Kodowanie i bezpieczeństwo informacji

Lista nr 4 do 29 III 2013

Zadanie 1 Jedna ze słabości RC4 wynika z faktu, że prawdopodobieństwo, że drugi bajt będzie równy 0 wynosi $P[\texttt{2gi bajt} = 0] = \frac{2}{256}$. Skonstruuj test statystyczny, który wykorzystuje tę słabość do rozróżnienia RC4 od ciągu losowego.

Zadanie 2 Oszacuj jakiej wielkości klucze jesteśmy w stanie łamać metodą *brute force*, jeśli w ciągu jednej sekundy potrafimy zaszyfrować 1 miliard tekstów jawnych. Ile potrzebujemy czasu aby złamać: CSS, A5/1, DES, 3DES a ile aby złamać AES-128/192/256? Ile czasu jest potrzebne do przeglądnięcia połowy możliwych kluczy?

Zadanie 3 Dany jest układ LFSR zdefiniowany przez $z_{i+10} = z_2 + z_8 + z_9 \bmod 2$. Wykorzystaj wyjście LFSR do zaszyfrowania słowa *Kot* (wykorzystaj tablicę ASCII). Jako klucz przyjmij numer swojego indeksu (znajdź reprezentację binarną numeru indeksu, LFSR zainicjuj 9-cioma najmniej znaczącymi bitami).

Zadanie 4 Znajdź numery indeksów wszystkich osób, którym w poprzednim zadaniu wyszedł ciąg 1111111 1111111 1111111 (przyjmujemy, że *Kot* = 1001011 1101111 1110100).

Zadanie 5 *Shrinking generator* definiuje się jako układ dwóch LFSR, jeden z nich określamy jako A-sequence, drugi S-sequence. Jeżeli wyjście S jest równe 1 to wyjściem shrinking generatora jest bit na wyjściu A. Jeżeli wyjście S jest równe 0 to wyjście A jest "zapominane" (shrinking generator w tym takcie nie generuje bitu).

Dany jest shrinking generator, w którym układy A i S są takie jak w zadaniu 3. Znajdź kryptogram słowa Kot.