MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

A MODIFIED HOMOPHONIC CIPHER WITH REDUCED ALPHABETS – PART 1

Author: Bernhard Esslinger

October 2010 (Updated: May 2019)

Introduction (1/2)

A *monoalphabetic substitution cipher* is a cryptographic technique which uses only one (fixed) ciphertext alphabet for encryption.

A modified version of the monoalphabetic substitution is the *homophonic encryption*. This encryption method was already widely used in the 17th century. In this case (in comparison to the „simple“ monoalphabetic substitution), one plaintext symbol (character) does not need to be mapped on the same ciphertext symbol every time.

Introduction (2/2)

Instead, for each plaintext symbol you have the choice to substitute it by one of several (different) ciphertext symbols. This means that the alphabet for the ciphertext is longer than the alphabet for the plaintext.

The aim of the homophonic substitution is to smoothen the different frequencies of the plaintext symbols so that the ciphertext symbols occur roughly equally frequent.

Challenge

We assume that our words in plaintext form are made up of the signs „0“ and „1“, i.e. the plaintext alphabet $A = \{0, 1\}$.
In common texts the „0“ occurs with a probability of 2/3, and the „1“ with a probability of 1/3.
Furthermore, the bigrams „00“, „01“, „10“ respectively „11“ occur with a probability of 18/30, 2/30, 2/30 respectively 8/30.

So, for instance, a homophonic substitution cipher replaces „0“ by „x“ or „y“ and „1“ by „z“. That way the cipher text is built of the alphabet $B = \{x,y,z\}$.

Challenge

1. Calculate the frequency distribution of the bigrams of the following cipher text. What's conspicuous?

2. Afterwards, determine the most probable plaintext.

xzxxzxzzxxxxzyxyyxzxzxzzxzyyxxxxzzzxzzyyyzzxxxxzxyxzxzyyyyy
yyxzyyzzzzxzzzxzzzzxzzxxxzzxxzzxxzzzyyyyyyyyxzzzxyyzzzzzxyy
yyyyyxxxzxxzzzxzzzxxxzxzzxzxzzxzxzxzxzxxxxxzyyyyyyxxxxzxxxxx
zxyyyyzxyyyyyyyyyyyyxx

The requested solution is the sequence of ones and zeros. It has a length of 199 digits.