Ćwiczenia z Sieci komputerowych
Lista 2

1. W kablu koncentrycznym używanym w standardowym 10-Mbitowym Ethernecie sygnał rozchodzi się z prędkością 10^8 m/s. Standard ustala, że maksymalna odległość między dwoma komputerami może wynosić co najwyżej 2,5 km. Oblicz, jaka jest minimalna długość ramki (wraz z nagłówkami).[1]

2. Rozważmy rundowy protokół Aloha we współdzielonym kanale, tj. w każdej rundzie każdy z n uczestników usiłuje wysłać ramkę z prawdopodobieństwem p. Jakie jest prawdopodobieństwo $P(p, n)$, że jednej stacji uda się nadać (tj. że nie wystąpi kolizja)? Pokaż, że $P(p, n)$ jest maksymalizowane dla $p = 1/n$. Ile wynosi $\lim_{n\to\infty} P(1/n, n)$?

3. Jaka suma kontrolna CRC zostanie dołączona do wiadomości `1010` przy założeniu że CRC używa wielomianu $x^2 + x + 1$? A jaka jeśli używa wielomianu $x^7 + 1$?

4. Pokaż, że CRC-1, czyli 1-bitowa suma obliczana na podstawie wielomianu $G(x) = x+1$, działa identycznie jak bit parzystości.

5. Pokaż, że kodowanie Hamming(7,4) umożliwia skorygowanie jednego przekłamanego bitu. Wskazówka: wystarczy pokazać, że odległość Hamminga między dwoma kodami wynosi co najmniej 3.

6. Załóżmy, że wyliczamy sumę CRC dla 4-bitowej wiadomości używając wielomianu $G(x) = x^3 + x + 1$; wtedy wiadomość wraz z sumą ma długość 7 bitów. Załóżmy, że co najwyżej jeden z tych 7 bitów został przekłamany. Pokaż, jak odbiorca takiego komunikatu może wykryć i skorygować takie przekłamanie.

7. Rozszerz podany w notatkach dowód poprawności algorytmu RSA na dowolne $m \in [0, n)$. Wskazówka: skorzystaj z Chińskiego twierdzenia o resztach.

8. Niech $n = p \cdot q$, gdzie p i q są liczbami pierwszymi. Pokaż, że znajomość $\phi(n)$ wystarcza, żeby podzielić n na czynniki pierwsze w wielomianowym czasie.[2]

9. Załóżmy, że co trzeci list to spam. Słowo `enlarge` występuje w 80% maili, które są spamem i w 5% maili, które spamem nie są. Dostajemy mail, w którym występuje słowo `enlarge`. Jakie jest prawdopodobieństwo[3], że jest to spam?

10. Dana jest deterministyczna funkcja skrótu h zwracająca na podstawie tekstu liczbę m-bitową. Losujemy $2^{m/2}$ tekstów i obliczamy na nich funkcję h. Zakładamy tutaj, że przy takim losowaniu tekstu x, $h(x)$ jest losową (wybraną z rozkładem jednostajnym) liczbą m-bitową. Pokaż, że prawdopodobieństwo, że wsród wylosowanych tekstów istnieją dwa o takiej samej wartości funkcji h jest $\Omega(1)$.

Lista i materiały znajdują się pod adresem `http://www.ii.uni.wroc.pl/~mbi/dyd/`

Marcin Bieńkowski

---

[1] W rzeczywistości sygnał rozchodzi się ok. 2 razy szybciej, ale opóźnienia występują nie tylko w kablu.

[2] To jest krok na drodze do udowodnienia, że odzyskanie klucza prywatnego (d, n) na podstawie klucza publicznego (e, n) jest co najmniej tak trudne jak podział n na czynniki pierwsze. Jeśli mamy d i e, możemy obliczyć $d \cdot e - 1$, czyli nie samo $\phi(n)$, ale jego wielokrotność.

[3] Zakładamy, że mail losowany jest jednostajnie z puli wszystkich maili.