CIS 3362 Homework #4: Crack DES
Assigned: 10/12/16
Due: 10/26/16

Groups: Please choose groups of four to work on this assignment

The goal will be to break the ciphertext given at the end of this assignment. A file with the same contents will also be posted on the course web site. You are given one block of matching plain and cipher text.

Protocol used to carry out DES

The original plaintext message was written using valid Radix-64 characters only. A list of these characters and their conversions to a 6-bit integer can be found online: https://en.wikipedia.org/wiki/Base64.

The original plaintext file contained exactly 10 Radix-64 characters per line. For each line, these characters were converted to their binary equivalent, yielding 60 bits. Then, four 0s were added to the end of this, creating 64 bits.

These 64 bits are the input to DES.

Then, the 64 output bits from DES were padded with two more 0s, creating a ciphertext of 66 bits.

These 66 bits were then converted back to 11 Radix-64 characters. Thus, the given ciphertext file consists of 11 Radix-64 characters per line.

To help you with the assignment, you may use the implementation of DES shown in class that is posted on the course web page.

Key Restrictions

20 bits of the key are restricted as follows (note: the convention being used is that the key bits are labeled from k_1 through k_{64} with the parity bits k_8, k_{16}, k_{24}, k_{32}, k_{40}, k_{48}, k_{56}, and k_{64}):

$k_i = k_{32+i}$ for the following values of i: 1 – 5, 9 – 13, 17 – 21, and 25 – 29.

What To Turn In (Over WebCourses)

Each group should make one submission. Namely, exactly one person from each group should submit the assignment. Each submission should contain the following:

1) All code used to help break the message.

2) A write-up explaining the process by which you tried to break the message, as well as a summary of the progress made, including the key and message, if found.

Matching Plaintext and Ciphertext

```
Plaintext block of 10 radix-64 chars: wewin2016+
Ciphertext block of 11 r-64 chars:   Azuigo8gxOE
```

Ciphertext to Break

```
cFdpCJTPTys
ScNJ/pChwdE
OTevA+r4Ps8
v+6nwCb7mOA
YSzFg3bTOQQ
a4pdozOAWPY
9mJSj6ie8H0
xRkY+wOO3mQ
rgFRfgUwbY8
eAVXR/08Gso
DnALUe8PSiE
3IhkGOzTd0E
Ods/XBgqCrE
q6YfX8DoTog
1p56/dJxhxs
A3KRLVOlcwQ
OZGzEY7uHn0
2lx68EFoX8w
ZbBvuNCAlnA
17S1W7u6Ass
yadEkUcrwGk
1BOW3guQSYU
vDP0GEYQCU4
nB8ETPqx8hE
OjZDh2dEKBk
tsG/5RIgYvI
E8cm7coQANc
jqqJWr5m21Y
P9KDzFxfQYY
JcFf1nymg+g
RZakYLLtYzw
91PZsCjFJ54
grsluLy9uwY
aLKxlsR+U3U
ypEeGvwG9a4
EwO01Qa0Fo4
ezssHbBuRJk
yQ/dRppz6u4
bY8l/RS6Yc8
zXnwSWInNRI
jrc+zYg9eYE
```