryczne

Najprostszą metodą kryptoanalizy jest wyczerpujące przeszukanie przestrzeni kluczy (ang. exhaustive key search, brute force).

Metoda ta polega na tym, że deszyfrujemy kryptogram kolejno z wykorzystaniem wszystkich kluczy z przestrzeni kluczy i sprawdzamy czy po deszyfrowaniu otrzymujemy sensowny tekst.

Przed wyczerpującym przeszukiwaniem przestrzeni kluczy zabezpieczyć się możemy wybierając szyfr z odpowiednio dużą przestrzenią kluczy.

Podstawowe szyfry symetryczne

Przykład – kryptoanaliza szyfru Cezara
Załóżmy, że wiemy, że poniższy kryptogram powstał przy użyciu szyfru Cezara, ale nie znamy klucza:

OVCTXSKVEQ

Zastosujmy wyczerpujące przeszukiwanie przestrzeni kluczy:

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
⋮																									

$k = 1$: OVCTXSKVEQ $\rightarrow$ NUBSWRJUDP
$k = 2$: OVCTXSKVEQ $\rightarrow$ MTARVQITCO
$k = 3$: OVCTXSKVEQ $\rightarrow$ LSZQUPHSBN
$k = 4$: OVCTXSKVEQ $\rightarrow$ KRYPTOGRAM

Podstawowe szyfry symetryczne

Przestrzeń kluczy szyfru Cezara liczy 26 elementów, dlatego atak metodą wyczerpującego przeszukania przestrzeni kluczy jest w tym wypadku możliwy.

Przestrzeń kluczy ogólnego monoalfabetycznego szyfru podstawieniowego liczy

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4 \cdot 10^{26} \approx 2^{88}$$

elementów.

Atak metodą wyczerpującego przeszukania przestrzeni kluczy jest w tym wypadku niemożliwy.

Szyfry permutacyjne

Rozważane dotąd szyfry były szyframi podstawieniowymi: w kryptogramie każda litera tekstu jawnego była zastępowana inną literą.

W szyfrach permutacyjnych litery pozostają niezmienione, zmienia się tylko ich położenie.

W takim szyfrze kluczem jest stała permutacja, π.

Niech, na przykład:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 5 & 3 & 2 & 6 \end{pmatrix}$$

a tekstem jawnym będzie:

To jest prosty tekst jawny.

T	o	j	e	s	t	p	r	o	s	t	y	t	e	k	s	t	j	a	w	n	y	x	x	x	x	x
1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7	1	2	3	4	5	6	7
e	p	t	s	j	o	t	y	e	r	y	s	o	t	j	n	k	a	t	s	w	x	x	y	x	x	x	x

To jest prosty tekst jawny $\rightarrow$ eptsjotyerysotjnkatswxxyxxxx

Transpozycje kolumn

Przykładem szyfru permutacyjnego jest transpozycja kolumn ze słowem kluczowym.[1mm]

1. Wybieramy słowo kluczowe, np:
   TABLICZKA
2. Tekst jawny zapisujemy poziomo, wiersze mają długość taką, jak słowo kluczowe:

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

3. Dopełniamy brakujące miejsca dowolnymi literami.
4. Numerujemy kolumny według kolejności alfabetycznej liter w kluczu (gdy litery się powtarzają, numerujemy od lewej).

Transpozycje kolumn

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

5. Kryptogram tworzymy zapisując kolumny jako wiersze, w kolejności określonej przypisanymi numerami:
   UJDO SSFX TEOW WTSI JYAN IKYX AMZA TUTR PEZA

6. Długość kolumn ustalamy na podstawie długości klucza. Gdy szyfrowany tekst jest bardzo długi możemy umówić się, że długość kolumn wynosi n i podzielić tekst na bloki długości $n\times$(długość klucza).

Tego rodzaju szyfr był używany przez niemiecką siatkę szpiegowską w Brazylii do kontaktów z Berlinem w czasie drugiej wojny światowej.

