2 RSA Practice

(a) 77

By the definition of RSA, since $p = 7, q = 11$, so $N = pq = 7 \cdot 11 = 77$.

(b) 60

By the definition of RSA, e is relatively prime to $(p-1)(q-1)$. Since $p = 7, q = 11$, so e is relatively prime to $(7-1)(11-1) = 6 \cdot 10 = 60$

(c) 7

Consider the list of primes from the smallest, which is the sequence $2, 3, 5, 7, \cdots$. Now, since e needs to be relatively prime to $60 = 2^2 \cdot 3 \cdot 5$, so none of $2, 3, 5$ is relatively prime to 60, and with 7 being relatively prime to 60, so the smallest possible prime is $e = 7$.

(d) 1

Since by definition of RSA, e and $(p-1)(q-1)$ are relatively prime, so it's equivalent to that $\gcd(e, (p-1)(q-1)) = 1$.

(e) 43

Since we have $7 \cdot 17 = 119 = 120 - 1 = 60 \cdot 2 - 1$, so $7 \cdot 17 \equiv -1 \pmod{60}$. With $7 \cdot 60 \equiv 0 \pmod{60}$, so we have $7 \cdot 43 = 7 \cdot 60 - 7 \cdot 17 \equiv 0 - (-1) \equiv 1 \pmod{60}$, which means that $7^{-1} \equiv 43 \pmod{60}$. By definition of RSA, d is the inverse of $e \bmod (p-1)(q-1)$, so $d = 43$.

(f) 2

By definition of RSA, when Alice wants to send Bob the message 30, where we have $e = 7, N = 77$ from parts (a) and (c), then she computes and sends $E(30) = 30^7 \bmod 77$. Now, since:

$30^1 \equiv 30 \pmod{77}$,

$30^2 = 900 = 77 \cdot 12 - 24 \equiv -24 \pmod{77}$,

$30^4 \equiv (-24)^2 = 576 = 77 \cdot 7 + 37 \equiv 37 \pmod{77}$,

so we have that $30^7 = 30 \cdot 30^2 \cdot 30^4 \equiv 30 \cdot (-24) \cdot 37 = (-720) \cdot 37 = (77 \cdot (-11) + 50) \cdot 37 \equiv 50 \cdot 37 = 1850 = 77 \cdot 24 + 2 \equiv 2 \pmod{77}$, which means that Alice would send 2.

(g) 30.

By definition of RSA, the message Bob recover from the encrypted message should be exactly the same as the original message of Alice, 30. I'll show below that this works as intended.

If $y = 2$ is the message Bob received, and with the $d = 43$ calculated in part (e) and $N = 77$, then by applying $D(y) = y^d = 2^{43} \bmod 77$, he could recover the original message ($x = 30$). Now, since:

$2^1 \equiv 2 \pmod{77}$, $2^2 = 4 \equiv 4 \pmod{77}$, $2^4 = 16 \equiv 16 \pmod{77}$,

$2^8 \equiv 16^2 = 256 = 77 \cdot 3 + 25 \equiv 25 \pmod{77}$,

$2^16 \equiv 25^2 = 625 = 77 \cdot 8 + 9 \equiv 9 \pmod{77}$,

$2^32 \equiv 9^2 = 81 = 77 + 4 \equiv 4 \pmod{77}$,

so we have that $2^{43} = 2^{32+8+2+1} = 2^{32} \cdot 2^8 \cdot 2^2 \cdot 2^1 \equiv 4 \cdot 25 \cdot 4 \cdot 2 = 800 = 77 \cdot 10 + 30 \equiv 30 \pmod{77}$.

Thus, with $y = 2$, then $D(y) = 30 = x$, as desired.