

# **Cypher**

| Task: cypher    | Day: Tuesday        |
|-----------------|---------------------|
| Time limit: 1 s | Memory limit: 32 MB |

For some time, the police has been intercepting encrypted messages from a terrorist group, however they have been unable to decrypt them. Last night, during a raid of an abandoned warehouse, they have seized the encryption device. Careful analysis has unveiled its inner workings.

Device's input consists of plain text, which is first converted to lowercase and stripped of anything but latin letters  $\mathbf{a} \dots \mathbf{z}$  resulting in string  $S = s_1 s_2 \dots s_n$  (making it harder to read). Afterwards, all n cyclical rotations of S ( $S_1 \dots S_n$ ;  $S_i = s_i \dots s_n s_1 \dots s_{i-1}$ ) are sorted lexicographically (see example below). The encrypted message then consists of the index i of the original message and a string R made by taking the last letter of each rotation in the given order.

The string abracadabra would be encoded as 3 rdarcaaaabb as shown in the example below.

- 1. aabracadabr = S11
- 2. abraabracad = S8
- 3. abracadabra = S1
- 4. acadabraabr = S4
- 5. adabraabrac = S6
- 6. braabracada = S9
- 7. bracadabraa = S2
- 8. cadabraabra = S5
- 9. dabraabraca = S7
- 10. raabracadab = S10
- 11. racadabraab = S3

You have been chosen to write a program to recover the string S given the encrypted message (i, R). The program needs to be efficient as the messages have been rather long. There are rumours the terrorists have been encrypting and sending Koran in a number of European languages in a plot to provoke terror and possibly convert some police officers to islam if they were ever forced to read the decrypted messages.

### Task

Given the encrypted message (i, R) on input calculate the original message S.

#### Input

The first line is the number i  $(1 \le i \le n)$ . The second line is the string R of length n  $(1 \le n \le 1\,000\,000)$ . The decrypted message S is guaranteed to exist and to be unique.

### Output

Output the string S on a single line.

## **Example**

| ${\rm input}$ | output      |
|---------------|-------------|
| 3             | abracadabra |
| rdarcaaaabb   |             |
| input         | output      |
| 4             | banana      |
| nnbaaa        |             |