Podstawy kryptoanalizy

We współczesnej kryptografii przyjmuje się tak zwaną zasadę Kerckhoffa sformułowaną w roku 1882 w pracy „Kryptografia wojskowa":

> Bezpieczeństwo systemu kryptograficznego powinno opierać sie na kluczu a nie na tajności samej metody szyfrowania. Innymi słowy zawsze należy zakładać, że osoba podsłuchująca wie jaka metoda jest wykorzystywana do szyfrowania nie zna tylko zastosowanego klucza.

Podstawy kryptoanalizy

Uzasadnienie zasady Kerckhoffa:

- Argumenty historyczne:
  Enigma – niemiecka maszyna szyfrująca używana w czasie II Wojny Światowej.
  Polscy kryptoanalitycy, którzy złamali szyfr Enigmy znali zasadę działania Enigmy.
  Maszyna szyfrująca Purple – maszyna używana przez Japończyków w czasie II Wojny Światowej do szyfrowania korespondencji dyplomatycznej.
  Alianci nigdy nie zdobyli nienaruszonego egzemplarza maszyny Purple, nawet po wojnie, ale mimo to amerykańscy kryptoanalitycy złamali szyfr Purple.

- Kryptografia stosowana we współczesnych zastosowaniach informatycznych – stosowane algorytmy są publicznie znane.

Podstawy kryptoanalizy

Nawet jeżeli podsłuchiwacz zna metodę szyfrowania, to możliwe są różne rodzaje ataków na system kryptograficzny:

- **Tylko tekst zaszyfrowany** Kryptoanalityk zna tylko kryptogram.

- **Znany tekst jawny** Kryptoanalityk zna tekst jawny oraz odpowiadający mu kryptogram.Wbrew pozorom to częsta sytuacja – znamy jeden komunikat nie znamy innych zaszyfrowanych tym samym kluczem.Przykłady – ENIGMA i komunikaty meteorologiczne, standardowe komunikaty w rodzaju magłówków plików.

- **Wybrany tekst jawny** Kryptoanalityk może wybrać tekst jawny i poznać odpowiadający mu kryptogram (np. możemy podsunąć tekst do zaszyfrowania).

- **Wybrany kryptogram** Kryptoanalityk może poznać tekst jawny odpowiadający wybranemu kryptogramowi.

Kryptoanaliza podstawienia monoalfabetycznego

Rozważmy najpierw najsłabszy atak, czyli atak typu „tylko szfrogram".

Najprostsza metoda kryptoanalizy czyli wyczerpujące przeszukanie przestrzeni kluczy jest w przypadku ogólnego podstawienia monoalfabetycznego bezużyteczna.

W języku naturalnym różne litery występują z różną częstością, to znaczy niektóre litery pojawiają się w tekście średnio częściej niż inne.

W podstawieniu monoalfabetycznym danej literze odpowiada inna, ale zawsze ta sama litera. Zatem w kryptogramie

zaszyfrowanym za pomocą podstawienia monoalfabetycznego pozostają różnice w częstości występowania różnych liter.

Metoda kryptoanalizy podstawienia monoalfabetycznego za pomocą analizy częstości została po raz pierwszy zaproponowana w IX wieku przez arabskiego uczonego i filozofa Al-Kindiego.

Częstości występowania poszczególnych liter

Litera	Język angielski	Język polski	Litera	Język angielski	Język polski
A	0,082	0,074	N	0,067	0,044
B	0,015	0,014	O	0,075	0,061
C	0,028	0,033	P	0,019	0,025
D	0,043	0,028	Q	0,001	0,001
E	0,127	0,065	R	0,060	0,035
F	0,022	0,002	S	0,063	0,035
G	0,020	0,013	T	0,091	0,030
H	0,061	0,009	U	0,028	0,018
I	0,070	0,072	V	0,010	0,001
J	0,002	0,018	W	0,023	0,035
K	0,008	0,026	X	0,001	0,001
L	0,040	0,019	Y	0,020	0,034
M	0,024	0,027	Z	0,001	0,049

