Background

Mr. C. Lueless was charged with designing a crypto system for his company. Instead of using regular DES, he chose to use a variant of double-DES which he called DDES-48, as follows.

- Input key: 48 bit key $Z$, as 6 bytes denoted $Z = (z_0, ..., z_5)$.
- Input plaintext: 64 bit value $P$
- $K_1 := 00\ 00\ 00\ 00\ 00\ z_0\ z_1\ z_2$  
  (the 3 left bytes of the key inserted into the 3 right bytes of $K_1$).
- $K_2 := 00\ 00\ 00\ 00\ 00\ z_3\ z_4\ z_5$
- Output ciphertext: $C := \text{DES}(K_2, (\text{DES}(K_1,P)))$

Example

$Z: 12\ 34\ 56\ 78\ 90\ ab$  
$K_1: 00\ 00\ 00\ 00\ 00\ 12\ 34\ 56$
$K_2: 00\ 00\ 00\ 00\ 00\ 78\ 90\ ab$
Encrypting: 61\ 61\ 61\ 61\ 61\ 61\ 61\ 61$ [ASCII ‘aaaaaaaa’]  
After 1st DES text is: 15\ ab\ 8b\ d9\ 08\ 8b\ 5e\ ec  
Output is: 64\ 25\ c8\ 1a\ a2\ be\ 83\ 19

Questions

1. Write a program that implements a meet-in-the-middle attack for Mr. Lueless’s DDES-48 cipher, and computes a valid encryption key. Note that there can be many equivalent keys — any one of them is a valid answer.

   Each student has a different key to break. For this, each student has one pair of plaintext-ciphertext.

   The plaintext for all students is “DESsDead” (in hex: 44\ 45\ 53\ 73\ 44\ 65\ 61\ 64). The table of ciphertexts is available at http://www.eng.tau.ac.il/~yash/crypto-netsec/ex3-data.html. If you see that there is no ciphertext for your TEUDAT ZEHUT number contact the teacher.

   Efficiency is important: try to minimize the enumeration space (how many times you do a DES encryption/decryption), and use reasonably efficient data structures. A well written program will run for several minutes on a PC running a 3GHz Pentium 4. If your program takes more than 30min to complete, you may be using an inefficient method.
Submission Instructions

Submission is both on paper and electronically.

- Hand in a printout of your program, and the results of its run. Code without reasonable comments will get a reduced grade!

- In addition, send the results of the question by email, as follows:
  1. Send your results via email to crypto-netsec@eng.tau.ac.il.
  2. The subject should be: **ex3**, exactly: in lower case letters, without a dash (“-”) between the “x” and the “3”.
  3. The body of the email should contain 2 lines, including the leading keywords and the “:=” symbols:

```
TZ := your "Teudat Zehut" number (9 digits)
Z := the key you broke (12 hex digits)
```