Problem 12. «The number of rounds»

A famous cryptographer often encrypts his personal data using his favourite block cipher. The block cipher has three variants with $r_1 = 10$, $r_2 = 12$ and $r_3 = 14$ rounds. On this occasion, the cryptographer no longer remembers which of the variants he used.

Fortunately, the cryptographer did ask his students to write down the number of rounds for him. However, in a creative mood, the students decided to encrypt it using a custom cipher E_k with a 4-bit block size. As illustrated in Figure below, round i of their construction XORs the i^{th} nibble k_i of the key $k = k_1 \| k_2 \| \ldots \| k_{r+1}$ with the state and then applies the function S given in Table below. Lacking confidence in their own abilities, the students decided to instantiate the cipher E_k with $r = r_1 \cdot r_2 \cdot r_3 + 1 = 1681$ rounds.

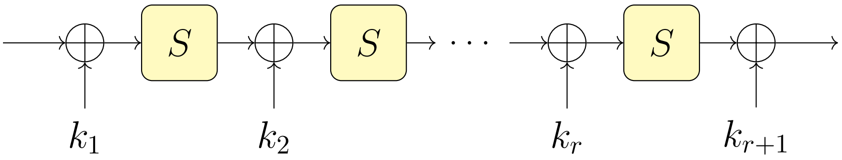

Figure: The students' encryption method.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	3	e	6	8	0	c	b	4	1	d	5	a	7	9	f	2

Table: Lookup table for the function S (in hexadecimal notation).

The students wrote down that the encryption of $r_1 = 10$ is 5 and of $r_2 = 12$ is 0, that is $E_k(1,0,1,0) = (0,1,0,1)$ and $E_k(1,1,0,0) = (0,0,0,0)$. Of course, the students forgot the key, but they still remember that it was an ASCII-encoding of a passphrase consisting only of upper- and lower case English letters. After hearing this, the famous cryptographer exclaims that the students have made a mistake.

How did he know that something was wrong?