Matematyka dla Ciekawych Świata Ćwiczenia 1

Metody szyfrowania

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

Algorytm ten można zapisać następująco:
C = (p+3) mod (26), gdzie 'C' jest zakodowaną literą a 'p' jest numerem litery do zakodowania.
Powyższy algorytm w przypadku ogólnym przyjmuje postać:
C = (p+k) mod (26), gdzie k jest z przedziału <1;25>; k jest przesunięciem.
Algorytm deszyfrujący jest prosty:
p = D(C) = (C-k) mod (26)
Uwaga. W poniższych zadaniach szyfrujemy znaki 26 literowego alfabetu przyporządkowując im liczby ze zbioru {0,1,2,…, 25}. (chyba, że z tresci zadania wynika cos innego)

1. 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.*

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

3. Funkcja szyfrująca jest w postaci wielomianowej $f(x) = ax^3 + bx^2 + cx + d$. 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 jako -4, 8.

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

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

6. **Kryptosystem Vigenera** proszę zaszyfrować i odszyfrować coś (proponuję pracę w grupach) korzystając z tabeli którą Państwo dostali. Sposób szyfrowania następujący wypisujemy tekst jawny a pod nim klucz (powtarzając tyle razy ile potrzeba) następnie wykonujemy „dodawanie” wg tabeli pierwsza litera każdej pary brana jest z pierwszej kolumny i dodawana do litery drugiej wybranej w pierwszym wierszu. Na przecięciu wiersza i kolumny zaszyfrowany tekst.

7. Wersja druga **Kryptosystemu Vigenera** wykorzystywany jest autoklucz tylko pierwsza litera klucza jest tajna a pozostałe to litery tekstu jawnego.

8. 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

   Odp. a) cezar k=3 w zdaniu tym jest podany klucz MUCHA do zdania drugiego

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

10. Funkcja szyfrująca zdefiniowana jest następująco: e(x) = reszta z dzielenia 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?

Uwaga. Szyfrować można dowolny tekst. Chciałabym aby uczniowie sami doszli do wniosku, że a musi być względnie pierwsze z 26 aby istniała funkcja odwrotna. Podobnie gdy e(x) =ax+k.

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

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

12. Niech A, B będą cyframi takimi, ze A + B < 10. Znaleźć cyfry $X_1,....X_n$ takie że $\frac{AX_1...X_nB}{BX_1...X_nB} = \frac{AB}{BA}$.

13. 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.

WSK. Każdemu ciągowi liczb (w_1, …w_{100}) przyporządkowujemy sumę modulo 100 i takie ciągi dzielimy na klasy w zależności od tej sumy. Ciąg liczb wypisanych na czołach więźniów należy do jednej z tych klas. Numerujemy wszystkich więźniów liczbami od 0 do 99. Strategia więźniów mogłaby być następująca. Więzień o numerze k mówi liczbę x_i taką, że suma tej liczby oraz wszystkich innych, które widzi na czołach współwięźniów jest równa k (mod 100).

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

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

16. 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 $2\sqrt{10}$.