TCOM 500: Modern Telecommunications
Prof. B.-P. Paris
Homework 5
Solution

Problems

1. **ISBN Correction:** Let the unknown digit be denoted by x.

   (a) 0-385-49531-?: the ISBN must satisfy

   $$0{\cdot}1{+}3{\cdot}2{+}8{\cdot}3{+}5{\cdot}4{+}4{\cdot}5{+}9{\cdot}6{+}5{\cdot}7{+}3{\cdot}8{+}1{\cdot}9{+}x{\cdot}10 = 0 \bmod 11.$$

   Evaluating the products, leads to

   $$192 + 10 \cdot x = 0 \bmod 11$$

   and, therefore, $x = 5$ because 242 is divisable by 11.

   (b) 0-201-1?794-2: the ISBN must satisfy

   $$0{\cdot}1{+}2{\cdot}2{+}0{\cdot}3{+}1{\cdot}4{+}1{\cdot}5{+}x{\cdot}6{+}7{\cdot}7{+}9{\cdot}8{+}4{\cdot}9{+}2{\cdot}10 = 0 \bmod 11.$$

   Evaluating the products, leads to

   $$190 + 6 \cdot x = 0 \bmod 11$$

   and, therefore, $x = 5$ because 220 is divisable by 11.

2. **Hamming Code:**

   (a) 0001 111 - Syndrome is 000, therefore this is a correct codeword.

   (b) 0101 101 - Syndrome is 100, therefore the most likely correct codeword is $0100\tilde{1}01$.

   (c) 0100 111 - Syndrome is 110, therefore the most likely correct codeword is $0100\tilde{1}01$.

3. **Transposition Cipher:**

   (a) There are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ different ways to permute the columns.

(b) Arrange the message into a 5x5 matrix:

$$\begin{array}{ccccc} H & L & A & T & E \\ T & E & S & S & M \\ A & E & W & S & G \\ S & O & M & A & C \\ L & T & E & P & E \end{array}$$

With a little bit of trial-and-error (the characters THE in the first row are pretty helpful), it is apparent that thet columns should be permuted as follows

$$\begin{array}{ccccc} T & H & E & L & A \\ S & T & M & E & S \\ S & A & G & E & W \\ A & S & C & O & M \\ P & L & E & T & E \end{array}$$

and we can decode: THE LAST MESSAGE WAS COMPLETE

4. **Substitution Cipher:**

(a) The number 26 is divisable by 2 and 13. Therefore, invertible keys cannot be divisable by 2 or 13. The invertible values of a are $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$.

(b) For $a = 11$, the pertinent substitutions are

Plaintext		Ciphertext	
plain letter	x	$y = a \cdot x \bmod 26$	cipher letter
C	3	7	G
E	5	3	C
I	9	21	U
K	11	17	Q
L	12	2	B
M	13	13	M
O	15	9	I
T	20	12	L

The encrypted message is: U BUQC LGIM.

(c) The presence of three 9's in the cipher text suggests that the corresponding plaintext letter is an E. The key $a = 7$ maps

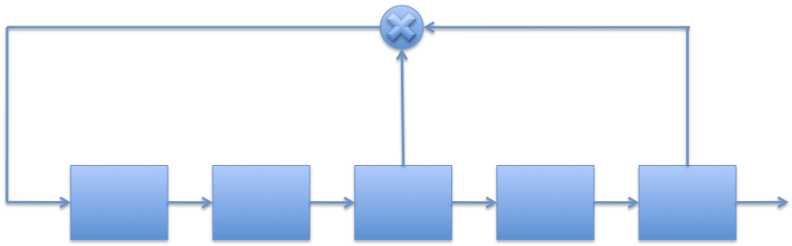
E to 9, because $7 \cdot 5 \bmod 26 = 9$. With the key $a = 7$, the pertinent substitutions are

Plaintext		Ciphertext	
plain letter	x	$y = a \cdot x \bmod 26$	cipher letter
A	1	7	G
E	5	9	I
T	20	10	J
I	9	11	K
M	13	13	M
N	14	20	T

and the decoded message is: MEET AT NINE.

5. **Feedback Shift Register:**

   (a)



   (b) The following table shows the contents of the shift register (MSB corresponds to rightmost register) and the corresponding output (which is just the MSB:

Register Contents	Output
11001	1
10011	1
00111	0
01111	0
11111	1
11110	1