WSTĘP DO TEORII LICZB – ZADANIA

Zestaw nr.11: Wstęp do kryptografii

część pierwsza – SZYFROGRAMY, KRYPTOGRAMY – do odgadnięcia
wskazówka: operujemy alfabetem 26-literowym:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Zad.1 Rozszyfruj kryptogram:

WHRULD OLFCE MHVW IDMQD L OXELH VLH MHM XFCBF ER GDMH GXCR SUCBMHPQRVFL

Zad.2 Rozszyfruj kryptogram :

wrfgrfoneqmbznqel

Zad.3 „Kod kreskowy" – zadanie doświadczalne

Poniżej jest zaszyfrowana pewna liczba w postaci kodu kreskowego:

0 – 0 – 1 – 0 - 1 – 0 – 1 – 0 – 1 – 1 – 0 – 0 – 1 – 0
0 – 0 – 0 – 0 - 0 – 1 – 0 – 0 – 0 – 0 – 1 – 1 – 0

Zad.4 Odgadnij (trudne!!) szyfrogram: **E C O I V N**.

wskazówka: operujemy alfabetem 26-literowym:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

część druga

Zad.1 (Koblitz) Przechwyciłeś wiadomość „SONAFQCHMWPTVEVY". Podejrzewasz, że jest to tekst powstały z zaszyfrowania wektorów-digramów, 2-literowych kombinacji 26-literowego alfabetu (A–Z), którego poszczególnym literom odpowiadają liczby (0–25). Analiza częstości (przeprowadzona na znacznie dłuższym kryptogramie o tej samej budowie) wykazała, że najczęstsze diagramy występujące w tekście zaszyfrowanym $\mathcal{C}$ to „KH" i „XW", które zapewne odpowiadają digramom „TH" i „HE" tekstu otwartego $\mathcal{P}$. Znajdź macierz rozszyfrującą $\mathcal{A}^{-1}$ i odczytaj wiadomość.

Zad.2 (Koblitz) Przechwyciłeś wiadomość „!IWGVIEX!ZRADRYD". Podejrzewasz, że jest to tekst powstały z zaszyfrowania wektorów-digramów, 2-literowych kombinacji 26-literowego alfabetu (A–Z), którego poszczególnym literom odpowiadają liczby (0–25), odstęp = 26, ? = 27 i ! = 28. Ostatnie pięć liter kryptogramu to „MARIA".

(1) Znajdź macierz rozszyfrującą $\mathcal{A}^{-1}$ i odczytaj wiadomość.

(2) Znajdź macierz szyfrującą $\mathcal{A}$ i nadaj do Marii wiadomość (jako przyjaciel Marii, Jo):

„DAMN FOG! JO"

Zad.3 (indywidualna praca domowa).

Ułóż sam tekst – najlepiej po angielsku (albo po polsku, ale bez diakrytyków) – minimum 16 znaków – i zaszyfruj go według schematu opisanego w zadaniu 2, wybierając sobie macierz szyfrującą $\mathcal{A}$ tak aby jej wyznacznik był względnie pierwszy z modułem 29.

Znajdź też macierz odwrotną $\mathcal{A}^{-1}$ i sprawdź, że Twoje szyfrowanie było poprawne.

Zad.4 (indywidualna praca domowa).

Szyfry wykładnicze – przykład (Song Yan) ostatni punkt z wykładu .

Ułóż sam tekst (najlepiej po angielsku) (minimum 20 znaków) i zaszyfruj go według schematu opisanego na wykładzie, wybierając jako moduł liczbę pierwszą rzędu tysiąca.
Skorzystaj np. z tych tabel .

Wykładnik potęgowy e wybierz jako liczbę na poziomie dziesięciu (lub kilku dziesiątek), względnie pierwszą z $p-1$. Przeprowadź szyfrowanie, następnie znajdź odwrotność multyplikatywną wykładnika, liczbę d; $e \cdot d \equiv 1 \pmod{[p-1]}$ i sprawdź czy Twoje zaszyfrowanie było poprawne. Takie zadanie można wykonywać w zespołach 2-osobowych.

Zad.5 Rozważmy liczbę $N = 51\,809$, która jest iloczynem dwóch liczb pierwszych p i q. Wiemy, że $\sigma(N) = 52\,416$. Znajdź p i q.

Zad.6 Pewien Bank szyfruje 3-cyfrowy numer PIN-u, używając do tego klucza RSA, z $e = 835$ i $N = pq = 1\,411 = 17 * 83$. Podaj PIN Alicji wiedząc, że jest on zaszyfrowany jako 002.