

秘密鍵

1 0 0 0 1 1 ...

.....

0 0 1 1 1 0 ...

.....

分割 1

1 0 0 0 1 1 ...

.....

分割 2

0 0 1 1 1 0 ...

.....

パリティ

1 0 1 1 0 1 ...

.....