



## Problem 5. «Nonlinear hiding»

Nicole is learning about secret sharing. She created a binary vector  $y \in \mathbb{F}_2^{6560}$  and splitted it into 20 shares  $x_i \in \mathbb{F}_2^{6560}$  (here  $\oplus$  denotes the bit-wise XOR):

$$y = x_1 \oplus x_2 \oplus \dots \oplus x_{20}.$$

Then, she created 20 more random vectors  $x_{21}, \dots, x_{40}$  and shuffled them together with the shares  $x_1, \dots, x_{20}$ . Formally, she chose a secret permutation  $\sigma$  of  $\{1, \dots, 40\}$  and computed

$$\begin{aligned} z_1 &= x_{\sigma(1)}, \\ z_2 &= x_{\sigma(2)}, \\ &\dots \\ z_{40} &= x_{\sigma(40)}, \end{aligned}$$

where each vector  $z_i \in \mathbb{F}_2^{6560}$ . Finally, she splitted each  $z_i$  into 5-bit blocks, and applied a secret bijective mapping  $\rho : \mathbb{F}_2^5 \rightarrow \mathcal{S}$ , where

$$\mathcal{S} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, y\}$$

(this strange alphabet has y instead of v).

Formally, she computed  $Z_i \in \mathcal{S}^{1312}$ ,  $1 \leq i \leq 40$  such that

$$Z_i = (\rho(z_{i,1\dots 5}), \rho(z_{i,6\dots 10}), \dots, \rho(z_{i,6556\dots 6560})).$$

After Nicole came back from school, she forgot all the details! She only has written all the  $Z_i$  and she also remembers the first 6432 bits of  $y$  (128 more are missing). The [attachment](#) contains the 6432-bit prefix of  $y$  on the first line and  $Z_1, \dots, Z_{40} \in \mathcal{S}^{1312}$  on the following lines, one per line.

Help Nicole to recover full  $y$ !