Kodowanie i bezpieczeństwo informacji

Lista nr 6 - od 22 kwietnia 2012

Zadanie 1 Napisz macierze generujące i macierze parzystości dla kodów Hamminga długości odpowiednio 3, 7 i 15.

Zadanie 2 Dla kodowania ze słowami długości k jaka jest minimalna długość kodów z korekcją jednego błędu (oparta na kodach Hamminga) dla tego kodowania. Jak stworzyć takie kody?

Zadanie 3 Pokaż, że odległość Hamminga jest metryką dla ciągów binarnych.

Zadanie 4 (2 pkt) Oszacuj prawdopodobieństwo (zależne od długości klucza) wyparcia się przez Alicję autorstwa dokumentu podpisanego za pomocą podpisu niezaprzeczalnego. Rozpatrz przypadek, gdy Alicja dokument podpisała jak i sytuację, w której nie jest autorką podpisu.

Zadanie 5 Przedstaw schemat ślepych podpisów opartych na RSA. Wytłumacz w jaki sposób można je wykorzystać do stworzenia systemu płatności elektronicznych i wyborów elektronicznych. Jakie są słabe strony ślepych podpisów?