# Number Theory
# Problem Set 6
# RSA Protocol, A Public Key Cryptosystem

1. Suppose that the following 40-letter alphabet is used for all plaintexts and ciphertexts: A-Z with numerical equivalents 0-25, blank=26, .=27, ?=28, $=29, the numerals 0-9 with numerical equivalents 30-39. Suppose that plaintext message units are digraphs and ciphertext message units are trigraphs.

   (a) Send the message "SEND $7500" to a user whose encryption key $(E, n) = (179, 2047)$.

   (b) Break the code by factoring $n$ and then compute the decryption key $(D, n)$.

2. Try to break the code who encryption key is $(E, n) = (3602561, 536813567)$. Factor $n$ by the dumbiest known algorithm i.e. dividing by all odd numbers $3, 5, 7, \cdots$. After factoring $n$, find the decryption key. Then decipher the message BNBPPKZAVQZLBJ, under the assumption that the paintext consists of 6-letter blocks in the usual 26-letter alphabet and the ciphertext consists of 7-letter blocks in the same alphabet.

3. Suppose that both plaintexts and ciphertexts consist of trigraph message units, but while plaintexts are written in the 27-letter alphabet (consisting of A-Z and blank=26), ciphertexts are writen in the 28-letter alphabet obtained by adding the symbol "/" (with numerical equivalent 27) to the 27-letter alphabet. We require that each user chooses $n$ $n$ between $27^3 = 19683$ and $28^3 = 21952$, so that a plaintext trigraph in the 27-letter alphabet corresponds to a residue $P$ modulo $n$, and then $C \equiv P^E \mod n$ corresponds to a ciphertext trigraph in the 28-letter alphabet.

(a) Id your decryption key is $(D, n) = (20787, 21583)$, decipher the message "YSNAUOZHXXH " (one blank at the end).

(b) If in part (a), you know that $\phi(n) = 21280$, find

i. $E \equiv D^{-1} \mod \phi(n)$,

ii. the factorization of $n$.