MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

KEYSHANC – PART 2

Author: Andrew C. Reed

May 2012

KeyshancRT

In this challenge a plaintext has been encrypted using the KeyshancRT version of Keyshanc. Keyshanc is a kind of monoalphabetic substitution. KeyshancRT improves upon the standard Keyshanc algorithm by integrating a time-based one-time pad (TOTP) that changes every minute. This causes the (yet monoalphabetic) cipher to also change every minute becoming a polyalphabetic cipher. In order to ensure proper decryption of the ciphertext, a custom timestamp is added to the beginning of the ciphertext.

More information can be found at `http://andrewcreed.com/2012/04/25/keyshanc-real-time-overview.html`.

The plaintext is an excerpt from one of William Shakespeare's plays that can be found at `http://www.gutenberg.org/`. It was encrypted using KeyshancRT.

The name of one of the characters in the play was transformed and used as the KeyshancRT password (the character chosen is not necessarily one of the characters from the excerpt). The character's name was transformed by shuffling the letters in the name and then converting the letters to alternating lowercase and uppercase. For example, a character name of "George" might have resulted in a KeyshancRT password of "oEeGrG".

The ciphertext can be found in an additional file that can be downloaded from the MTC3 page for this challenge.

Challenge

What is the next word spoken in the play?

Submit this word in its plaintext form in CAPITAL letters. Please submit only the word – do not submit any surrounding spaces or punctuation marks.