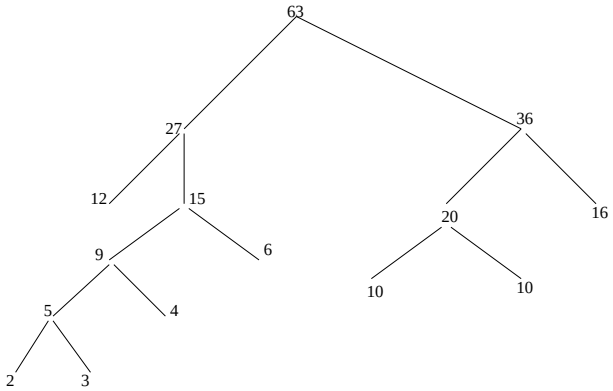
1. (Compression)

   (a) A Huffman tree for symbols with the frequencies {6, 4, 10, 3, 16, 2, 10, 12} is shown below.



   (b) Table 1 shows the dictionary. Concatenate the words in the dictionary to get the transmitted string. It is $p|q|r|rq|s|pq|rr|qs|pqr|rqr|pq\#|$; I have placed | at the positions where a transmission takes place.

index	word	transmission
0	$\langle\rangle$	none
1	p	$(0, p)$
2	q	$(0, q)$
3	r	$(0, r)$
4	rq	$(3, q)$
5	s	$(0, s)$
6	pq	$(1, q)$
7	rr	$(3, r)$
8	qs	$(2, s)$
9	pqr	$(6, r)$
10	rqr	$(4, r)$
11	$pq\#$	$(6, \#)$

Table 1: Transmission using Lempel-Ziv Code

2. (Error Correction)

(a) $L \cup R$ is a dependent set because $\hat{L} \oplus \hat{R} = \hat{L} \oplus \hat{L} = 0$. From the given construction, $l \cup r = L \cup R$. So, $l \cup r$ is a dependent set and partitioning it into l and r yields sets with the same exclusive-or.

(b) First, we compute the hamming distances between the codewords, see Table 2. Since the minimum distance is 4, we can detect 3 errors and correct 1 error.

	11111111	11001100	10011001	10010110
11111111	0	4	4	4
11001100	4	0	4	4
10011001	4	4	0	4
10010110	4	4	4	0

Table 2: Hamming distances between the codewords, Problem 2

(c) We compute the distances of the received strings from the codewords, see Table 3. Since the minimum distance for 11001000 is 1, we can correct the error and claim that 11001100 was sent. For 11011101, the minimum distance is 2, and we can only claim that there have been two errors in the transmission.

	11111111	11001100	10011001	10010110
11001000	5	1	3	5
11011101	2	2	2	4

Table 3: Hamming distances between codewords and received word, Problem 2

(d) We show that the distance between any two rows of the matrix at any point during the computation is 2^{n-1}. This is our invariant.

The claim is initially true because the matrix is H_n. We show that each of the operations preserves the distances among the rows. Complementing the bits in a row keeps its distance from all other rows at 2^{n-1}; see the observation (reproduced from the notes, below). Complementing all the bits in a column preserves the distance between any two rows, because two rows which matched at that column continue to match and those which differed continue to differ. Exchanging two rows does not affect distances among rows. And, exchanging two columns also does not affect distances among rows.

Observation Let p and q be words of even length, say $2 \times t$. Then

$$\begin{aligned} d(p,q) = t &\equiv d(\overline{p},q) = t \\ d(p,q) = t &\equiv d(p,\overline{q}) = t \\ d(p,q) = t &\equiv d(\overline{p},\overline{q}) = t \end{aligned}$$

□

3. (Cryptography)

(a)
$$
\begin{aligned}
& 23^{28} \bmod 7 \\
= \quad & \{\text{Modular Simplification Rule}\} \\
& (23 \bmod 7)^{28} \bmod 7 \\
= \quad & \{23 \bmod 7 = 2\} \\
& 2^{28} \bmod 7 \\
= \quad & \{\text{rewrite } 2^{28}\} \\
& (2^6 \times 2^6 \times 2^6 \times 2^6 \times 2^4) \bmod 7 \\
= \quad & \{\text{use Modular Simplification Rule to convert } 2^6 \text{ to } 2^6 \bmod 7\} \\
& ((2^6 \bmod 7)^4 \times 2^4) \bmod 7 \\
= \quad & \{7 \text{ is prime, and 2 and 7 are relatively prime;} \\
& \quad \text{from Fermat's Theorem, } 2^6 \bmod 7 = 1\} \\
& ((1)^4 \times 2^4) \bmod 7 \\
= \quad & \{\text{simplify}\} \\
& 16 \bmod 7 \\
= \quad & \{\text{compute}\} \\
& 2
\end{aligned}
$$

(b) Let the i^{th} plaintext block be p_i, and the encrypted block be b_i, $i > 0$. Let the secret key be denoted by p_0. Then,

$$b_i = p_i \oplus p_{i-1},\ i > 0$$

Each encrypted block is the exclusive-or of two p blocks. Taking exclusive-or of any two b_is yields a block which is exclusive-or of even number of p terms, because even number of terms (possibly 0) get cancelled by taking exclusive-or. Therefore, no single p term can ever be isolated.