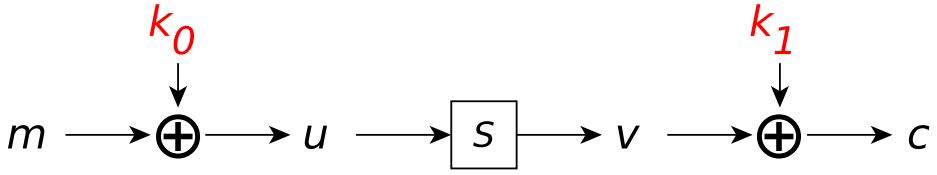
Date: 02/09/2022

Group Name:_____

Make Your Own Mask

$\alpha = (\ ,\ ,\ ,\ ),\quad \beta = (\ ,\ ,\ ,\ )$

*Do **not reuse** masks shown in class*



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S[x]	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5

$\alpha \cdot x$	
$\beta \cdot S[x]$	

$p = ?$

$$\Pr\left[\alpha \cdot x = \beta \cdot S[x]\right] =$$

or

$$\Pr\left[\alpha \cdot x \oplus 1 = \beta \cdot S[x]\right] =$$