Ćwiczenia: klasyczne metody szyfrowania

Projekt „Matematyka dla ciekawych świata”
spisała: Barbara Roszkowska–Lech, Maria Gokieli

14 kwietnia 2016

Zadania bez punktacji sa przeznaczone do pracy w grupach.

1. Przechwyciłeś zaszyfrowaną wiadomość: ABACDGB—AHBIJKLŁTD. Udało się podejrzeć drugie słowo jeszcze nie zaszyfrowanej wiadomości :—SZYFRUJĄCE. Odczytaj wiadomość.

2. KYPAGL to zaszyfrowane szyfrem Cezara imię. Nie znamy jednak klucza, który został użyty. Pracując w grupach, spróbujcie odszyfrować tę wiadomość. Ile czasu Wam to zajęło? Jak doszliście do rozwiązania?

3. Kryptosystem Vigenera. W grupach zaszyfrujcie i odszyfrujcie wybraną wiadomość, korzystając z tabeli z szyfrem Vigenera. Sposób szyfrowania jest 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.

4. To samo w drugiej wersji druga Kryptosystemu Vigenera: wykorzystywany jest autoklucz: tylko pierwsza litera klucza jest tajna, a pozostałe to litery tekstu jawnego.

5. (1p) Funkcja szyfrująca e(x) = reszta z dzielenia x^3 przez 15.

   a) Zaszyfruj wiadomość 2, 4, 3.

   b) Zaszyfruj wiadomość 5, 15, 30.

   c) Zaszyfruj wiadomość 16, 301, 45001.

   d) Zaszyfruj wiadomość 12, 40, 35.

   e) Czy możesz odszyfrować wiadomość: 5, 0?

6. (1p) 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

   Uwaga — rozwiązanie pierwszego punktu da Ci klucz do drugiego.

7. (1p) Funkcja szyfrująca jest postaci: $e(x)$ = reszta z dzielenia x przez pewną liczbę naturalną n. $e(47) = 11$, $e(36) = 0$. Zakoduj liczbę 11.

8. (2p) Odczytaj kryptogramy. Ile rozwiązań ma każdy z nich? (Różnym literom odpowiadają różne cyfry).

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

9. (3p) Ile (mniej więcej) jest możliwych kluczy w kryptosystemach Cezara, Playfaira i Viegenera? (Dwa ostatnie zależą od długości klucza).

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