”Mathematics consists of proving the most obvious thing in the least obvious way.”
– George Pólya

Multigrafy a szyfry

WMS AGH

VOL.I. . . No.1 *14 KWIETNIA 2023*

To tylko parę kropek i kresek

By JULIANA PALMEN

ILUSTRACJA – GABRIELA MAKAR

Profesor Brown upił kolejny łyk zimnej już od paru minut kawy. Przewrócił stronę w gazecie, by sprawiać wrażenie, że jest pochłonięty lekturą. Przy stoliku obok trwała prowadzona szeptem dyskusja.

– To zbyt ryzykowne . . . lepiej przeprowadzić operację w innym miejscu.

– Pamiętaj, że w centrum będą tłumy – odezwał się drugi głos.

– Ma rację. Jak przewieziesz X w środku dnia, nie wzbudzając zainteresowania gapiów?

– Panowie, spokojnie. Zapomnieliście, że ja tu jestem od myślenia.

Na moment zapadła cisza. Pan Brown dyskretnie wyjął notatnik i ołówek.

– Zastosujemy stary jak świat numer z . . . – tutaj padł odpowiedni kryptonim.

Siedzący przy stole pokiwali głowami. Profesor stwierdził, że nie ma chwili do stracenia i zaczął przygotowywać wiadomość z zamiarem nadania jej, gdy tylko opuści kawiarenkę. Wiedział jednak, że od jakiegoś czasu jest obserwowany przez jednego ze spiskowców. Kilka ruchów ołówka później złożył gazetę i z notatnikiem w dłoni ruszył w kierunku wyjścia.

– Chwileczkę, profesorze Brown – przywołał go jeden z mężczyzn, jak się okazało, asystent laboratoryjny – czy mógłbym pożyczyć od pana gazetę?

– Jak najbardziej – Brown z niemałą obawą podszedł do stolika.

– I notatnik – rzucił podejrzliwy spiskowiec.

– Daj spokój Morgan, profesor Brown pracuje pewnie nad kolejnym wykładem dla studentów.

Brown wziął głębszy oddech i starał się brzmieć przekonująco, gdy kładł notatnik na stole:

– To tylko parę kropek i kresek . . .

Wstęp teoretyczny

Zanim przedstawimy taktykę, jaką zastosował profesor Brown do zakodowania wiadomości, konieczne będzie wprowadzenie kilku definicji. Ponizej podajemy potrzebne pojęcia z teorii grafów i kryptografii. Czytelnik już z nimi obeznany może pominąć ten fragment.

Multigraf:
Multigrafem nazywamy trójkę $G = (V, E, \varphi)$, gdzie $G = (V, E)$ jest grafem, a $\varphi : E \to \mathbb{N}$ jest funkcją określającą krotność krawędzi. W multigrafie mogą więc wystąpić krawędzie wielokrotne, łączące dwa ustalone wierzchołki.

Macierz sąsiedztwa multigrafu:
Jest to macierz kwadratowa o stopniu równym liczbie wierzchołków multigrafu. Każdy wierzchołek jest indeksowany jedną z kolejnych liczb od 1 do n. Element a_{ij} macierzy jest równy liczbie krawędzi pomiędzy wierzchołkami i oraz j. W artykule skupimy się na multigrafach nieskierowanych i bez pętli – zatem w tym przypadku macierz sąsiedztwa będzie symetryczna, z zerami na głównej przekątnej.

Ścieżka Hamiltona:
Ścieżką Hamiltona w grafie G nazywamy ścieżkę przechodzącą przez wszystkie wierzchołki grafu dokładnie raz.

Operacja XOR:
W kryptografii XOR-owaniem określa się dodawanie do siebie dwóch ciągów binarnych (bit po bicie) według następującej zasady: $0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 1 = 0$. Dla przykładu:
$1001010 \oplus 10111 = 1001010 \oplus 0010111 = 10111101$.

Kody ASCII:
American Standard Code for Information Interchange (ASCII) to przyporządkowanie każdemu znaku pewnego kodu liczbowego. I tak na przykład literze A odpowiada liczba 65.

Szyfrowanie wiadomości

Wyposażeni w odpowiednie narzędzia, to jest: notes, ołówek i tablica kodów ASCII (którą profesor Brown jest w stanie wyrecytować o każdej porze dnia i nocy) możemy przystąpić do działania.

1. Na początku zapisz wiadomość, używając wielkich liter. Każdą literę będziemy kodować osobno.

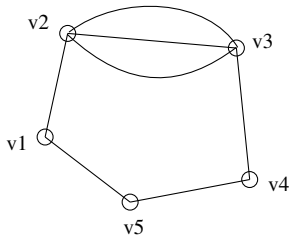
2. Odczytaj wartość danej litery w kodzie ASCII, a następnie zapisz ją w systemie binarnym.
   Dla przykładu: $G = 71 = 1000111$.

