PARCTICE FOR QUIZ 5 : MATH 4161

OPEN BOOK, OPEN NOTE, OPEN CALCULATOR, CLOSED FRIENDS, ENEMIES and INTERNET.

(1) In the following cryptogram, the Vernam system was used with key lengths 2 and 3. Say that we are told that the letter A occurs in the plaintext in the 3^{rd}, 12^{th}, 22^{nd}, 28^{th}, 36^{th} and 44^{th} position.

RUSJN XTDJP GEIAJ TUWTP OBTIG NGBRH XZYUH EIAXG IGXMD T

   (a) Find a key of length 2 and one of length 3 which are used to decrypt the cyphertext.
   (b) Two English words were used as the keys, what were they?

(2) The RSA system is used with $m = 127 \cdot 13 = 1651$ and an encrypting exponent of 275.
   (a) What is the decrypting exponent?
   (b) If the cyphertext message is 1389, then what is the plaintext message?

(3) The integer $1960200 = 11^2 \cdot 5^2 \cdot 2^3 \cdot 3^4$, find the value of the Euler-phi function $\phi(1960200)$. Use it to calculate

$$7^{475217} \ (mod\ 1960200)$$

(4) Calculate 17^{395} $(mod\ 787)$. Hint: $\left(\frac{17}{787}\right) = -1$.

(5) In the RSA system a three letter word is encoded by $A \to 0, B \to 1, C \to 2$, etc. and the message is the first letter plus 26 times the second letter plus 26^2 times the third letter. The message is encrypted with the public modulus of $m = 3953 = 59 \cdot 67$ and an encypting exponent of 17. The cyphertext in this case is 3319.
   (a) Find the decrypting key
   (b) Find the message given the following powers of the cyphertext and convert that message back into a three letter word (hint: it is a product of two values in the table below)

n	5	13	388	463	644	2014	3131
3319^n $(mod\ 3953)$	753	2057	1701	3721	2150	1644	2364

(6) Say that I calculate

$$345^{213288251} \equiv 401646933 \ (mod\ 426576503)\ .$$

What does this calculation say about the primality of any of the integers in the equation?

(7) Find the Jacobi symbol $J(7, 938457394589)$. Hint: 938457394589 is equivalent to 1 (mod 4) and 1 (mod 7).

(8) Find the solution to the equation

$$2477x \equiv 101 \ (mod\ 3828)$$

(9) Calculate

$$27^{1277} \ (mod\ 3953)$$