

## 1 Simplifying Some “Little” Exponents

For the following problems, you must both calculate the answers and show your work.

- (a) What is  $7^{3,000,000,000} \pmod{41}$ ?
- (b) What is  $2^{2017} \pmod{11}$ ?
- (c) What is  $2^{(5^{2017})} \pmod{11}$ ?

## 2 RSA Warm-Up

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

- (a) 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.
- (b) Now suppose that  $p = 5$ ,  $q = 17$ , and  $e = 3$ . What is the public key?
- (c) What is the private key?
- (d) Alice wants to send a message  $x = 10$  to Bob. What is the encrypted message she sends using the public key?
- (e) Suppose Bob receives the message  $y = 24$  from Alice. What equation would he use to decrypt the message?

## 3 RSA Short

Background: Alice wants a signature of  $x$  from Bob but doesn't want Bob to know  $x$ .

Let  $(N, e)$  be Bob's public key, and  $d$  be his decryption key. Alice chooses a random  $r$  that is relatively prime to  $N$ , and sends Bob  $r^e x \pmod{N}$  to sign, and Bob returns  $m = (r^e x)^d \pmod{N}$  to Alice.

Give an expression that yields Bob's signature of  $x$ :  $x^d \pmod{N}$ . Your expression may use the variables  $m$ ,  $x$ ,  $r$ ,  $N$  and  $e$ .

## 4 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  $(e, N_1), \dots, (e, N_k)$  where no two  $N_i$ 's are the same. Assume that the message is  $x$  such that  $0 \leq x < N_i$  for every  $i$ .

- (a) Suppose Eve sees the public keys  $(7, 35)$  and  $(7, 77)$  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.
- (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  $(3, 5 \times 23)$ ,  $(3, 11 \times 17)$ , and  $(3, 29 \times 41)$  along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.