CS 70 Discrete Mathematics and Probability Theory Spring 2022 Koushik Sen and Satish Rao

DIS 4A

1 RSA Warm-Up

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

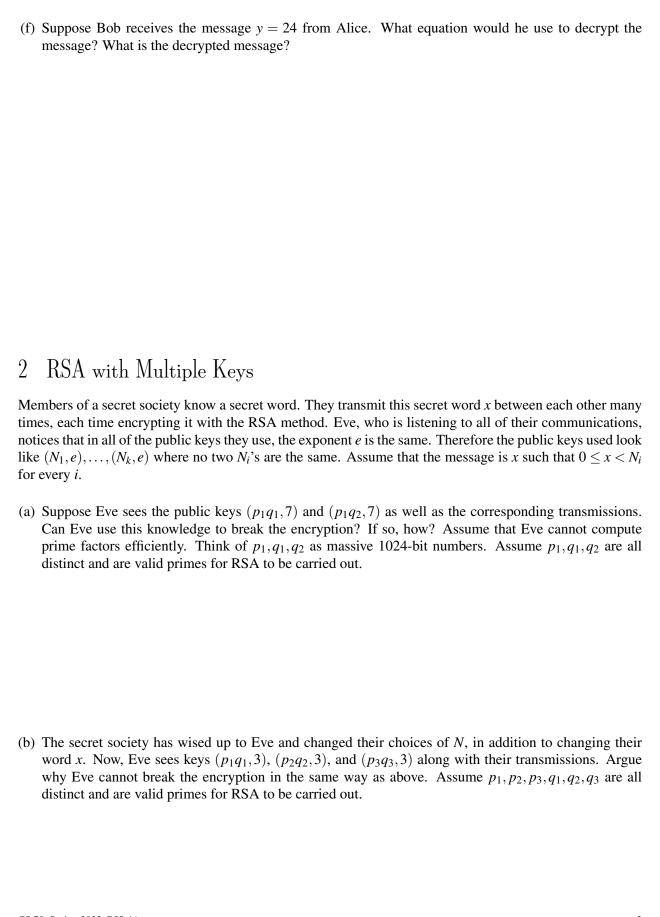
(a) What is wrong with using the exponent e = 2 in an RSA public key?

(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, Spring 2022, DIS 4A 2

(c)	Let's say the secret x was not changed ($e = 3$), so they used the same public keys as before, but did not transmit different messages. How can Eve figure out x ?
}	RSA for Concert Tickets
vai	ce wants to tell Bob her concert ticket number, m , which is an integer between 0 and 100 inclusive. She its to tell Bob over an insecure channel that Eve can listen in on, but Alice does not want Eve to know ticket number.
a)	Bob announces his public key $(N = pq, e)$, where N is large (512 bits). Alice encrypts her message using RSA. Eve sees the encrypted message, and figures out what Alice's ticket number is. How did she do it?
b)	Alice decides to be a bit more elaborate. She picks a random number r that is 256 bits long, so that it is too hard to guess. She encrypts that and sends it to Bob, and also computes rm , encrypts that, and sends it to Bob. Eve is aware of what Alice did, but does not know the value of r . How can she figure out m ?

CS 70, Spring 2022, DIS 4A 3