

Mathematics of Coding and Cryptography
Worksheet 9

1. Suppose you know $n = pq = 1,219,326,314,583,142,793$ for primes p and q , and $\phi(n) = 1,219,326,312,360,920,580$. Find p and q using the method we discussed in class.
2. Compute the first 8 continued fraction approximations to

$$\frac{1 + \sqrt{5}}{2}.$$

3.
 - (a) Find two 5 digit primes p and q .
 - (b) Find an integer e with at least 3 digits such that $\gcd(e, \phi(p, q)) = 1$.
 - (c) Exchange $n = pq$ and e with another group.
 - (d) Using their key (their choices of n and e) encrypt a 4 letter word using the RSA algorithm.
 - (e) Exchange encrypted messages with the other group.
 - (f) Decrypt the message they encrypted for you.