

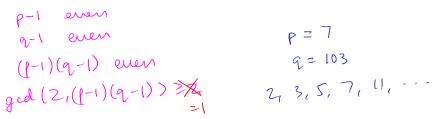
CS 70 Fall 2021 Discrete Mathematics and Probability Theory

DIS 4B

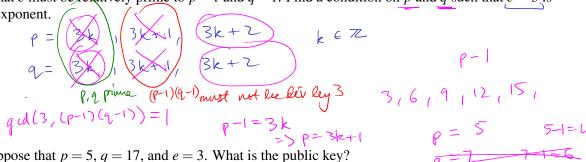
RSA Warm-Up

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?

$$(N, e)$$

 $(\pi \times 5, 3) = (85, 3)$

(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?

$$10^3 = 100 \times 10 = 15 \times 10 = 65 \pmod{85}$$

(f) Suppose Bob receives the message y = 24 from Alice. What equation would he use to decrypt the message? What is the decrypted message?

$$2u^{3} = \chi \equiv a \pmod{p} \qquad p_{1}q \pmod{p}$$

$$2u^{13} = \chi \equiv b \pmod{q}$$

$$\chi \equiv 2u^{13} \equiv (-1)^{13} \equiv -1 \equiv 4 \pmod{5}$$

$$\chi \equiv 2u^{13} \equiv 1^{13} \equiv (-2)^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 2u^{13} \equiv 1^{13} \equiv (-2)^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 2u^{13} \equiv 1^{13} \equiv (-2)^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 2u^{13} \equiv 1^{13} \equiv (-2)^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 2u^{13} \equiv 1^{13} \equiv (-2)^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4 \cdot 4^{2} + 1u \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4 \cdot 4^{2} + 1u \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4 \cdot 4^{2} + 1u \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4 \cdot 4^{2} + 1u \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4 \cdot 4^{2} + 1u \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4 \cdot 4^{2} + 1u \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4 \cdot 4^{2} \cdot 7 \pmod{17}$$

$$\chi \equiv 4^{2} \cdot 7 \pmod{17}$$

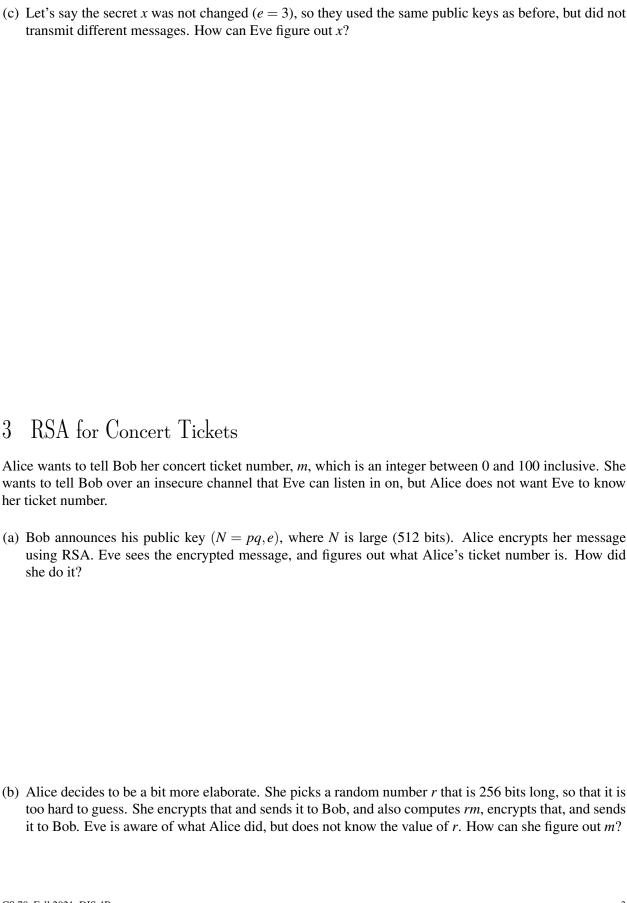
2 RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_k, e)$ where no two N_i 's are the same. Assume that the message is x such that $0 \le x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(p_1q_1,7)$ and $(p_1q_2,7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve cannot compute prime factors efficiently. Think of p_1,q_1,q_2 as massive 1024-bit numbers. Assume p_1,q_1,q_2 are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(p_1q_1,3)$, $(p_2q_2,3)$, and $(p_3q_3,3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

CS 70, Fall 2021, DIS 4B



CS 70, Fall 2021, DIS 4B 3