Sławomir Górawski

Lista 2, zadanie 5. Przy przesyłaniu szyfrogramu w DES nastąpiło przekłamanie jednego bitu. Ile bitów tekstu jawnego zostało utraconych jeśli DESa użyto w trybie ECB, CBC, CFB, OFB, k-CFB, k-OFB, CTR.

Rozwiązanie. Niech m_i będzie i-tym blokiem tekstu jawnego, a C_i – szyfrogramu. Załóżmy, że to właśnie tam nastąpiło przekłamanie. Wtedy, w zależności od trybu:

- ECB: w tym trybie $m_i = D_K(C_i)$, zatem utraciliśmy tekst jawny tylko w i-tym bloku, ponieważ żadne inne nie zależą od C_i. Utracony został co najmniej jeden bit, bo nie jest możliwe, żeby D_K dało taki sam wynik dla dwóch różnych wartości. (Tutaj: C_i przekłamanym bitem i bez). Możemy oszacować liczbę utraconych bitów na 1–64.
- CBC: tutaj $m_i = D_K(C_i) \oplus C_{i-1}$. Tracimy 1–64 bitów tekstu jawnego w i-tym bloku, jak wyżej. C_i ma również wpływ na wartość m_{i+1}, jednak jest tylko XORowane z odszyfrowanym C_{i+1}, więc w bloku $i+1$ tekstu jawnego tracimy 1 bit.
- CFB: $m_i = E_K(C_{i-1}) \oplus C_i$. Rozumując jak wyżej, tracimy 1 bitów w m_i i 1–64 bitów w m_{i+1}.
- OFB i CTR: to szyfry strumieniowe. Niech r_i – i-ty klucz wygenerowany przez generator pseudolosowy, wtedy $C_i = m_i \oplus r_i$. Zakładając, że klucz do generatora pseudolosowego jest nienaruszony, tracimy 1 bit tekstu jawnego, ponieważ $m_i = C_i \oplus r_i$, a r_i jest poprawne.
- k-CFB: m_i to C_i zXORowane z k bitami zaszyfrowanego bloku $C_{i-1}, C_{i-2}, \ldots$. W i-tym bloku tracimy 1 bit, natomiast C_i ma wpływ jeszcze na kilka kolejnych $(64/k)$. Nie wiemy, ile błędów pojawi się w k ostatnich bitach zaszyfrowanego bloku podczas kolejnych rund deszyfrowania – maksymalnie k – więc możemy oszacować z góry liczbę utraconych bitów w blokach od $i+1$ w górę jako $k \cdot 64/k = 64$.
- k-OFB: jak w OFB, $m_i = C_i \oplus r_i$, zakładamy poprawność r_i, więc tracimy 1 bit tekstu jawnego.