MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Substitution Cipher with Non-Prefix Codes

Authors: Rashmi Bangalore Muralidhar, Mark Stamp

June 2011

Introduction

Substitution ciphers normally use prefix-free codes, i.e. within the ciphertext alphabet there is no symbol which is the prefix of another symbol.

Usually prefix-free codes are used for encryption because it makes the decryption process easier at the receiver's end.
However, this challenge deals with a substitution cipher with non-prefix codes.

The advantage of using non-prefix codes is that extracting statistical information is more difficult.
However, the ciphertext is nontrivial to decrypt, even with the knowledge of the key.

This challenge involves a substitution cipher, where the plaintext is English, the ciphertext symbols are binary strings, and the length of the strings varies.

Introductory Example

For example, consider the following key:

a = 1001	b = 10100	c = 1100	d = 101	e = 11001
f = 1101	g = 10	h = 10000	i = 11011	j = 11
k = 11111	l = 10101	m = 1010	n = 10111	o = 100
p = 1011	q = 1110	r = 0	s = 11000	t = 1111
u = 10010	v = 10001	w = 1000	x=1	y = 111
z = 10110				

Using this key, the plaintext

`thequickbrownfoxjumpsoverthelazydog`

is encrypted as

```
111110000110011110100101101111001111110100010010001011111011001111001010101011
110001001000111001011111000011001101011001101101111011001 0
```

The Challenge

If the key is known, and the plaintext consists of English dictionary words, it is shown in [RBM11] that we can successfully decrypt, using a dynamic program.

In this challenge the additional difficulty is that you do not know the key. The key is different from the one above. So, you have to perform a "ciphertext-only attack".
Determine the plaintext for the ciphertext on the following page, where the plaintext is English.

Note, that only the 26 lowercase letters occur (no word space or punctuation) and all of the words are dictionary words.

Please hand in the whole plaintext as solution, all letters written in lowercase.

Ciphertext and References

```
11011001110101101011111111001111110111110111111011011110111110011010011101111
01111101111110111011111010110101110011011111101110011110010011100110011001010 0
10111101111101100111111010110111111001111010011011111101001100111101110111110
11101101111100111100101101110101110011011110111010011101110111100111011111011
11011111001011010101101011110011110111111101011101100110011101111001101111101 1
11111011101111001101111110111110111011001101111101001011111101110111011111011 1
10011111010001111101111101110011111111110101100111111001011110101010010011100
10111100100111001100111111001
```


[RBM11] R. Bangalore Muralidhar: Substitution Cipher with Non-Prefix Codes, Master's Report, Department of Computer Science, San Jose State University, Spring 2011