1 RSA Warm-Up

Consider an RSA scheme with modulus N = pq, where p and q are distinct prime numbers larger than 3.

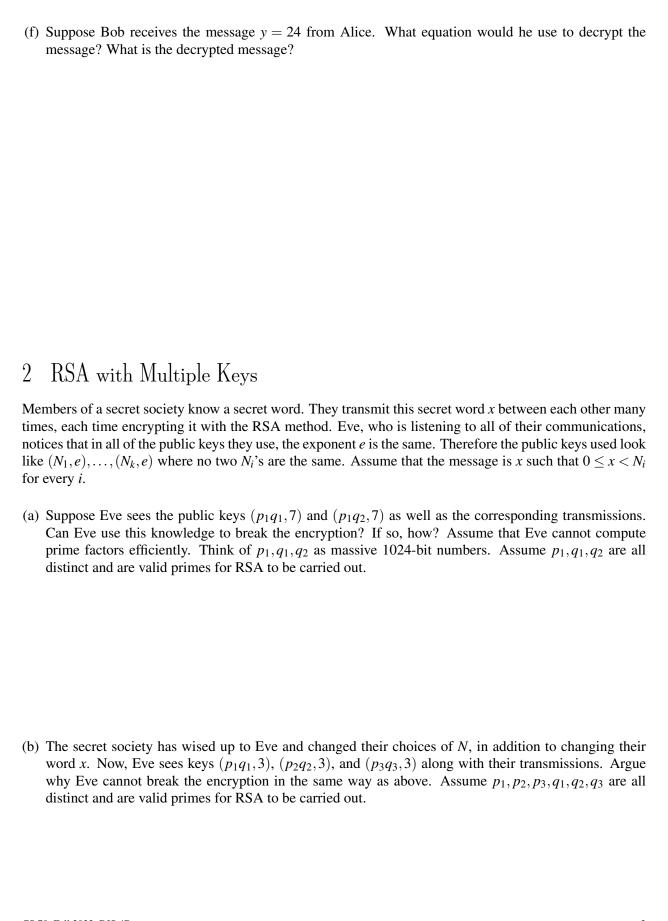
(a) What is wrong with using the exponent e = 2 in an RSA public key?

(b) Recall that e must be relatively prime to p-1 and q-1. Find a condition on p and q such that e=3 is a valid exponent.

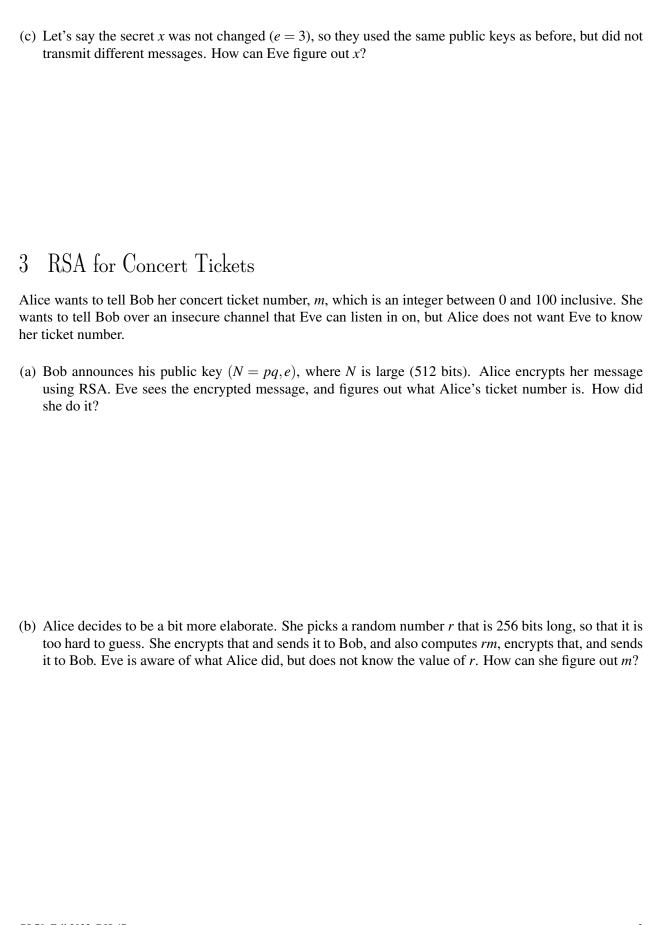
(c) Now suppose that p = 5, q = 17, and e = 3. What is the public key?

(d) What is the private key?

(e) Alice wants to send a message x = 10 to Bob. What is the encrypted message E(x) she sends using the public key?



CS 70, Fall 2022, DIS 4B 2



CS 70, Fall 2022, DIS 4B 3