1.10.02

KRYPTOGRAFIA, 2002

Lista nr 1

1. Mamy znaleźć klucz pasujący do określonej pary kryptogram - tekst jawny. Zakładamy, że istnieje dokładnie jeden taki klucz, oraz że długość klucza wynosi k bitów. Zakładając, że w czasie 1 sekundy nasz komputer może przetestować 1 milion kluczy (poprzez zaszyfrowanie tekstu jawnego hipotetycznym kluczem i porównanie otrzymanego kryptogramu z podanym nam), ile powinno to zająć czasu? Odpowiedz na to pytanie dla $k = 40$, $k = 56$, $k = 90$, $k = 128$. W razie potrzeby (gdy czas jest bardzo długi) założyć należy, że wszytkie komputery na świecie (a jest ich nie więcej niż ludzi) uczestniczą w naszym przedsięwzięciu.

2. Algorytm one-time pad ma tę własność, że dlugości klucza i tekstu jawnego są takie same. Pokazać, że niemożliwe jest osiągnięcie *bezpieczeństwa doskonałego*, gdy długość klucza jest mniejsza od długości tekstu jawnego. (Bezpieczeństwo doskonałe oznacza, że dla każdego kryptogramu każdy tekst jawny jest równie prawdopodobny).

3. Gdy podpisujemy się w banku, niekiedy dla rozwiania wątpliwości musimy podpisać się ponownie. Wskaż na procedurę pozwalającą podpisać elektronicznie po raz drugi ten sam dokument. Mamy wykorzystywać technikę podpisywania poznaną na wykładzie, tj. używać asymetrycznego algorytmu szyfrującego RSA (oczywiście trzeba coś dorobić).

4. Schematem podpisów Lamporta nazywamy następującą procedurę:
   Wybieramy losowo $y_{i,0}, y_{i,1}$ z pewnego zbioru Y dla $i \leq m$. Obliczamy $z_{i,j} = f(y_{i,j})$ dla $i \leq m, j = 0, 1$, gdzie f jest ustaloną funkcją hashującą. Liczby $z_{i,j}$ ujawniamy, zaś liczby $y_{i,j}$ pozostają sekretem autora podpisów.
   Podpis ciągu bitów $x_1, \ldots, x_m$ tworzony jest jako $y_{1,x_1}, \ldots, y_{m,x_m}$.

   Przedyskutuj bezpieczeństwo i możliwości praktycznych zastosowań schematu Lamporta.

5. Zakładamy, że mamy do dyspozycji dobry algorytm szyfrujący (symetryczny). Jak w tej sytuacji skonstruować funkcję hashującą?

6. Protokół zobowiązania bitowego wykonywany przez Alicję i Boba polega na tym, że

   - w kroku 1 Alicja wybiera losowo bit b, koduje go jako m i przekazuje Bobowi
   - Bob nie jest w stanie odczytać z m czy Alicja wybrała zero czy 1
   - w odpowiedniej chwili Alicja *odkrywa* b poprzez odpowiednie oblicznia na m

   Ważne jest by Alicja nie mogła oszukać izmienić wartości b po przekazaniu m Bobowi.

   Jak zrealizować zobowiązanie bitowe mając
   (a) algorytmy szyfrowania asymetrycznego, (b) jednostronne funkcje hashujące?

7. Wykorzystaj protokół zobowiązania bitowego do skonstruowania protokołu, przy pomocy którego dwie osoby rozmawiające przez telefon mogłyby „rzucić monetą“, tj. wylosować bit tak, aby żadna z osób nie mogła ustalić wyniku.

/-/ Mirosław Kutyłowski