Matematyka dla Ciekawych Świata Ćwiczenia 1, 2 lutego 2017

Metody szyfrowania

Barbara Roszkowska Lech

Wydz. MiNI Politechnika Warszawska

SZYFR CEZARA

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
Numer litery	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
Alfabet zaszyfrowany	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

Uwaga. W poniższych zadaniach szyfrujemy znaki 26 literowego alfabetu przyporządkowując im liczby ze zbioru {0,1,2,…, 25}. (chyba, że z treści zadania wynika cos innego)

.

ZADANIA BARDZO ŁATWE

1. Przechwyciłeś zaszyfrowaną wiadomość: ABACDGB_AHBIJKLŁTD. Udało się podejrzeć drugie słowo jeszcze nie zaszyfrowanej wiadomości :_ SZYFRUJĄCE. Odczytaj wiadomość.

2. Szyfr Zakonu Krzyżackiego- podstawą są trzy litery L, S, K (pierwsze litery niemieckich słów L lesen czytać, S swigen – milczeć, K keren obracać). Każdy wyraz w tekście zaszyfrowanym rozpoczynał się od jednej z tych liter- S na początku oznaczało, że należy ten wyraz pominąć, L że należy to co jest po L przeczytać, a K że należy przeczytać wspak. Rozszyfruj zdanie STU KOT LJEST KOZDRAB SOK LTRUDNE KEINADAZ.

3. **Kryptosystem Vigenera.** Zaszyfruj swoje imię i nazwisko korzystając z tabelki Viegenere z kluczem „CIEKAWI”

4. Zaszyfruj MATEMATYKA za pomocą kryptosystemu Viegenera korzystając z autoklucza pierwsza litera C. .

5. Odszyfruj wiadomość zaszyfrowaną szyfrem Polibliusza 43 13 24 43 31 15 44 11 24 33 15.

ZADANIA ŁATWE

6. Funkcja szyfrująca jest wielomianem $e(x) = ax^3 + bx^2 + cx + d$. Szyfrujemy wszystkie liczby naturalne. Zaszyfruj swoje imię wiedząc, że -2 oraz 3 szyfrują się tak samo, a+b = c+d, 2 oraz -1 szyfrują się odpowiednio jako -4, 8.

7. Funkcja szyfrująca jest postaci: e(x) = reszta z dzielenia x przez pewną liczbę naturalną n. e(47)=11, e(36)=0. Znajdź e(11)

8. Funkcja szyfrująca e(x) = reszta z dzielenia x^3 przez 15. Zaszyfrować wiadomość 2,4,3. Znaleźć funkcję deszyfrującą**.**

9. Funkcja szyfrująca zdefiniowana jest następująco: e(x) = reszta z dzielenia x + k przez pewną liczbę n. Znaleźć najmniejsze, takie k oraz n , dla których wiadomość *ZS* została zaszyfrowana jako *CY*. Odszyfrować wiadomość: *ZLRVQD*.

10. Rozszyfruj podane zdania stosując w jednym zdaniu szyfr Cezara, a w drugim szyfr Playfaira poznany na wykładzie

    a) DEBRGVCBIURZDF GUXJLH CGDQLH XCBMFLH NOXFCD PXFKD

    b) UMRGUMSZOUEK MH LB OU XZ HA QYOM ZG

11. Oszacować liczbę możliwych kluczy w krypto systemach Cezara, Playfaira i Viegenera (zależy od długości klucza).

12. Funkcja szyfrująca zdefiniowana jest następująco: e(x) = reszta z dzielenia iloczynu ax przez pewną liczbę n. (a jest liczbą naturalną mniejszą od n). Sprawdzić szyfrowanie w przypadku n=26 oraz a= 3, 7, 9. Czy a może być równe 2? a 13?

13. Odczytaj kryptogramy. Ile rozwiązań ma każdy z nich? (Różnym literom odpowiadają różne cyfry)

$$\begin{array}{cccccc} & & L & I & S & \\ + & S & Z & U & K & A \\ \hline & M & Y & S & Z & Y \end{array} \qquad + \begin{array}{cccccc} & W & I & L & K & \\ & & N & I & E & \\ \hline & & & J & E & \\ \hline L & U & D & Z & I & \end{array}.$$

14. Czy podstawiając za każdą literę inna cyfrę w kryptogramie AB · CD = EEFF można otrzymać poprawne mnożenie?

15. Reszta z dzielenia kwadratu pewnej liczby *a* przez liczbę pierwszą *p* jest równa 1. Znaleźć resztę z dzielenia liczby *a* przez *p*.

16. Funkcja szyfrująca liczbie naturalnej k przyporządkowuje k-ty wyraz pewnego ciągu geometrycznego. Zaszyfrować 26, wiedząc, że 14 oraz 2 szyfrują się kolejno jako 40960 i 10.

17. Jakie wspólne dzielniki mają liczby n oraz n+6, gdy n jest liczbą naturalną.

18. Dane są liczby całkowite k, l takie, że liczba k+2l jest podzielna przez 3. Wykaż, że liczba 2k+ l też jest podzielna przez 3.

19. Dane są liczby całkowite k, l, m takie, że liczba 2k + 3l +4m jest podzielna przez 5. Wykaż, że liczba k+ 2m+ 4l też jest podzielna przez 5.

ZADANIA NIECO TRUDNIEJSZE

20. Funkcja szyfrująca 2 elementowe bloki wiadomości x_1, x_2 koduje je jako współrzędne punktu symetrycznego do punktu (x_1 , x_2), względem punktu P. Znajdź współrzędne punktu P jeśli wiesz, że jest on odległy od (4,6) o $\sqrt{13}$, natomiast punkt (2,2) jest zaszyfrowany jako punkt odległy od (4,6) o $2\sqrt{10}$.

21. Naczelnik w więzieniu w którym znajduje się 100 więźniów każdemu więźniowi zapisał losowo na czole jedną z liczb naturalnych od 0 do 99. Liczby mogą się powtarzać. Żaden więzień nie zna liczby zapisanej na swoim czole ale widzi liczby zapisane na czołach współwięźniów. Naczelnik obiecał wszystkim wolność, jeśli chociaż jeden z nich odgadnie liczbę wypisaną na jego czole. Więźniowie po zapisaniu liczb na czołach nie mogą się komunikować, ale mogą opracować wcześniej strategię. Jaką szansę na wolność mają więźniowie gdy będą losowo wybierali liczbę. Czy istnieje strategia gwarantująca wolność wszystkim więźniom?

22. Jaką resztę z dzielenia przez 7 daje liczba 2^{2017}?

23. Znajdź cyfrę jedności liczby $1 + 2^2 + 3^3 + 4^4 + 5^5 + 6^6 + 7^7 + 8^8 + 9^9 + 10^{10}$.

24. Uzasadnij, że liczba $321^{654} + 123^{456}$ jest podzielna przez 10.

25. Znajdź dziesięć kolejnych nieparzystych liczb naturalnych, których suma jest podzielna przez 99.

26. Znajdź najmniejszą liczbę naturalną podzielną przez 111, której suma cyfr jest równa 111.

	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