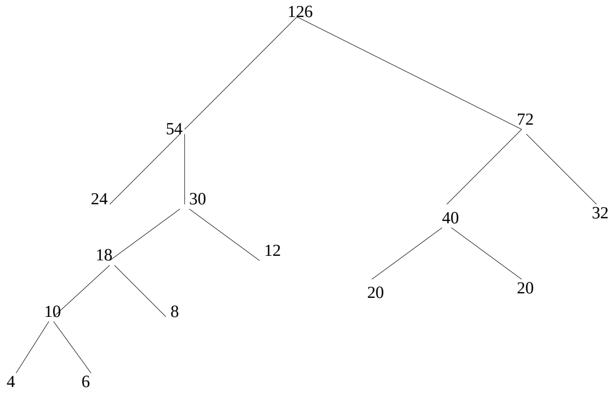
CS 337 **Solution to Test 1** **2/21/07**

1. (Compression)

   (a) A Huffman tree for symbols with the frequencies {12, 8, 20, 6, 32, 4, 20, 24} is shown below.



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

index	word	transmission
0	$\langle\rangle$	none
1	t	$(0, t)$
2	a	$(0, a)$
3	c	$(0, c)$
4	ca	$(3, a)$
5	ta	$(1, a)$
6	cc	$(3, c)$
7	ag	$(2, g)$
8	tac	$(5, c)$

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: *taccataccagtac*.

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

   (c) Suppose that the string *Ophelia* appears in a text, but the letter *O* appears nowhere else. The first occurrence of this word adds *O* as an entry in the trie, the next occurrence adds *Op* as an entry, etc. Since *Ophelia* has 7 letters, its 7^{th} occurrence will add the entire word to the trie.

index	word	transmission
9	agt	$(7, t)$
10	ac	$(2, c)$
11	cag	$(4, g)$
12	#	$(0, \#)$

Table 2: The transmissions corresponding to $agtaccag\#$

2. (Error Correction)

(a) To get the necessary and sufficient condition on x, y and z so that $((x + y) \oplus z) < z$, consider Exercise 6.3 in Section 2.1.2, Page 25, of the Notes. There we derive the condition for $(x \oplus u) < x$, which is: x has a 1 in the position where the leading 1 bit of u appears.

To match the given pattern, we rewrite the inequality as $(u \oplus x) < x$, and set u to $x + y$ and x to z to get $((x + y) \oplus z) < z$. Rewriting the condition: z has a 1 in the position where the leading 1 bit of $x + y$ appears.

(b) We prove that the number of 1s in H_n, the Hadamard matrix of size $2^n \times 2^n$, is $2^{n-1} \times (2^n + 1)$, by induction on n.

• $n = 0$: H_0 has one 1, and $2^{0-1} \times (2^0 + 1) = 1$.

• $n + 1$: We have to show that H_{n+1} has $2^n \times (2^{n+1} + 1)$ 1s. To compute the number of 1s in H_{n+1}, we have to know the number of zeroes in H_n, because $\overline{H_n}$ appears as a component. Since the total number of entries in H_n is $2^n \times 2^n$ and, inductively, $2^{n-1} \times (2^n + 1)$ are 1s, the number of zeroes is $2^n \times 2^n - 2^{n-1} \times (2^n + 1)$. Therefore, the number of 1s in H_{n+1} is:

$$\begin{aligned}
& 3 \times 2^{n-1} \times (2^n + 1) + 2^n \times 2^n - 2^{n-1} \times (2^n + 1) \\
=\ & 2 \times 2^{n-1} \times (2^n + 1) + 2^n \times 2^n \\
=\ & 2^n \times (2^n + 1) + 2^n \times 2^n \\
=\ & 2^n \times (2^n + 1 + 2^n) \\
=\ & 2^n \times (2^{n+1} + 1)
\end{aligned}$$

(c) The sender is transmitting 9-bit strings as 13-bit codes using Hamming code.

i. Hamming code can correct at least one error. From the Theorem of Page 39 in the notes, the distance between any two codewords exceeds 2 × 1; so, the distance is at least 3.

ii. Consider the string which has a 1 in its lowest bit. It will be encoded as the second row of Table 3. And the string which is all zero is coded as an all zero string, shown in the last row of Table 3. Their distance is exactly 3.

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

Table 3: Hamming code encoding of two strings

3. (Cryptography)

(a)

$$\begin{array}{ll}
 & 36^{36} \bmod 11 \\
= & \{\text{Modular Simplification Rule}\} \\
 & (36 \bmod 11)^{36} \bmod 11 \\
= & \{36 \bmod 11 = 3\} \\
 & 3^{36} \bmod 11 \\
= & \{\text{rewrite } 3^{36}\} \\
 & ((3^{10})^3 \times 3^6) \bmod 11 \\
= & \{\text{use Modular Simplification Rule to convert } 3^{10} \text{ to } 3^{10} \bmod 11\} \\
 & ((3^{10} \bmod 11)^3 \times 3^6) \bmod 11 \\
= & \{\text{11 is prime, and 3 and 11 are relatively prime;} \\
 & \quad \text{from Fermat's Theorem, } 3^{10} \bmod 11 = 1\} \\
 & ((1)^3 \times 3^6) \bmod 11 \\
= & \{\text{simplify}\} \\
 & 3^6 \bmod 11 \\
= & \{\text{simplify}\} \\
 & (3^3 \bmod 11)^2 \bmod 11 \\
= & \{\text{simplify}\} \\
 & 5^2 \bmod 11 \\
= & \{\text{compute}\} \\
 & 3
\end{array}$$

(b) Given that Bob's public key is the pair $(3, 355)$, we factor 355 to get 5×71. Then $\phi(355) = 4 \times 70 = 280$. We need to find d such that $3d \overset{\bmod 280}{\equiv} 1$. We can use extended Euclid's algorithm. But inspection with a few small values shows that $2 \times 280 + 1 = 561$, which is divisible by 3; i.e., $3 \times 187 = 561$. Therefore, $3 \times 187 \overset{\bmod 280}{\equiv} 1$, or $d = 187$.

(c) Using 1 for encryption is silly, the encrypted message is same as the original message, so it is same as sending the message in plaintext.

If $(1, n)$ is the private key, i.e., $d = 1$, then $e \overset{\bmod \phi(n)}{\equiv} 1$. So, $e = \phi(n) + 1$. We show that the encrypted message is same as the original message.

Let M be encrypted to M' and then decrypted to M''. We know $M = M''$. Now, $M'' = (M')^1 \bmod n = M'$. Therefore, $M' = M'' = M$.

If we are transmitting a text in English, the encrypted message is easily seen to be meaningful, and hence decrypted. However, if we are sending a string (without any apparent meaning), such as a password, no one will know that we are transmitting in plaintext. (yet, I would not recommend this transmision strategy; it is vulnerable if the eavesdropper merely attempts using the password).