1.10.02

KRYPTOGRAFIA I BEZP. KOMP.,
WPPT, INF. INŻ. 2002

Lista zadań 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 $k = 40$, $k = 56$, $k = 90$, $k = 128$.

2. Algorytm one-time pad dla długich tekstów jawnych i klucza długości $k_0 k_1 \ldots k_{n-1}$ można zastosować w ten sposób, że dla zaszyfrowania i-tego bitu stosujemy wzór:

$$c_i = t_i \text{ XOR } k_{i \bmod n}$$

Jakie informacje można wyciagnąć z takiego kryptogramu?

3. Jak przy pomocy algorytmów asymetrycznych zapewnić jednocześnie poufność listu i udokumentować jego pochodzenie?

4. 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). Wskazówka: można dołączać do dokumentu wartości funkcji hashującej ...

/-/ Mirosław Kutyłowski