Kolokwium: Kryptografia i bezpieczeństwo, 2.12.03
WPPT, informatyka inż., M.Kutyłowski

Nazwisko i imię: .....
numer indeksu: .....
pseudonim: .....

Odpowiedz zwięźle na arkuszu z pytaniami. Odpowiedź powinna dotyczyć jądra zagadnienia. W każdym zadaniu można zdobyć 3 punkty. Czas rozwiązywania zadań - 90 minut

1. Tygrysek, Prosiaczek i Kłapouchy mają wybrać losowo ze swego grona kogoś, kto odgarnie śnieg. Porozumiewają się przy pomocy telefonów. (Połączenie mogą uzyskać każdorazowo tylko dwie osoby.) Jak zrobić, by prawdopodobieństwo wybrania było równe $\frac{1}{3}$ dla każdego z nich? Nikt nie powinien mieć możliwości takiego wykonania protokołu, aby zmniejszyć swe prawdopodobieństwo wybrania do odśnieżania.

2. Czy może się zdarzyć, że mając parę (tekst jawny, kryptogram) można wykluczyć, że kryptogram powstał z podanego klucza jawnego? Rozważ to pytanie dla DES-a i dla one-time pad. Uzasadnij odpowiedź.

3. Alicja zaszyfrowała tekst M strumieniowo używając w tym celu generatora LFSR. W trakcie obliczeń w pewnej chwili nieprawidłowo został wyznaczony wynik operacji XOR. Następnie Bob odszyfrował otrzymany od Alicji kryptogram. Jaki fragment tekstu jawnego otrzyma Bob w prawidowej postaci? Opisz, które fragmenty zostaną zmienione.

4. Prosiaczek nie może zapamiętać długiego klucza dla 3-DESa. Wpadł więc na pomysł, że klucz ten będzie otrzymywał z 64-bitowego klucza K biorąc odpowiednią liczbę początkowych bitów z wyniku SHA-1(K). Klucz K jest krótszy i Prosiaczek potrafi go zapamiętać. Prosiaczek jest niepewny czy robi dobrze. Odpowiedz mu!

5. Tygrysek zaimplementował schemat podpisów ElGamala: Parametr k wybierany jest tak by się nie powtórzył – zawsze jest to stan zegara systemowego. (Tygrysek zapamiętał z wykładu, że nie wolno stosować tego samego k daw razy) Czy jest to bezpieczny sposób? Uzasadnij wskazując atak bądź jakiś dowód bezpieczeństwa.