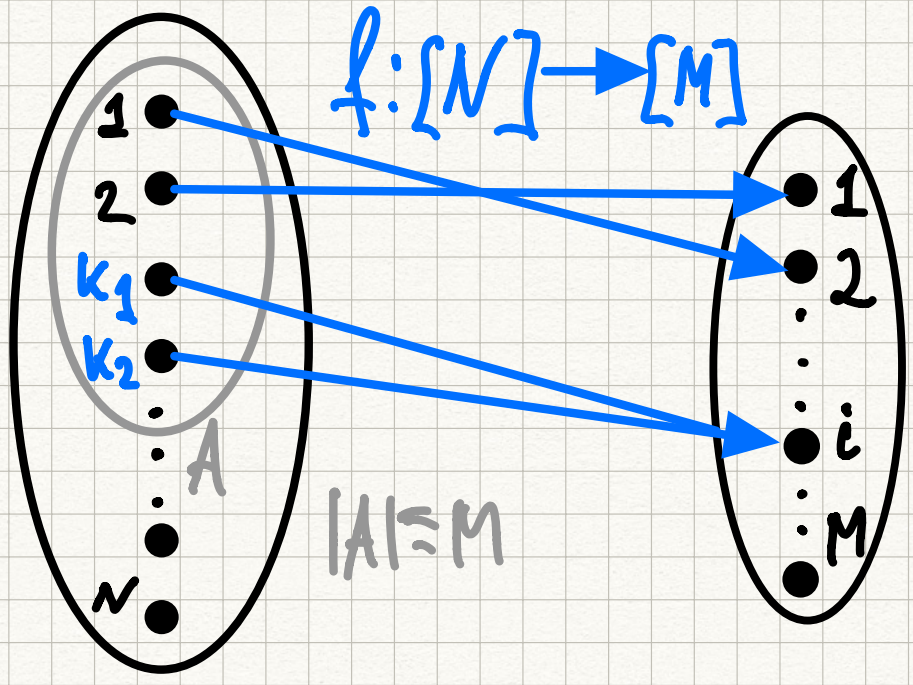

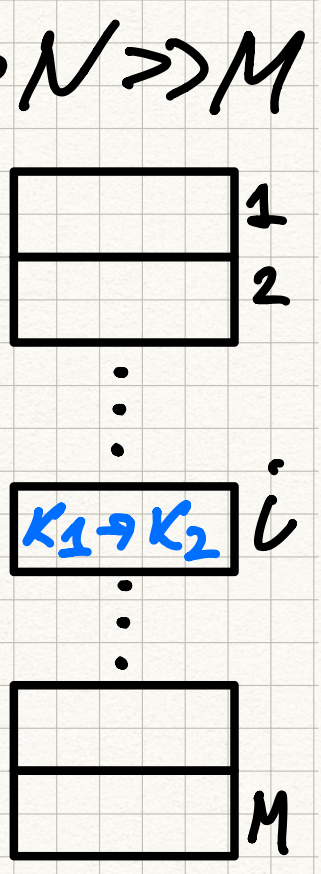

Ключи

$(255)^{30}$

$f \in \mathcal{H}$ – универс.

Семейство хеш. – функций

$$P_{\mathcal{H}}\left[f(x)=f(y)\right]=\frac{1}{M}$$

$256^4 = N$

$M = 257$

$$f_{\vec{a}}(\vec{x}) = a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3 + a_4 x_4 \bmod M.$$

$$\sum_i a_i x_i = \sum_i a_i y_i$$

$$\sum_{i=1}^{3} a_i \left(x_i - y_i\right) = a_4 \left(y_4 - x_4\right) \neq 0$$

$x_4 \neq y_4$

$$a_4 = \left(y_4 - x_4\right)^{-1} \times \sum_{i=1}^{3} a_i \left(x_i - y_i\right)$$

$$\Pr\left(f(x) = f(y)\right) = \frac{\#\ \text{бл. исх}}{\#\ \text{всех исх.}} = \frac{1 \cdot M^3}{M^4}$$

$$= \frac{1}{M} = |\mathcal{H}|$$