

**Math 55 — Discrete Mathematics — Spring 2003**

Quiz 4 Solutions

Version 1

(a) For the RSA cryptography system with public key  $n = 13 \cdot 17 = 221$ ,  $e = 77$  and encryption function  $E(x) = x^e \pmod{n}$ , find the private key  $d$  such that  $D(x) = x^d \pmod{n}$  is the decryption function.

(b) Decrypt to find the original message if the encrypted message is 007.

Version 2

(a) For the RSA cryptography system with public key  $n = 11 \cdot 13 = 143$ ,  $e = 37$  and encryption function  $E(x) = x^e \pmod{n}$ , find the private key  $d$  such that  $D(x) = x^d \pmod{n}$  is the decryption function.

(b) Decrypt to find the original message if the encrypted message is 002.

Solution

(a) We compute  $d$  as the inverse of  $e \pmod{(p-1)(q-1)}$ . In Version 1,  $d = 77^{-1} \pmod{192}$ . Using the Euclidean algorithm on 192 and 77 and back-substituting gives  $1 = 5 \cdot 77 - 2 \cdot 192$ , so  $d = 5$ .

In Version 2,  $d = 37^{-1} \pmod{120}$  and the calculation gives  $1 = 13 \cdot 37 - 4 \cdot 120$ , so  $d = 13$ .

(b) In Version 1, we must compute  $7^5 \pmod{221}$ . By repeated squaring we find  $7^1 \equiv 7$ ,  $7^2 \equiv 49$ ,  $7^4 \equiv 2401 \equiv 191$ . Then  $7^5 \equiv 7^4 \cdot 7 \equiv 1337 \equiv 11$ .

In Version 2, we must compute  $2^{13} \pmod{143}$ . By repeated squaring we find  $2^1 \equiv 2$ ,  $2^2 \equiv 4$ ,  $2^4 \equiv 16$ ,  $2^8 \equiv 256 \equiv 113$ . Then  $2^{13} \equiv 2^8 \cdot 2^4 \cdot 2^1 \equiv 113 \cdot 32 \equiv 3616 \equiv 41$ .