



Figure 9.6 Example of RSA Algorithm

4. Select  $e$  such that  $e$  is relatively prime to  $\phi(n) = 160$  and less than  $\phi(n)$ ; we choose  $e = 7$ .
5. Determine  $d$  such that  $de \equiv 1 \pmod{160}$  and  $d < 160$ . The correct value is  $d = 23$ , because  $23 \times 7 = 161 = 10 \times 160 + 1$ ;  $d$  can be calculated using the extended Euclid's algorithm (Chapter 4).

The resulting keys are public key  $KU = \{7, 187\}$  and private key  $KR = \{23, 187\}$ . The example shows the use of these keys for a plaintext input of  $M = 88$ . For encryption, we need to calculate  $C = 88^7 \bmod 187$ . Exploiting the properties of modular arithmetic, we can do this as follows:

$$\begin{aligned}
 88^7 \bmod 187 &= [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187 \\
 88^1 \bmod 187 &= 88 \\
 88^2 \bmod 187 &= 7744 \bmod 187 = 77 \\
 88^4 \bmod 187 &= 59,969,536 \bmod 187 = 132 \\
 88^7 \bmod 187 &= (88 \times 77 \times 132) \bmod 187 = 894,432 \bmod 187 = 11
 \end{aligned}$$

For decryption, we calculate  $M = 11^{23} \bmod 187$ :

$$\begin{aligned}
 11^{23} \bmod 187 &= [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times \\
 &\quad (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187 \\
 11^1 \bmod 187 &= 11 \\
 11^2 \bmod 187 &= 121 \\
 11^4 \bmod 187 &= 14,641 \bmod 187 = 55 \\
 11^8 \bmod 187 &= 214,358,881 \bmod 187 = 33 \\
 11^{23} \bmod 187 &= (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = \\
 &\quad 79,720,245 \bmod 187 = 88
 \end{aligned}$$

### Computational Aspects

We now turn to the issue of the complexity of the computation required to use RSA. There are actually two issues to consider: key generation and encryption/decryption. Let us look first at the process of encryption and decryption and then return to the issue of key generation.