MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Autokey Cipher

Author: Chaoyun Li, ECRYPT-NET, KU Leuven

August 2018

Autokey Cipher

We assign $A = 0, B = 1, \cdots, Z = 25$. Assume that the plaintext is $P = p_0 p_1 \cdots p_{n-1}$ and the key is $K = k_0 k_1 \cdots k_{n-1}$, where $p_i, k_i \in \{A, B, \cdots, Z\}$. Then the ciphertext is obtained by

$$c_i = p_i + z_i \pmod{26},\ 0 \leqslant i \leqslant n-1\,. \tag{1}$$

For an autokey cipher the secret key is generated by adding a short keyword to the front of the plaintext.

An Example

Suppose the keyword is “VAUX" and the plaintext is “AUTOKEYCIPHER". Then the key is “VAUXAUTOKEYCI". The encryption process is given below.

plaintext	A	U	T	O	K	E	Y	C	I	P	H	E	R
key	V	A	U	X	A	U	T	O	K	E	Y	C	I
ciphertext	V	U	N	L	K	Y	R	Q	S	T	F	G	Z

To decrypt the message, the recipient would start by writing down the agreed-on key again. Then she can compute $p_1 = V - V = A$. Next, $U - A = U$, and so on. Thus she obtains the first four plaintext characters “AUTO", which can be used as next key characters. This continues until the entire plaintext is reconstructed.

Challenge

Here is a given ciphertext which is encrypted by an autokey cipher:
CLWYSXGHAXASPVVHRFQFFDRKMVKOVYY

Your task is to decrypt this given ciphertext. Please enter the solution in capital letters with spaces between the words.

Hint: The message contains the word "world".