13 lutego 2024

Zadania z kryptografii, lista nr 1

1. W czterech plikach załączonych do listy znajdują się teksty angielskie i jeden francuski zaszyfrowane odpowiednio szyfrem podstawieniowym, szyfrem Viegenere'a, szyfrem afinicznym i nieustalonym szyfrem. W każdym przypadku ustal teksty jawne.

2. Jak liczna jest przestrzeń kluczy dla szyfru Hilla jeśli szyfrujemy tekst zapisany w 26-literowym alfabecie i podzielony na bloki długości 2? A jak jest dla bloków długości m?

3. Ile jest takich kluczy kodujących w szyfrze Hilla z poprzedniego zadania ($m = 2$), które są zarazem kluczami dekodującymi?

4. Wyznacz macierz szyfrowania, jeśli wiadomo że tekst
   BREATHTAKING
   po zaszyfrowaniu szyfrem Hilla (z nieznaną wartością m) otrzymano kryptogram
   RUPOTENTOIFV

5. Rozważamy wszystkie układy liczb dodatnich $p_A, \ldots, p_Z$ takie, że $p_A + p_B + \cdots + p_Z = 1$. Dla jakiego układu liczb wartość sumy $\sum_l p_l^2$ jest najmniejsza i ile ona wynosi?

6. Rozważamy wszystkie układy liczb dodatnich $p_A, \ldots, p_Z$ takie, że $p_A + p_B + \cdots + p_Z = 1$. Dla jakiego układu liczb wartość entropii $-\sum_l p_l \log_2 p_l$ jest największa? W jaki sposób można posłużyć się funkcją entropii do znajdowania długości s bloku szyfru Vigenèra.

7. W algorytmie one-time pad długości tekstu jawnego i klucza są takie same. Algorytm ten ma własność *bezpieczeństwa doskonałego* to znaczy przy znanym szyfrogramie wszystkie teksty jawne są równie prawdopodobne jak gdy nie znamy szyfrogramu. Pokaż, że niemożliwe jest osiągnięcie bezpieczeństwa doskonałego, gdy długość klucza ma być mniejsza od długości tekstu jawnego.

8. Pokaż, że grupa cykliczna rzędu d ma $\varphi(d)$ generatorów. Ile jest w niej elementów rzędu e dla $e|d$? Wylicz wartość sumy
   $$\sum_{e:e|d} \varphi(e).$$

9. Pokaż, że jeśli p jest liczbą pierwszą i $x^2 \equiv 1 \bmod p$, to $x \equiv -1, 1 \bmod p$.

10. Niech p będzie liczbą pierwszą, a α ustaloną liczbą naturalną. Ile jest takich reszt x modulo p^α, że $x^2 \equiv 1 \bmod p^\alpha$. Osobno rozważ przypadek $p = 2$

11. Niech $n = p_1^{k_1} \cdots p_s^{k_s}$. Ile jest takich $x \in \mathbb{Z}_n$, że $x^2 \equiv 1 \bmod n$?

12. Pokaż, że jeśli w grupie przemiennej G istnieją elementy g, h rzędów odpowiednio a i b, gdzie $a \perp b$, to w G istnieje element rzędu ab.

13. Niech a będzie różnym od 1 elementem grupy takim, że $a^q = 1$ dla pewnej liczby pierwszej q. Jaki jest rząd elementu a?

14. Sformułuj jak najprostszy sposób mnożenia liczb modulo $2^{16} + 1$ (0 interpretujemy jako 2^{16}), jeśli dysponujesz procesorem wykonującym dodawania liczb 16-bitowych 2^{16} (z wyniem 17-bitowym) i mnożenie liczb 16-bitowych (z wynikiem 32-bitowym).