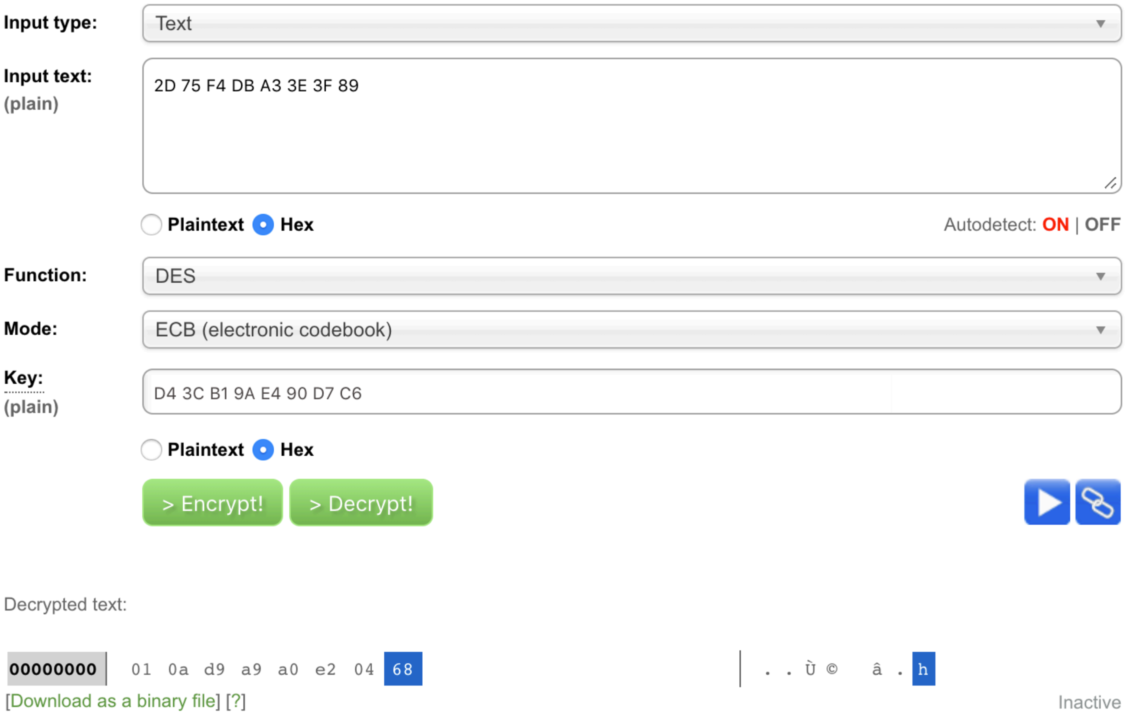
Willis Allstead
October 10, 2018
CS 450

Homework 2

1.

The 64-bit output of round 1 in DES using the provided plaintext and key is:

01 0A D9 A9 A0 E2 04 68



Input type: Text

Input text: (plain) 2D 75 F4 DB A3 3E 3F 89

○ Plaintext ● Hex Autodetect: ON | OFF

Function: DES

Mode: ECB (electronic codebook)

Key: (plain) D4 3C B1 9A E4 90 D7 C6

○ Plaintext ● Hex

Decrypted text:

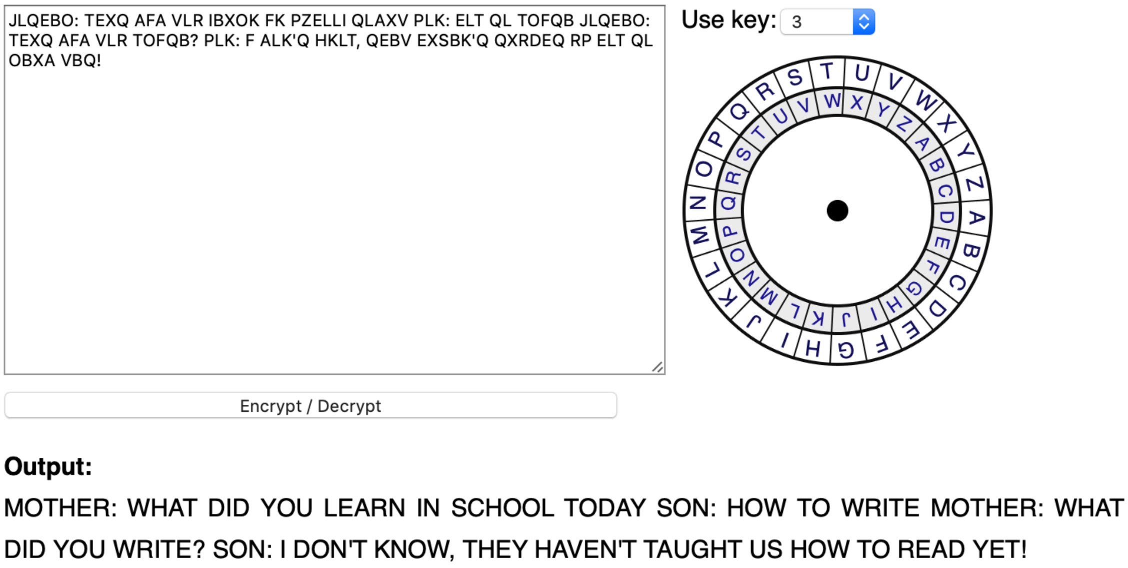
```
00000000  01 0a d9 a9 a0 e2 04 68          . . Ù ©   â . h
```

Above is the website I used with the inputs I used.

2.

Given the encrypted text and running it through the site you gave with the "use key" box set to guess, it arrived at the key of 3 with a plain text output (with my own formatting) of:

MOTHER: WHAT DID YOU LEARN IN SCHOOL TODAY
SON: HOW TO WRITE
MOTHER: WHAT DID YOU WRITE?
SON: I DON'T KNOW, THEY HAVEN'T TAUGHT US HOW TO READ YET!



JLQEBO: TEXQ AFA VLR IBXOK FK PZELLI QLAXV PLK: ELT QL TOFQB JLQEBO: TEXQ AFA VLR TOFQB? PLK: F ALK'Q HKLT, QEBV EXSBK'Q QXRDEQ RP ELT QL OBXA VBQ!

Use key: 3

Output:

MOTHER: WHAT DID YOU LEARN IN SCHOOL TODAY SON: HOW TO WRITE MOTHER: WHAT DID YOU WRITE? SON: I DON'T KNOW, THEY HAVEN'T TAUGHT US HOW TO READ YET!

Above is the exact way the site looked and what I inputed to revive the output.

3.

I’m going to do my calculations based on the processor speed of my 4 year old MacBook Pro, which I think accurately represents the average processor speed these days, especially in laptops: 2.2GHz.

Let’s also assume it takes 220 cycles for an ordinary computer to brute force for each DES key/AES key.

A = 2^56 keys
B = 220 cycles
C = 2200000000 Hz
D = years it will take
E = 2^128 keys (for AES)

So for cracking a DES encryption by testing all 2^56 possible keys it it would take:

D = A * B / 365 days / 24 hours / 60 minutes / 60 seconds / C
= about 228.49 years.

So for cracking a AES encryption by testing all 2^128 possible keys it it would take:

D = E * B / 365 days / 24 hours / 60 minutes / 60 seconds / C
= about 1.079028307E24 years. (longer than the time since the big bang)