

Given  $ax+by = \gcd(a,b) = 1 \Rightarrow (a < b) \wedge (b \text{ is a prime})$

Claim.  $r_0 \cdot S_0 + r_1 \cdot S_1 = \text{size} \cdot k$ ,  $k \in \mathbb{Z}$   
choose  $S_0$  in range  $[33, 126]$   
solve  $S_1$  and  $k$ , in this case we only consider  $S_1$ .

Proof.  $r_0 \cdot S_0 + r_1 \cdot S_1 = \text{size} \cdot k$   
 $\Rightarrow r_1 \cdot S_1 - \text{size} \cdot k = -r_0 \cdot S_0$   
To make it solvable,  
 $r_1 \cdot S_1 + \text{size}(-k) = 1 = \gcd(r_1, \text{size})$

Then use extended euclid algorithm to solve  $S_1$  and  $-k$   
and let  $x_0$  be one solution to  $S_1$  and  $y_0$  be one solution to  $-k$   
 $r_1(x_0) + \text{size}(y_0) = 1$

$$\Rightarrow r_1(-r_0 \cdot S_0 \cdot x_0) + \text{size}(-r_0 \cdot S_0 \cdot x_0) = -r_0 \cdot S_0$$

$$\Rightarrow r_1(r_0 \cdot S_0 \cdot x_0) + \text{size}(r_0 \cdot S_0 \cdot x_0) = r_0 \cdot S_0$$

By definition of linear diophantine equation, the general solution is

$$S_1 = r_0 \cdot S_0 \cdot x_0 + \text{size} \cdot c, \quad -k = \cancel{r_0 \cdot S_0 \cdot x_0 - r_1 \cdot c}, \quad c \in \mathbb{Z}$$

No need to solve  $-k$  in this case, then  $x_0$  must be positive (take absolute)  
Since the character  $S_1$  should be a printable character, then

$$33 \leq S_1 \leq 126$$

$$\Rightarrow 33 \leq r_0 \cdot S_0 \cdot x_0 + \text{size} \cdot c \leq 126$$

$$\Rightarrow 33 - r_0 \cdot S_0 \cdot x_0 \leq \text{size} \cdot c \leq 126 - r_0 \cdot S_0 \cdot x_0$$

Consider  $r_0 \cdot S_0 \cdot x_0 - p = S_1$ , need to find the greatest value within the bound.  
In case of negative bound,

$$\Rightarrow \min\{|33 - r_0 \cdot S_0 \cdot x_0|, |126 - r_0 \cdot S_0 \cdot x_0|\} \leq \text{size} \cdot c \leq \max\{|33 - r_0 \cdot S_0 \cdot x_0|, |126 - r_0 \cdot S_0 \cdot x_0|\}$$

Find  $p$ ,  $\exists i \in \mathbb{Z}^+$ ,  $p = \max\{|33 - r_0 \cdot S_0 \cdot x_0|, |126 - r_0 \cdot S_0 \cdot x_0|\} - i$   
s.t.  $p \bmod \text{size} = 0$

Once we found  $p$ , calculate  $S_1' = r_0 \cdot S_0 \cdot x_0 - p$  is one solution<sup>for  $S_1$</sup> , then  $\exists j \in \mathbb{Z}^+$

$$S_1 = S_1' + j \text{ s.t. } 33 \leq S_1 \leq 126$$

Hence, combined all, thus to obtain the formula

$$\exists i, j \in \mathbb{Z}^+ \quad S_1 = [r_0 \cdot S_0 \cdot x_0 - (\max\{|33 - r_0 \cdot S_0 \cdot x_0|, |126 - r_0 \cdot S_0 \cdot x_0|\} - i)] + j$$

$$\text{s.t. } (\max\{|33 - r_0 \cdot S_0 \cdot x_0|, |126 - r_0 \cdot S_0 \cdot x_0|\} - i) \bmod \text{size} = 0 \wedge 33 \leq S_1 \leq 126.$$