Broc Nickodemus

HW 8

R7 and R8 on page 744

R7. Suppose n = 10,000, a = 10,023, and b = 10,004. Use an identity of modular

arithmetic to calculate in your head (a • b) mod n .

((10,023 mod 10000) x (10,004 mod 10,000)) mod 10,000

= (23 \* 4) mod 10000

= 92 mod 10000

= 92

R8. Suppose you want to encrypt the message 10101111 by encrypting the decimal number that corresponds to the message. What is the decimal number?

(section 8.3)

1+2+4+8+32+128

10101111 = 175

P1. Using the monoalphabetic cipher in Figure 8.3, encode the message “This is an easy problem.” Decode the message “rmij’u uamu xyj.”

di XOR ci = ki4

“rmij’u uamu xyj.” 🡺 wasn’t that fun

P3. Consider the polyalphabetic system shown in Figure 8.4. Will a chosen plain text attack that is able to get the plaintext encoding of the message “The quick brown fox jumps over the lazy dog.” be sufficient to decode all messages? Why or why not?

Yes, assuming that there is no punctuation, “The quick brown fox jumps over the lazy dog.” contains every letter of the alphabet and is therefore sufficient to decode all messages.