Sławomir Górawski

Lista 2, zadanie 3. Niech $\overline{x}$ będzie logicznym dopełnieniem ciągu x złożonego z zer i jedynek. Niech E oznacza szyfrowanie DESem. Pokaż, że jeśli $y = E_K(x)$, to $\overline{y} = E_{\overline{K}}(\overline{x})$. Jak używając tej tożsamości można zredukować dwukrotnie liczbę szyfrowań przy kryptoanalizie DESa poprzez przeszukanie przestrzeni kluczy dla danej pary tekst jawny – szyfrogram?

1. Weźmy dowolny 64-bitowy ciąg x. Pokażemy, że dla danego klucza K jeśli $y = E_K(x)$, to $\overline{y} = E_{\overline{K}}(\overline{x})$. W tym celu przyjrzyjmy się, co dzieje się z tekstem jawnym przy szyfrowaniu DESem:

1. Na początku ciąg jest permutowany i dzielony na dwie 32-bitowe części: l_0 i r_0.
2. Następnie obie części przechodzą przez 16 cykli szyfrowania – niech (l_i, r_i) będą wynikiem i-tego cyklu.
3. Po wykonaniu tych operacji l_{16} oraz r_{16} łączone są w jeden ciąg i dokonywana jest permutacja końcowa, która daje szyfrogram.

Niech L_i i R_i będą wynikami i-tego cyklu szyfrowania tekstu x kluczem K. Permutacje zachowują dopełnienie, tj. dla dowolnej permutacji bitów π zachodzi $\pi(\overline{x}) = \overline{\pi(x)}$. Wynika z tego, że aby wynikiem permutacji końcowej był ciąg $\overline{y}$, musi ona dostać na wejściu $\overline{L_{16}}$ i $\overline{R_{16}}$. Pokażemy, że przy szyfrowaniu tekstu $\overline{x}$ kluczem $\overline{K}$ wynikiem i-tego cyklu szyfrowania są $\overline{L_i}$ oraz $\overline{R_i}$, dla każdego i od 0 do 16.

Dowód. Na początku pokażemy, że $l_0 = \overline{L_0}$ i $r_0 = \overline{R_0}$. Wiemy, że permutacje bitów zachowują dopełnienie, więc jeśli wejściem do permutacji początkowej był $\overline{x}$, to jej wynikiem będzie $(\overline{L_0}, \overline{R_0})$. Teraz chcemy pokazać, że każdy cykl szyfrowania zachowuje dopełnienie. Załóżmy, że $l_i = \overline{L_i}$ oraz $r_i = \overline{R_i}$. Pokażemy, że wynikami kolejnego cyklu szyfrowania są wtedy $\overline{L_{i+1}}$ oraz $\overline{R_{i+1}}$. W DESie otrzymuje się je tak:

$$\begin{aligned} l_{i+1} &= r_i, \\ r_{i+1} &= l_i \oplus f(k_i \oplus w(r_i)), \end{aligned}$$

gdzie k_i oraz w wyjaśnimy niżej. Dla lewej strony dowód jest krótki:

$$l_{i+1} = r_i = \overline{R_i} = \overline{L_{i+1}}.$$

Klucz k_i jest tworzony przez przestawienie bitów i wybór 48 z nich. Ta operacja zachowuje dopełnienie; jeśli przy szyfrowaniu kluczem K mieliśmy $k_i = k$, to obecnie $k_i = \overline{k}$. Do rozszerzenia prawej części wejścia używamy permutacji rozszerzonej w, polega to na permutacji ze zduplikowaniem niektórych bitów; to również zachowuje dopełnienie. Razem daje to:

$$\begin{aligned} r_{i+1} &= l_i \oplus f(k_i \oplus w(r_i)) \\ &= \overline{L_i} \oplus f(\overline{k} \oplus w(\overline{R_i})) \\ &= \overline{L_i} \oplus f(\overline{k} \oplus \overline{w(R_i)}) \\ &= \overline{L_i} \oplus f(k \oplus w(R_i)) && (\overline{a} \oplus \overline{b} = a \oplus b) \\ &= \overline{L_i \oplus f(k \oplus w(R_i))} && (\overline{a} \oplus b = \overline{a \oplus b}) \\ &= \overline{R_{i+1}}. \end{aligned}$$

Nie musimy tutaj wiedzieć dokładnie, jak działa f – wystarczy nam, że wynik jest taki sam, jak przy szyfrowaniu tekstu x kluczem K. Z zasady indukcji $l_i = \overline{L_i}$ i $r_i = \overline{R_i}$ dla $i \in \mathbb{N}$. Nie wiemy, czym jest k_i dla $i > 16$, jednak istotne dla nas jest, że $l_{16} = \overline{L_{16}}$ oraz $r_{16} = \overline{R_{16}}$. □

2. Aby wykorzystać udowodnioną tożsamość, by zredukować liczbę szyfrowań przy kryptoanalizie DESa, potrzebujemy dwóch par tekst jawny – szyfrogram: (x, c_1) oraz $(\overline{x}, c_2)$. Następnie sprawdzamy po kolei potencjalne klucze – dla danego K obliczamy $y = E_K(x)$. Następnie:

1. Jeśli $y = c_1$, to K jest szukanym kluczem.
2. Jeśli $y = \overline{c_2}$, to szukanym kluczem jest $\overline{K}$.
3. Jeśli żadna z równości nie jest prawdziwa, możemy odrzucić K i $\overline{K}$ z przestrzeni poszukiwań.

W ten sposób jesteśmy w stanie przy pomocy jednego szyfrowania sprawdzić dwa potencjalne klucze naraz. Ciągów bitów mogących być kluczami jest 2^{56}, ale wystarczy 2^{55} szyfrowań by sprawdzić je wszystkie.