

A file with 64 characters has the letters distributed as given in the table below.

A	B	C	D	E
24	18	12	2	8

a) Draw the Huffman tree associated to this file. What is the expected file length when this comma free code is used to encode the file?

b) Draw a tree from heights. Remove any branches that make the tree incomplete. What is the expected file length when this comma free code is used to encode the file?

c) What is the entropy of this file? What is the minimum number of binary registers needed to encode this file?

1. (a) Compute  $\gcd(119, 315)$ , the greatest common divisor of 119 and 315.

(b) Find  $r$  and  $s$  such that  $\gcd(119, 315) = 119r + 315s$ .

2. (a) Encode the message "SUN" one letter at a time, using the RSA system with  $m = 77$  and  $e = 7$ . In translating letters into numbers, send A to 10, B to 11, ..., Z to 35. Leave your answer as a sequence of numbers.

(b) Using the same system as part (a), decode the message "73", a single letter.

(3) In devising an RSA system you choose a public modulus  $m = 1081 = 23 \cdot 47$  and an encrypting exponent of 73. Find the decrypting exponent.

3. The RSA system is used with a public exponent of  $e=27$  and modulus  $m=1189=(29)(41)$ . Find the decrypting exponent.

(b) Compute  $13^{2409} \pmod{4819}$ . (Hint:  $13^{39} = 1 \pmod{4819}$ )

(1) Find  $\phi(206437)$  (note:  $206437 = 7^2 \cdot 11 \cdot 383$ ).

(2) Calculate

$$3^{160445} \pmod{206437}.$$

1. (a) Compute  $\gcd(741, 221)$ , the greatest common divisor of 741 and 221.

(b) Find  $r$  and  $s$  such that  $\gcd(741, 221) = 741r + 221s$ .

The following cyphertext was first encrypted with a 5 letter key and then a 3 letter key. The sender believed that this was equivalent to encrypting the text with a 15 letter key. Given that the 5-gram "ETPVI" represents the plaintext "rains" and the last three letters of the cyphertext "CJO" corresponds to the word "out," determine the plaintext.

JXZPE LCIXS PQHYM EFPVT JFUQB QPWXG

GLVWF VEYTO IJXBT ETPVI WRQXC JO