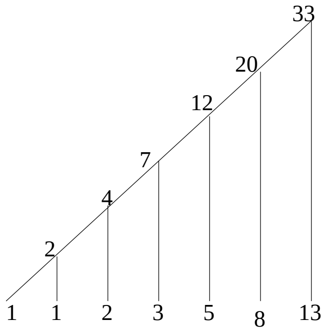
1. (Compression)

   (a) The probability of each symbol is $1/16$. The entropy is $16 \times (-1/16) \times log(1/16) = -log(1/16) = 4$.

   (b) A Huffman tree for symbols with the frequencies $\{1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13\}$ is shown below.



   The weight of the tree is easily computed by adding the weights at the internal nodes; it is 78.

   (c) i. The transmissions corresponding to the given trie are shown in Table 1.

index	word	transmission
0	$\langle\rangle$	none
1	a	$(0, a)$
2	aa	$(1, a)$
3	c	$(0, c)$
4	b	$(0, b)$
5	cb	$(3, b)$
6	cc	$(3, c)$
7	bb	$(4, b)$
8	aaa	$(2, a)$
9	aad	$(2, d)$
10	ad	$(1, d)$
11	ba	$(4, a)$

Table 1: The transmissions corresponding to the given trie

   ii. The transmitted string is the concatenation of the strings in the second column of the table given above: $aaacbcbccbbaaaaadadba$.

index	word	transmission
12	*cbc*	$(5, c)$
13	*bba*	$(7, a)$
14	*bbb*	$(7, b)$
15	*cba*	$(5, a)$
16	*cbb*	$(5, b)$
17	*bbc*	$(7, c)$
18	#	$(0, \#)$

Table 2: The transmissions corresponding to *cbcbbabbbcbacbbbbc#*

iii. The pairs that have to be transmitted for *cbcbbabbbcbacbbbbc#* given that this trie already exists are listed in Table 2.

2. (Error Correction)

(a) Charles creates 4 words $r_{00}, r_{01}, r_{10}, r_{11}$, and sends them to Alice. He also creates a 2-bit number d and sends d and r_d to Bob.

Now, suppose Bob needs r_c, $c \in \{00, 01, 10, 11\}$. Then he sends e, where $e = c \oplus d$. Alice responds by sending a 4-tuple $(f_{00}, f_{01}, f_{10}, f_{11})$, where $f_i = m_i \oplus r_{e \oplus i}$. Bob computes $f_c \oplus r_d$; we show that this is m_c.

$$\begin{aligned} & f_c \oplus r_d \\ =\ & m_c \oplus r_{e \oplus c} \oplus r_d \\ =\ & m_c \oplus r_{c \oplus d \oplus c} \oplus r_d \\ =\ & m_c \oplus r_d \oplus r_d \\ =\ & m_c \end{aligned}$$

(b) He can't always remove from the largest pile. Consider three piles with 2, 4 and 5 chips. Their execlusive-or is $010 \oplus 100 \oplus 101 = 011$. Since the result is non-zero, this is a winning configuration for the first player. The first player should remove enough chips from a pile so that the execlusive-or of the piles becomes 0, to retain a winning strategy. If he removes from pile with 5 chips and leaves x chips there, the requirement forces us to have $010 \oplus 100 \oplus x = 000$, i.e., $x = 010 \oplus 100 = 110 = 6$. This is impossible given that the pile has 5 chips to start with.

We wish to derive the condition under which the first player can remove an entire pile. Let the execlusive-or of the remaining piles be y. After his move, the state is a losing state, i.e., $y = 0$. Thus the required condition for removing a pile is that execlusive-or of the remaining piles is 0. Equivalently, a pile with x chips can be removed only if the excusive-or of all the piles is x.

(c) We see that 4 check bits are needed. We place the check bits in positions 1, 2, 4, 8. So, the data bits are placed as shown in Table 3.

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	1	0	0	*	1	1	1	*	0	*	*

Table 3: Hamming code transmission, data bits only

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	1	0	0	1	1	1	1	1	0	0	0

Table 4: Hamming code transmission, complete string

Next, we need to compute the check bit values. Take the positions where the data bits are 1s and form their exclusive-or.

$$\begin{array}{cll} & 1\ 1\ 1\ 1 & (=15) \\ \oplus & & \\ & 1\ 1\ 0\ 0 & (=12) \\ \oplus & & \\ & 1\ 0\ 1\ 1 & (=11) \\ \oplus & & \\ & 0\ 1\ 1\ 1 & (=7) \\ \oplus & & \\ & 0\ 1\ 1\ 0 & (=6) \\ \oplus & & \\ & 0\ 1\ 0\ 1 & (=5) \\ = & 1\ 1\ 0\ 0 & \end{array}$$

Therefore, we store 1s in positions 8 and 4 and 0s in positions 2 and 1. The string that is transmitted is shown in Table 4.

(d) First, we compute the hamming distances between the codewords, see Table 5. Since the minimum distance is 2, we can detect 1 errors and correct 0 error.

	11111	10001	00111	01000
11111	0	3	2	4
10001	3	0	3	3
00111	2	3	0	4
01000	4	3	4	0

Table 5: Hamming distances between the given codewords

(e) We compute the distances of the received strings from the codewords, see Table 6. Since the minimum distance for 10101 is 1, we take the nearest codeword, 10001, as the transmitted string. For 10100, we choose any codeword other than 10001.

	11111	10001	00111	01000
10101	2	1	2	4
01011	2	3	2	2

Table 6: Hamming distances between codewords and received word

3. (Cryptography)

   (a) Each bidder needs to send a number between 1 and 99. If these numbers are sent directly, there are 99 possible messages, and it is easy for an interceptor to decode even an encrypted message (he just constructs all 99 encoded strings using the public key of eBay). Therefore, we need a scheme where the number of possible messages is large, but each message can be decoded into one of 99 possible values using an algorithm. (The requirement that an algorithm has to be used eliminates the possibility of sending messages such as, "I can go no higher than 50".)

   Let eBay proclaim that a bidder should send any number k in encrypted fashion, where $1 \leq k \leq M$, for a suitably large M. The bid is k mod 100.

   (b)
$$\begin{array}{ll}
 & 79^{62} \bmod 7 \\
= & \{\text{Modular Simplification Rule}\} \\
 & (79 \bmod 7)^{62} \bmod 7 \\
= & \{79 \bmod 7 = 2\} \\
 & 2^{62} \bmod 7 \\
= & \{\text{rewrite } 2^{62}\} \\
 & ((2^6)^{10} \times 2^2) \bmod 7 \\
= & \{\text{use Modular Simplification Rule to convert } 2^6 \text{ to } 2^6 \bmod 7\} \\
 & ((2^6 \bmod 7)^{10} \times 2^2) \bmod 7 \\
= & \{7 \text{ is prime, and 2 and 7 are relatively prime;} \\
 & \quad \text{from Fermat's Theorem, } 2^6 \bmod 7 = 1\} \\
 & ((1)^{10} \times 2^2) \bmod 7 \\
= & \{\text{simplify}\} \\
 & 2^2 \bmod 7 \\
= & \{\text{simplify}\} \\
 & 4
\end{array}$$

   (c) Given that Alice's public key is the pair $(7, 155)$, we factor 155 to get 5×31. Then $\phi(155) = 4 \times 30 = 120$. We need to find d such that $7 \times d \overset{\text{mod } 120}{\equiv} 1$. Inspection with a few small values shows that $6 \times 120 + 1 = 721$, which is divisible by 7. That is, $7 \times 103 = 721$, or $7 \times 103 \overset{\text{mod } 120}{\equiv} 1$. So, $d = 103$.