3. Następnie wykonaj działanie XOR-owania z binarnym odpowiednikiem 32, czyli:
   $G \oplus 32 = 1000111 \oplus 0100000 = 1100111$.
4. Oznacz przez k liczbę jedynek w tak otrzymanym ciągu.
5. Przygotuj macierz stopnia k, z zerami na głównej przekątnej. Jak już zapowiadaliśmy, będzie to macierz symetryczna, tak więc $a_{ij} = a_{ji}$.
6. Dla pierwszych $k - 1$ jedynek w zakodowanej literze:
   - policz liczbę zer stojących bezpośrednio po jedynce, a następnie dodaj 1 do tej liczby,
   - wpisz otrzymaną liczbę nad pierwszym zerem, nad którym nie została wpisana dotychczas żadna liczba (czyli dla i-tej jedynki wpisz wartość w komórce o indeksie $[i, i + 1]$).
7. Jeśli za k-tą jedynką stoi L zer, to $a_{1k} = L + 1$. Dany wzór stosujemy również w przypadku, gdy za ostatnią jedynką nie ma zer ($L = 0$).
8. Uzupełnij macierz, wypełniając pozostałe komórki zerami.

Poniżej przedstawiamy macierze, odpowiadające literom G, A oraz P.

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \quad A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 5 \\ 1 & 5 & 0 \end{bmatrix} \quad P = \begin{bmatrix} 0 & 1 & 5 \\ 1 & 0 & 1 \\ 5 & 1 & 0 \end{bmatrix}$$

Profesor Brown nie rysował jednak tablic, tylko "kropki i kreski". W ostatnim kroku należy z każdej macierzy odtworzyć multigraf, traktując daną tablicę jako macierz sąsiedztwa. Poniżej prezentujemy literę G.



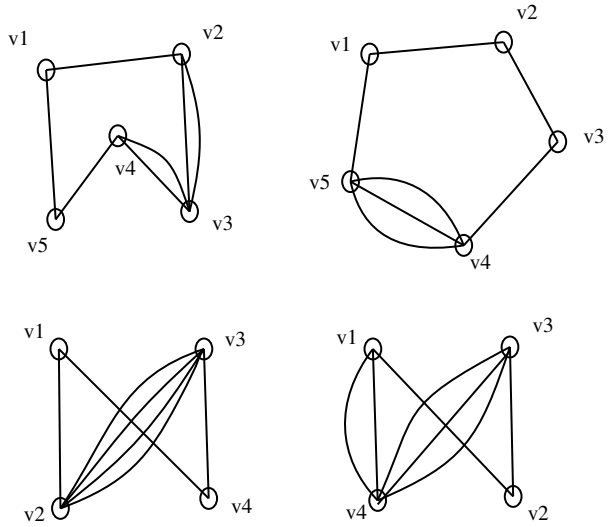
Deszyfrowanie wiadomości

Aby odczytać zaszyfrowaną wiadomość należy przejść przez proces kodowania w odwrotnej kolejności. Przypuśćmy, że otrzymaliśmy multigraf G, w którym ponumerowano wierzchołki. Budujemy macierz sąsiedztwa, a następnie odtwarzamy ciąg binarny (zakładamy przy tym, że znamy sposób szyfrowania wiadomości). Otrzymany ciąg XOR-ujemy z binarnym odpowiednikiem 32. Wynik zapisujemy w systemie dziesiętnym, by w kolejnym kroku, korzystając z tablicy ASCII (lub niezwykłej pamięci profesora), odczytać literę.

Zauważmy, że gdybyśmy w tym samym multigrafie ponumerowali wierzchołki inaczej (co odpowiadałoby skonstruowaniu innej ścieżki Hamiltona), otrzymalibyśmy inną macierz incydencji, a co za tym idzie, odmienną literę (problem ten obrazują na przykład grafy dla liter A i P). Ścieżka Hamiltona stanowi więc klucz w procesie deszyfrowania. Profesor Brown wraz z odbiorcą wiadomości uzgodnili wcześniej sposób numerowania wierzchołków. Gdyby wiadomość dostała się w niepowołane ręce, nie mogłaby zostać rozszyfrowana bez znajomości poprawnego numerowania.

Zadanie – Kryptonim operacji

Nieustraszony naukowiec niezwłocznie wysłał zaszyfrowaną wiadomość do zaufanego pracownika służb specjalnych, kapitana Hastingsa. Ten ponumerował wierzchołki według ustalonego systemu. Jaki jest kryptonim operacji?



Rozwiązanie zagadki wraz z imieniem, nazwiskiem i nazwą wydziału prosimy przesyłać na adres mailowy koła: knmd@agh.edu.pl

Ciekawostki

- Jedną z nowszych metod szyfrowania jest kryptografia kwantowa, która wykorzystuje losowo zmieniane fotony jako nośniki informacji. Za prekursora tej dziedziny z pogranicza fizyki, informatyki i matematyki uważa się prof. Artura Ekerta.
- W IX wieku arabski filozof Al–Kindi napisał traktat "O odczytywaniu zaszyfrowanych listów", w którym zaproponował metodę przełamania szyfru podstawieniowego przy użyciu analizy częstości.
- Rozwój kryptografii i kryptoanalizy niejako zapoczątkował erę komputerów oraz informatyki.
- W Polsce 25 stycznia obchodzony jest Dzień Kryptologii, natomiast 21 października przypada Global Encryption Day.