Name:Chao Jiang
ECE5563 — Spring 2015 **HW 1** Due: Jan. 28

Problem 2.1

A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C:

$$C = E([a, b], p) = (ap + b)\, mod\, 26$$

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for $a = 2$ and $b = 3$, then $E([a, b], 0) = E([a, b], 13) = 3$.

a. Are there any limitations on the value of b? Explain why or why not.

   No, but the effective range of b is from 0 to 25. Because any number of b larger than 25, we always can replace it with one from 0 to 25 to take the same function.

b. Determine which values of a are not allowed.

   0,2,4,6,8,10,12,13,14,16,18,20,22,24 are not allowed in the range from 0 to 25. Like the answer above, we also do not need to take any number larger than 25.

c. Provide a general statement of which values of a are and are not allowed. Justify your statement

   The value of a and 26 must be relatively prime. From the question we know that we must satisfy $E(p) \neq E(q)\; if\; p \neq q$, so we can derive from the suppose that if $E(p) = E(q) when p \neq q$. $(ap+b) mod 26 = (aq+b) mod 26 \Rightarrow a(p-q) = (k_1-k_2)*26$. Then we can deduct that and should have no common positive integer factor other than 1.

Problem 2.2

How many one-to-one affine Caesar ciphers are there?

From the question 2.1 we can get that, a has 12 values and b has 26 values that can be chosen. Thus the total number of one-to-one affine Caesar ciphers is $12 * 26 = 312$.

Problem 2.18a

Determine the inverse mod 26 of

$$\begin{pmatrix} 2 & 3 \\ 1 & 22 \end{pmatrix}$$

From $det \begin{pmatrix} 2 & 3 \\ 1 & 22 \end{pmatrix} = 2 * 22 - 1 * 3 = 41\, mod\, 26 = 15,\; then\; 15^{-1}\, mod\, 26 = 7$, we know that $A^{-1} = (det(A))^{-1} \begin{pmatrix} cof_{11}(A) & cof_{12}(A) \\ cof_{21}(A) & cof_{22(A)} \end{pmatrix} = 7 \times \begin{pmatrix} 22 & -3 \\ -1 & 2 \end{pmatrix} mod\, 26 = \begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}$

Name:Chao Jiang

ECE5563 — Spring 2015 **HW 1** Due: Jan. 28

Problem 3.7

Show that DES decryption is, in fact, the inverse of DES encryption.

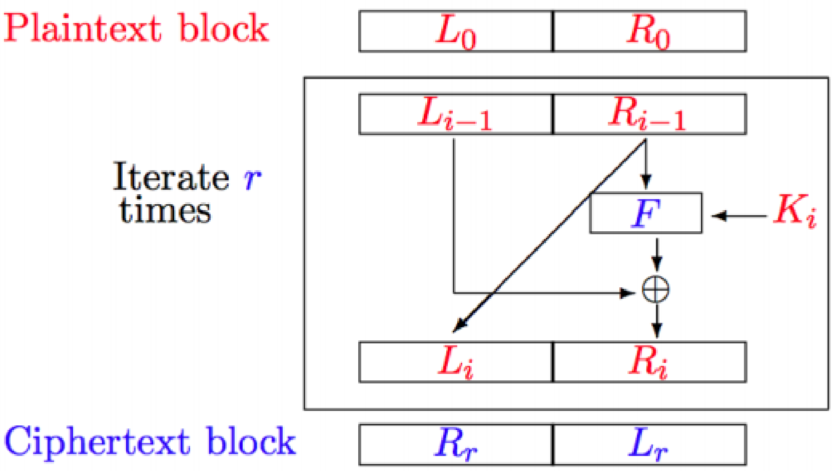
For Encryption(E)

- Input plaintext to initial permutation box to get L_0 and R_0.
- Repeat 16 times with
  $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
  $L_i = R_{i-1}$
  to get L_{16} and R_{16}
- Swap them to get $R_{16}L_{16}$
- Put $R_{16}L_{16}$ to inverse permutation box to get ciphertext

For Decryption(D)

- Input ciphertext to initial permutation box to get A_{16} and B_{16}.
- Repeat 16 times with
  $B_{i-1} = A_i \oplus f(B_i, K_i)$
  $A_{i-1} = B_i$
  to get A_0 and B_0
- Swap them to get B_0A_0
- Put B_0A_0 to inverse permutation box to get back the plaintext

DES is basically a multi round Feistel cipher that accepts 64 bit plaintext blocks as input and a 56 bit key. At the same time, Feistel decryption is the inverse of Feistel encryption. The structure of Feistel Cipher is shown as the below figure. Therefore, needless to say, DES decryption is the inverse of DES encryption.


Plaintext block
L_0
R_0
L_{i-1}
R_{i-1}
Iterate r times
F
K_i
L_i
R_i
Ciphertext block
R_r
L_r