MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

AES ECB Wrong Encoding

Author: Miroslav Dimitrov

December 2017

Introduction

AES is meant to be a very secure encryption method. But it is not only important HOW you encrypt something, but also WHAT you encrypt.

This challenge uses AES in ECB mode with a block size of 16 bytes.

The plaintext of this challenge was wrongly encoded before the encryption.

Challenge

With this kind of encoding, AES degenerates to a mono-alphabetic substitution and can be broken easily. Normally this does not work with AES.

You can find the ciphertext in the additional zip file. The file is called "AES-ECB-ciphertext.txt".

Your task is to break the ciphertext and ... well, additional information can be found in the plaintext :-)