Theoretical Brute Force Strategy.

Method: Try to find the correct matrices P, S.

- Pick a P and and S
- Input into a decryption method
- Try again if necessary.

Runtime:

- How long does 1 decrypt take, and how possible P, S are there? Overall time = $c \cdot$ (# of key combos)

Decrypt Computations: c

1. Invert P
2. Multiply Cipher and P^{-1}
3. reedsolo.decode(Cipher, t).
4. Invert S
5. decode $\cdot S^{-1}$

Number of Perm $(n \times n)$:

- Comes from vector permutatation
- So $n!$

Non-singular $(K \times K)$:

of binary matrices $\cdot$ prob. of nosingular

- 1 or 0 for each spot

$$\begin{bmatrix} 2 & \cdot & 2 \\ \cdot & & \cdot \\ 2 & \cdot & 2 \end{bmatrix}$$

posible 2^K row

posible 2^K column.

2^{K^2} binary $K \times K$ matrice

$P < 1$, so $P(2^{K^2})$

Runtime: $c \cdot n! \cdot P(2^{K^2})$: big $O(2^{K^2} n!)$