Lista zadań. Nr 3. 6 marca 2005

Kryptografia

IIUW.

1. (1pkt) Działanie LFSR opisywane jest rekurencją liniową postaci $k_{m+1} = \sum_{i=1}^{m} c_i k_i$ (m jest stopniem rekurencji).
   - Wykaż, że:
     - maksymalny okres takiego LFSR jest nie większy niż $2^m - 1$;
     - nie więcej niż połowa rekurencji stopnia m daje LFSR o okresie $2^m - 1$.
   - Wypisz wszystkie rekurencje stopnia 4, które definiują LFSR o okresie 15.
2. (2 pkt) Przedstaw w jaki sposób można przeprowadzić kryptoanalizę szyfru strumieniowego opartego na LFSR mając do dyspozycji tekst jawny długości $2m - 1$, gdzie m jest stopniem rekurencji opisującej działanie LFSR.
3. (1pkt) Wykaż, że do deszyfowania w systemie DES można użyć algorytmu szyfrującego DES.
4. (1pkt) Wykaż, że DES(x, K)=DES(x', K'), gdzie DES(x, K) oznacza wynik szyfrowania x-a kluczem K a ($y' = 1^{|y|} \oplus y$).
5. (1pkt) W załączonym do listy pliku narysowane są schematy popularnych trybów szyfrowania. Narysuj schematy odpowiadających im trybów deszyfrowania.
6. (1pkt) Zaletą szyfrowania w trybie ECB jest to, że przekłamanie jednego bloku w trakcie transmisji nie wpływa na mołiwość odkodowania przez Boba pozostałych bloków. Zastanów się, jak to jest w przypadku innych trybów.