Cryptography Fall 2013: Cipher Challenge
Group Project (Groups of 4)

The Rules

Every group will create a **symmetric** cipher system that has a key size of 48 bits and encrypts blocks of 48 bits in electronic codebook mode. (Thus, the total number of possible keys should equal 2^{48}.) The output for your algorithm must also be exactly 48 bits. Note: electronic codebook mode is defined in the text on page 199. Your cipher must NOT resemble any of the well-known ciphers too closely. In essence, I am looking for creativity as opposed to ripping off a scheme that you've already seen.

Part I (Due Friday, 10/18, via email to dmarino@cs.ucf.edu)

Each group should give me a formal description of the cryptosystem they have created (Word doc), as well as a function I can use to encrypt a single block, in Java, using their system. A sample prototype for the function is included below. (Note: Each group will be assigned a color.)

```
// Precondition: plaintext and key are arrays of length 6
// Postcondition: The ciphertext will be returned in an array of size 6.
public static byte[] Red_Encrypt(byte[] plaintext, byte[] key);
```

Also write a corresponding decryption function with the following prototype:

```
// Precondition: key is an array of length 6
// Postcondition: The ciphertext will be returned in an array of size 6.
public static byte[] Red_Decrypt(byte[] ciphertext, byte[] key);
```

Since you are creating a symmetric scheme, it is expected that the same key is used to decrypt a message as was used to encrypt the message.

Part II(Friday, 10/25 or Monday 10/28)

Each group will be given the opposing group's encryption code and a single encrypted message (many blocks) using the opposing group's cipher. Your team's goal will be to determine the plaintext AND the key the opponent used.

Note: These files will be written in Radix-64, with 8 Radix-64 characters per line. Each line will store a single block. Feel free to come and ask me further questions if this isn't clear.

Part III(Nov 22 - 27)

Each group will present on their work for the contest. Each presentation will be in two phases:

1) Creation of the group's cipher and explanation of design choices.
2) Discussion of attempts to break the opposing cipher.

Part IV(Monday, 12/2)

Your group should give me two reports:

1) A detailed description of your cipher and the design choices made.

1) A detailed description of the process used to break (or at least attempt to break) the cryptosystem you were given. Discuss how you used each added piece of information to help deduce how the system works, what the key was, and what the plain text to the original messages was.

How the winner will be chosen and how the project will be graded

Although this may not be 100% fair, I will choose the winner based on who decrypts the original message first AND determines the encryption key. You may simply email to me (to dmarino@cs.ucf.edu) what you think the plaintext corresponding to these original messages is as well as the key. Whichever email I receive first with a correct response wins**. The project will be graded almost solely upon the final presentation and write-up.** I will be looking for a methodical explanation to your decrypting attempts that utilize ideas presented in class. I will also be looking for sound mathematical justifications for evidence of the difficulty or lack thereof, of the cryptosystem you create. Thus, you could get a 100% on this project even if you don't win.

As the dates come closer, I will give you a more detailed description of what I expect for each part of the project.