Soluții

1a) Relația $y_j = x_j \oplus z_j$ conduce la $x_j = y_j \oplus z_i$, $\forall j = \overline{1,n}$. Ca urmare, având IV și secvența $y = y_1 \dots y_n$, se refac z_j-urile în ordinea $j = 1, \dots, n$ și se obține x_j, pentru orice j.

1b) Fie $L_r(z)$ primii r biți ai lui z și $R_m(z)$ ultimii m biți ai lui z. Putem scrie:

$$y_1 = x_1 \oplus z_1 \Rightarrow x_1 = y_1 \oplus z_1$$
$$y_2 = x_2 \oplus z_2 \Rightarrow x_2 = y_2 \oplus z_2$$
$$y_3 = x_3 \oplus z_3 \Rightarrow x_3 = y_3 \oplus z_3$$

$$z_1 = L_r(e_k(IV))$$
$$z_2 = L_r(e_k(R_m(IV\, y_1)))$$
$$z_3 = L_r(e_k(R_m(IV\, y_1\, y_2)))$$

Ca urmare, dacă în y_3 se modifică bitul de pe poziția p, atunci bitul de pe poziția p va fi modificat și în x_3 (a se observa că z_3 nu depinde de y_3).

Deci, același atac se poate monta și în cazul CFB, cu deosebirea că de data aceasta trebuie modificat y_3 și nu y_2.

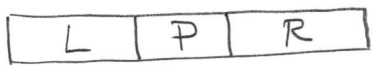
2a) $$y_1^j = e_k(x_1^j \oplus y_1^{j-1})$$
$$y_2^1 = e_k(x_2^1 \oplus y_1^{e_1}).$$

Modificăm x_2^1 la $x^* \oplus y_1^{j-1} \oplus y_1^{e_1}$.

Atunci, $y_2^1 = e_k(x^* \oplus y_1^{e_1})$.

Comparând y_1^j cu y_2^1 putem decide dacă $x_1^j = x^*$ sau $x_1^j \neq x^*$.

2b) Presupunem că x_1^j conține o parolă mică ca sub-bloc al lui x_1^j:



P = parola

Putem presupune că L și R sunt cunoscute deoarece parola este în general inclusă într-un format standard printre primele blocuri ale formatului SSL.

Dacă intrusul are un număr de variante posibile pentru P, fie acestea $\bar{P}_1, \dots, \bar{P}_t$, atunci el poate forma $x_i^* = L \bar{P}_i R$ și verifica (2a) dacă $\bar{P}_i$ este sau nu P.

2c) Criptarea blocurilor X_i, cu $i \geq 2$, cu vectori de inițializare aleși random (vezi 2a). De exemplu, pentru X_2 se poate genera random un vector de inițializare y_2^0 după care criptarea decurge normal:

$$y_2^j = e_k(x_2^j \oplus y_2^{j-1}).$$

Criptotextul Y_2 va fi de această dată:

$$Y_2 = e_k(y_2^0)\, y_2^1 \dots y_2^{t_2}.$$