Joshua Marks 1000275m Cyber Security AE1

Cyber Security Report

Known Plain Text Attack

Message: “It is interesting to note that the death penalty for individuals is less controversial than the mere suggestion that a few corporations may have forfeited their right to exist. How many people does a company have to harm before we question if it ought to exist?”
Key: 0xACB4

Cipher Only Attack

Message: “Knowledge possession is not a necessity but what is necessary is the ability to accquire knowledge”
Key: 0x71AA

Theoretical Blocks Needed

Unicity distance = H(k)/D

D = R - r

R = log2(26) = 4.7

r = 1.5

Redundancy of English = 4.7-1.5 = 3.2

Possible keys = 2^{16}

$H(x) = SUM(p(x) * \log_2(1/P(x_i))$ from i = 0 - 2^{16}
$= 2^{16} * 2^{-16} \log_2 (2^{16}))$
$= 2^{16} * 2^{-16} * 16 = 16$

16/3.2 = 5

which = 2.5 blocks or 3 rounded up.

My System is capable of decrypting the given message with just 5 blocks of cipher text. Other messages have been decrypted using just 3 blocks.

TMT

Message: “All I ask is a chance to prove that money can't make me happy”
Key: 0x36A0