Częstości występowania poszczególnych liter

Litery specyficzne dla języka polskiego[3mm]

Litera	Prawdop.	Litera	Prawdop.
ą	0,0093	ó	0,0071
ć	0,0042	ś	0,0066
ę	0,0120	ź	0,0007
ł	0,0227	ż	0,0079
ń	0,0013		

Analiza częstości pojedynczych liter

Ze względu na częstość występowania litery w języku angielskim dzieli się na następujące grupy:[2mm]

E	prawdop. ok. 0.120
T, A, O, I, N, S, H, R	prawdop. między 0.06 i 0.09
D, L	prawdop. ok. 0.04
C, U, M, W, F, G, Y, P, B	prawdop. między 0.015 i 0.028
V, K, J, X, Q, Z	prawdop. poniej 0.01

Homofony

Homofony to różne znaki odpowiadające tej samej literze.

Możemy na przykład każdej literze alfabetu przyporządkować liczbę dwucyfrową. Literom występującym częściej przyporządkowujemy więcej liczb dwucyfrowych.

A	52, 63, 74	H	53, 64, 75	O	54, 65, 76	V	11
B	27, 38	I	55, 66, 77	P	28, 39	W	24, 35
C	21, 32	J	13	Q	15	X	14
D	41, 43, 45	K	12	R	56, 67, 78	Y	29, 31
E	51, 62, 73, 84	L	42, 44, 46	S	81, 85, 89	Z	16
F	25, 36	M	23, 34	T	83, 87, 91		
G	26, 37	N	93, 95, 97	U	22, 33		

EMENTALER $\rightarrow$ 512362938352427356

Symbole puste to symbole, które nie odpowiadają żadnym znakom tekstu jawnego. Dodawane są w celu utrudnienia kryptoanalizy.

Np. w powyższym przykładzie symbole puste: 47, 99.

EMENTALER $\rightarrow$ 51236247938352427356

Szyfrowanie digramów

Możemy również szyfrować nie pojedyncze litery ale większe grupy kolejnych liter, np. digramy (dwie kolejne litery).

Częstości występowania digramów są rozłożone bardziej równomiernie niż częstości pojedynczych liter dlatego analiza częstości jest w tym przypadku trudniejsza.

Przykładem szyfru opartego o digramy jest tak zwany system Playfair'a, używany przez Brytyjczyków w czasie wojen burskich i I wojny światowej.

Przykładem szyfru pozwalającego szyfrować grupy liter dowolnej długości jest szyfr Hilla, wynaleziony przez Lestera Hilla w roku 1929.

System Playfair'a

Wykorzystujemy 25 liter alfabetu angielskiego (J utożsamiamy z I).

Wybieramy hasło (dowolny ciąg liter), np.: TAKIE HASLO.

Wpisujemy wszystkie 25 liter alfabetu w kwadrat 5×5. Najpierw wpisujemy hasło, pomijając powtarzające się litery, a następnie pozostałe litery w kolejności alfabetycznej.

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

Tekst jawny dzielimy na grupy dwuliterowe (jeżeli tekst ma nieparzystą liczbę liter to dodajemy na końcu ustaloną literę, np. X).

KRYPTOGRAM $\rightarrow$ KR|YP|TO|GR|AM

System Playfair'a

Każda para liter wyznacza rogi prostokąta. Litery te zastępujemy literami stojącymi w pozostałych rogach prostokąta (zachowując odpowiedni porządek).

Jeżeli litery stoją w jednym wierszu lub jednej kolumnie to zastępujemy je literami stojącymi na prawo od nich.

Jeżeli w tym wypadku litera będzie położona w ostatniej kolumnie z prawej strony to wtedy zastępujemy ją pierwszą literą wiersza.

KR|YP|TO|GR|AM

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

KR $\rightarrow$ IQ | YP $\rightarrow$ WR | TO $\rightarrow$ IH | GR $\rightarrow$ MU | AM $\rightarrow$ ED [3mm] KRYPTOGRAM $\rightarrow$ IQWRIHMUED