TCOM 500: Modern Telecommunications
Prof. B.-P. Paris
Homework 5
Due: March 4, 2010

Reading Chapters 30 and 31 in Forouzan; review class notes.

Problems

1. **ISBN Correction:** Find the missing digit in the ISBN below:
   (a) 0-385-49531-?
   (b) 0-201-1?794-2
2. **Hamming Code:** Messages are sent using the (7,4) Hamming code discussed in class. For each of the following received code words, decide if an error has occured and if so, determine the most likely corrected code word.
   (a) 0001 111
   (b) 0101 101
   (c) 0100 111
3. **Transposition Cipher:** A transposition cipher uses a five-by-five matrix and permutes columns before reading them out.
   (a) How many different column permutations (keys) are possible with such a cipher?
   (b) Decrypt the following - you will have to guess the key:
   HTASL LEEOT ASWME TSSAP EMGCE
4. **Substitution Cipher:** Linear ciphers are a systematic way to construct substitution cipher using a key a. Let a be an integer between 1 and 26 aand let x be the integer corresponding to one of the 26 letters in the alphabet. The linear cipher transforms the plaintext x into the ciphertext y by

   $$y = a \cdot x \bmod 26.$$

   For example, if $a = 3$ and the message is "d," then the ciphertext is $y = 3 \cdot 4 = 12$. If the message is "k," the ciphertext is $y = 3 \cdot 11 \bmod 26 = 7$.

   For a key a to be acceptable, the value of a must be invertible modulo 26. That means the correspondence btween x and y can

be uniquey inverted. A case that does not have this property is $a = 4$, because then both $x = 3$" ("c") and $x = 16$ ("p") lead to $y = 12$. One can show that an a is invertible if it has no common factors with 26. Hence, 4 is not invertible because both 4 and 26 can be divided by 2.

(a) List all invertible values of a.

(b) For $a = 11$, encrypt the plaintext I LIKE TCOM.

(c) Decipher the following ciphertext (you'll have to guess a):

13 9 9 10 7 10 20 11 20 9

5. **Feedback Shift Register:**

(a) Draw a diagram of the feedback shift register with feedback connections 101001.

(b) Compute the first four outputs of this shift register if the initial contents is 11001.