

THE ONE TIME PAD DECRYPTION PROBLEM

You are to create a C# program called OnetimePad that will read a string, a key and encrypt the string using the **ONE-TIME PAD** method of encryption. The program will only deal with lowercase letters. The program will also calculate the decryption-key for that text and decrypt the initially encrypted text.

http://en.wikipedia.org/wiki/One-time_pad

The **ONE-TIME PAD** is a nearly-perfect method of encryption, invented in 1917 by Major Joseph Mauborgne and Gilbert Vernam. The method is also known as the **SECRET LOOKUP TABLE** among clinical laboratory specialists and is the only method of encryption sanctioned by the U. S. **HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)** (2001, as amended). In this method, the sender and receiver agree upon a common secret text, which forms the key. Each key letter is used exactly once, and then discarded forever. Ideally, the key should be completely random. For example, if the receiver and sender employ the text for George Orwell's **1984** as their one-time pad, then the encryption-key becomes:

itwasabrightcolddayinaprilandtheclockswerestrikingthirteenwinston....

Analogously, the decryption-key becomes:

sheaiazjsuthympxxacsna1jspanxhtwypmyqiewjw

Encryption of the plaintext, thequickbrownfox, yields the ciphertext, baaqmidbjxvpptza, as follows:

	thequickbrownfox
(+)	itwasabrightcold

	baaqmidbjxvpptza

that is:

(a-00, b-01, etc.) (use remainder 26)

	19	07	04	16	20	08	02	10	01	17	14	22	13	05	14	23	(plaintext)
(+)	08	19	22	00	18	00	01	17	08	06	07	19	02	14	11	03	(encryption-key)

	01	00	00	16	12	08	03	01	09	23	21	15	15	19	25	00	(ciphertext)
	B	A	A	Q	M	I	D	B	J	X	V	P	P	T	Z	A	

Decryption of the ciphertext, baaqmidbjxvpptza, returns the plaintext, thequickbrownfox, as follows:

	baaqmidbjxvpptza	
(+)	sheaiazjsuthympx	
	<hr/>	
	thequickbrownfox	

that is:

	01	00	00	16	12	08	03	01	09	23	21	15	15	19	25	00	(ciphertext)
(+)	18	07	04	00	08	00	25	09	18	20	19	07	24	12	15	23	(decryption-key)
	<hr/>																
	19	07	04	16	20	08	02	10	01	17	14	22	13	05	14	23	(plaintext)

The decryption-key is calculated as $(26 - \text{encryption-key}) \% 26$

Example: $26 - 8 = 18$ and $18 \% 26 = 18$

This is a sample program run:

Input (code.txt)

```
1
itwasabrightcolddayinapril
thequickbrownfox
```

Output

```
baaqmidbjxvpptza
sheaiazjsuthympxxacsnaajsp
thequickbrownfox
```