Lista zadań. Nr 2. 1 marca 2005

Kryptografia

IIUW.

1. (?pkt)[1] W czterech plikach załączonych do listy znajdują się teksty zaszyfrowane odpowiednio szyfrem podstwieniowym, szyfrem Vigenere'a, szyfrem afinicznym i nieustalonym szyfrem. W każdym przypadku ustal teksty jawne.
2. (1pkt) Szyfr Hilla jest szyfrem blokowym, w którym bloki przekształacane są przekształceniem liniowym. Jak liczna jest przestrzeń kluczy dla tego systemu, w którym kodujemy bloki (oczywiście tekstu angielskiego) o długości $m = 2$?
3. (1pkt) Czy może się zdarzyć, by klucz kodujący w szyfrze Hilla był jednocześnie kluczem dekodującym? Jeśli tak, to ile jest takich kluczy dla kodowania bloków długości $M = 2$? Jeśli nie, wyjaśnij przyczynę.
4. (1pkt) Wyznacz macierz szyfrowania, jeśli wiadomo, że tekst jawny

   BREATHTAKING

   po zaszyfrowaniu szyfrem Hilla (z nieznaną wartością m) otrzymano kryptogram

   RUPOTENTOSUP
5. (2pkt) Udowodnij, że procedura deszyfrowania w algorytmie RSA jest poprawna.

[1] Zadania 1-4 pochodzą z książki Stinsona