SKETCH OF SOLUTIONS (HOMEWORK X)

3.- DWWDF NDWGD ZQ

14.- E is mapped into J and E is mapped into O. $a = 9$ and $b = 25$ the message is: WE USE FREQUENCIES OF LETTERS TO DECRYPT SECRET MESSAGES

15.- $C \equiv 17(5P + 13) + 3 \equiv 85P + 224 \equiv 7P + 16 \mod 26$

Section 8.2

1.- VSPJXH HIPLKB KIPMIE GTG

3.- Look for repeated patterns of letters, the gcd of the lengths of the distances between patterns is likely to be the length of the cipher, or period (say it is k). Then perform the frequency-count analysis on characters which are at distance k from each other.

4.- The period is 3. The cipher is BOX. The plaintext is: TOBEO RNOTT OBETH ATIST HEQUE STION WHETH ERTIS NOBLE RINTH EMIND TOSUF FERTH ESLIN GSAND ARROW SOFOU TRAGE OUSFO RTUNE

13.- $C = AP \mod 26$ where

$$A = \begin{pmatrix} 11 & 6 \\ 2 & 13 \end{pmatrix}$$

18.- DQ BC IG KT AC EX

19.-

$$P \equiv \begin{pmatrix} 17 & 4 \\ 1 & 7 \end{pmatrix} C + \begin{pmatrix} 22 \\ 15 \end{pmatrix} \mod 26$$

Section 8.4

3.- Since a block of ciphertext p is less than n, we must have $(p, n) = p$ or $(p, n) = q$. Therefore the cryptanalyst has a factor of n

4.- The probability that it is divisible by p is $1/p$ and the probability that it is divisible by q is $1/q$. Also, since 0 is the only integer between 0 and $n - 1$ which is divisible by both p and q, the probability of being divisible by both of them is $1/pq$. Using the formula for the probability of the union we get $P(\gcd(P, n) > 1) = 1/p + 1/q - 1/pq$

6.- 101900141066218713492155

7.- GR EE TI NG SX

11.- Let P be the plaintext message and the two encrypting exponents e_1 and e_2. Let $a = (e_1, e_2)$. Then there exist integers x and y such that $e_1x + e_2y = a$. Let $C_1 \equiv P^{e_1} \mod n$ and $C_2 \equiv P^{e_2} \mod n$ be the two cipher texts. Since C_1, C_2, e_1 and e_2 are known, and since x and y can be computed, we can compute $C_1^x C_2^y \equiv P^{e_1 x} P^{e_2 y} \equiv P^{e_1 x + e_2 y} \equiv P^a \mod n$. Then computing the ath roots of P^a we recover P