

# Merkle-Hellman Knapsack Cryptosystem

11/4/19

Reg 0-1 Knapsack  $S = \{79, 16, 44, 85, 9, 101\}$

Target = 129

Do some subset of values in  $S$  add upto 129?

NP-Complete (HARD!)

$S = \{3, 6, 10, 22, 47, 100, 207, 511\}$

target = 639

$$a_i > \sum_{j=1}^{i-1} a_j$$

→ Super increasing set.

$$639 - 511 = 128$$

$$128 - 100 = 28$$

$$28 - 22 = 6$$

Secret Set =  $\{3, 6, 10, 22, 47, 100, 207, 511\}$

msg = 0 0 1 1 1 0 1 0

$$\text{conv plain} = 10 + 22 + 47 + 207 = 286$$

① Pick a prime  $> 2 * a_n$  prime = 1091

② Pick multiplier  $k$   $1 < k < p$   $k = 677$ .

③ Public Set is  $\{677 \cdot 3 \pmod{1091}, 677 \cdot 6 \pmod{1091}, \dots, 677 \cdot a_i \pmod{1091}\}$

$T = \{940, 789, 224, 711, 100, 58, 491, 100\}$

public key  
plain 0 0 1 1 1 0 1 0  
cipher =  $224 + 711 + 100 + 491 = 1526$

Recipient knows  $k = 677$  (secret) 11/14/19 @  
can calculate  $k^{-1} \bmod p$

$$677^{-1} \bmod 1091 = 867$$

$$\begin{aligned} \text{Decrypt} &= (\overset{1606}{\cancel{1534}} + 867) \% 1091 \\ &= \cancel{2401} \text{ should get } \underline{286} \\ &= 286 \quad \checkmark \end{aligned}$$

Now we can find the subset of  
the secret super-increasing set

$$\{ 3, 6, 10, 22, 47, 100, 207, 511 \}$$

that adds upto 286, to retrieve

0 0 1 1 1 0 1 0

as the plaintext