Lista zadań. Nr 1. 21 lutego 2005

Kryptografia

IIUW.

1. (1pkt) (Bezpieczeństwo doskonałe systemu one-time pad) Rozważ metodę one-time pad. Udowodnij, że po przechwyceniu kryptogramu, wiedza Ewy o rozkładzie prawdopodobieństwa w przestrzeni tekstów jawnych nie ulega zmianie.

2. (1pkt) Udowodnij, że jeśli przestrzeń kluczy jest mniejsza od przestrzeni tekstów jawnych, to powyższe twierdzenie nie jest prawdziwe.

3. (1pkt) Ewa wie, że Bob używa systemu one-time pad nie zmieniając klucza. Jakich informacji dowie się Ewa po przechwyceniu trzech różnych kryptogramów wysłanych przez Boba?

4. (1pkt) Niech przestrzeń tekstów jawnych $M = \{1, 2, 3, 4\}$ oraz przestrzeń kluczy $C = \{1, 2, 3, 4\}$. Niech funkcja szyfrująca $E_k(m) = km \bmod 5$.
   - Jaka jest funkcja deszyfrująca?
   - Czy ten kryptosystem posiada cechę bezpieczeństwa doskonałego?

5. Alicja umówiła się ze swoim maklerem Bobem, że polecenia kupna bądź sprzedaży akcji będzie przesyłać zasyfrowane systemem one-time pad używającym 96-bitowych kluczy. W tym celu wygenerowała losowo i przekazała Bobowi odpowiedni zapas takich kluczy. Każde zlecenie Alicja zapisuje jako 11 znakowy tekst w kodzie ASCII (a więc 96-bitowy) o następującej składni:
   - Pierwszy znak jest równy 'S' (sprzedaj) albo 'K' (kup).
   - Drugi znak jest spacją.
   - Pięć kolejnych znaków tworzy liczbę (oznaczającą liczbę akcji). W razie potrzeby liczba ta poprzedzona jest nieznaczącymi zerami.
   - Kolejny znak to spacja.
   - Końcowe znaki to co najwyżej trzyliterowy skrót nazwy spółki giełdowej, zapisany dużymi literami.

   Chcąc wysłać i-te zlecenie, Alicja używa kolejnego klucza z ustalonej puli. Przeanalizuj bezpieczeństwo takiego systemu.