Avete intercettato la stringa

00001101101110101011111101110100110
11110010011110000101100010101010101

e avete ragione di credere che sia un messaggio in ASCII a 7 bit, cifrato con un registro a scorrimento lineare a 7 bit, e che le prime due lettere del messaggio in chiaro siano `Su`. Decrittate il messaggio.

Su in ASCII a 7 bit = 10100111110101.

I primi 14 bit della stringa sono 00001101101110.

$$\begin{array}{ll} 10100111110101 & \oplus \\ 00001101101110 & = \\ \hline 10101010011011 & \end{array}$$

Questi sono i primi 14 bit di output del registro.

Bisogna risolvere il sistema

$$
\begin{aligned}
0 &= a_0 + a_2 + a_4 + a_6 \\
0 &= a_1 + a_3 + a_5 \\
1 &= a_0 + a_2 + a_4 \\
1 &= a_1 + a_3 + a_6 \\
0 &= a_0 + a_2 + a_5 + a_6 \\
1 &= a_1 + a_4 + a_5 \\
1 &= a_0 + a_3 + a_4 + a_6
\end{aligned}
$$

la soluzione del sistema è $(a_0, \ldots, a_6) = (1, 1, 0, 1, 0, 0, 1)$;

la funzione di retroazione è $x^7 + x^6 + x^3 + x + 1$.

Possiamo generare tutti i 70 bit della chiave, e quindi avere il messaggio in ASCII (facendo lo $\oplus$).

Il testo in chiaro è: `Surrender!`