1 Quick Computes

(a) 5

Since 11 is a prime and $1 \leq 3 \leq 11-1=10$, which means that $3 \in \{1,2,...,11-1\}$, so using Fermat's Little Theorem, we have that $3^10 \equiv 1 \pmod{11}$.

Thus, $3^{33} = 3^{10\cdot 3+3} = (3^{10})^3 \cdot 3^3 \equiv 1^3 \cdot 27 = 27 \equiv 5 \pmod{11}$

(b) 5

Since $10001 = 17 \cdot 588 + 5$, so $10001^{10001} \equiv 5^{10001} \pmod{17}$. Again, since 17 is prime and $5 \in \{1,2,...,17-1\}$, so using Fermat's Little Theorem, we have that $5^16 \equiv 1 \pmod{17}$.

Thus, $10001^{10001} \equiv 5^{10001} \pmod{17} = 5^{16\cdot 625+1} = (5^{16})^{625} \cdot 5^1 \equiv 1^{625} \cdot 5 \equiv 5 \pmod{17}$

(c) 1

Since $10 = 7\cdot 1+3, 20 = 7\cdot 2+6, 30 = 7\cdot 4+2, 40 = 7\cdot 5+5$, so $10^{10}+20^{20}+30^{30}+40^{40} \equiv 3^{10}+6^{20}+2^{30}+5^{40} \pmod{7}$

Then again, since 7 is prime and $3,6,2,5 \in \{1,2,...,7-1\}$, so using Fermat's Little Theorem, we have that $3^6 \equiv 6^6 \equiv 2^6 \equiv 5^6 \equiv 1 \pmod{7}$

Thus, $10^{10} + 20^{20} + 30^{30} + 40^{40} \equiv 3^{10} + 6^{20} + 2^{30} + 5^{40} \equiv 3^6 \cdot 3^4 + (6^6)^3 \cdot 6^2 + (2^6)^5 + (5^6)^6 \cdot 5^4 \equiv 1 \cdot 81 + 1^3 \cdot 36 + 1^5 + 1^6 \cdot 625 = 81 + 36 + 1 + 625 = 743 = 7 \cdot 106 + 1 \cdot 1 \pmod{7}$

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 mod $(p-1)(q-1)$, 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.

3 Squared RSA

(a) Direct Proof

Proof. We proceed by a direct proof. Given that p is prime and a, p is coprime, let $a = kp + r$ where $k \in \mathbb{Z}, 1 < r < p$ since $r \neq 0$, so $r \in \{1, 2, ..., p-1\}$ and that $a \equiv r \pmod{p}$. Thus, using Fermat's Little Theorem, we have that $a^{p-1} \equiv r^{p-1} \equiv 1 \pmod{p}$, and so $a^p \equiv 1 \cdot p \equiv p \pmod{p}$.

Let A denote the set of non-zero integers mod p^2, i.e. $A = \{0, 1, 2, ..., p^2 - 1\}$. Let S be the subset of A where we exclude the multiples of p, i.e. $0, p, 2p, 3p, ..., (p-1)p$. There are $p-1$ such multiples of p, so S has $p^2 - p = p(p-1)$ elements, and contains all the elements from 0 to $p^2 - 1$ that are not multiples of p, i.e. $S = \big\{kp + r \mid k \in \{0, 1, 2, ..., p-1\}, r \in \{1, 2, ..., p-1\}\big\}$.

Consider the sequence of numbers as we multiply each element of S by a, given that a, p are coprime, which represents $S^* = \big\{a(kp+r) \mid k \in \{0, 1, 2, ..., p-1\}, r \in \{1, 2, ..., p-1\}\big\}$. We claim that these are all distinct modulo p^2.

First, we provide the proof for a smaller claim, that none of these numbers could be a multiple of p. Since $\forall k, r \leq p-1, k \in \mathbb{N}, r \in \mathbb{Z}^+$, we have that $a(kp+r) = akp + ar \equiv ar \pmod{p}$. Since p is prime and that $\gcd(p, a) = 1$, $\gcd(p, r) = 1$, so we have $\gcd(p, ar) = 1$, which gives us that $a(kp+r) \equiv ar \not\equiv 0 \pmod{p}$. Therefore, for any $e \in S^*$, then $p \nmid e$. Moreover, let $e \equiv x \pmod{p^2}$, so $e = qp^2 + x, q \in \mathbb{Z}$. If $p \mid x$, then with the fact that $qp^2 = (qp)p, qp \in \mathbb{Z}$, so $p \mid (qp^2)$, and so $p \mid (qp^2 + x) = e$, which gives the contradiction. Thus, $p \nmid x$.

Thus, $\forall e \in S^*$, let $e \equiv x \pmod{p^2}$, then $p \nmid x$. So, there are $p^2 - p$ possible remainders modulo p^2 (just as how I proved the number of elements in S). Now, we claim that for all elements in S^*, they are distinct modulo p^2.

Assume for a contradiction that $\exists e_1, e_2 \in S^*, e_1 \neq e_2$, and $e_1 \equiv e_2 \pmod{p^2}$. So, $p^2 \mid (e_1 - e_2)$. Let $e_1 = a(k_1 p + r_1), e_2 = a(k_2 p + r_2)$ where $k_1, k_2, r_1, r_2 \leq p-1, k_1, k_2 \in \mathbb{N}, r_1, r_2 \in \mathbb{Z}^+$, and let $e_1 - e_2 = k_p p^2, k_p \in \mathbb{Z}$. So $e_1 - e_2 = a(k_1 p + r_1) - a(k_2 p + r_2) = a(k_1 - k_2)p + a(r_1 - r_2)$ Since $p^2 \mid (e_1 - e_2)$, so $p \mid (e_1 - e_2)$, and since $a, k_1, k_2 \in \mathbb{Z}$, so $a(k_1 - k_2) \in \mathbb{Z}$, so $p \mid a(k_1 - k_2)p$, so $p \mid a(r_1 - r_2)$, since $\gcd(p, a) = 1$, so $p \nmid a$, and with p being prime, so $p \mid (r_1 - r_2)$. If $r_1 \neq r_2$, then $0 < |r_1 - r_2| < p - 2$, which means that $p \nmid (r_1 - r_2)$, implying contradiction, so $r_1 = r_2$.

Then, since $e_1 \neq e_2$, so $k_1 \neq k_2$. With a similar argument as above, so $p \nmid (k_1 - k_2)$, and let R be this assertion. However, with $r_1 = r_2$, so $a(r_1 - r_2) = 0$, so $k_p p^2 = e_1 - e_2 = a(k_1 - k_2)p$. Since $p \neq 0$, divide both sides by p and we have $k_p p = a(k_1 - k_2)$, so $p \mid a(k_1 - k_2)$. Again, since $\gcd(p, a) = 1$, so $p \nmid a$, and since p is prime, so $p \mid (k_1 - k_2)$, which implies $\neg R$. So, $R \wedge \neg R$ holds, reaching a contradiction, so for all elements in S^*, they are distinct modulo p^2.

Thus, the set of numbers $S' = S^* \bmod p^2 = \big\{a(kp+r) \bmod p^2 \mid k \in \{0, 1, 2, ..., p-1\}, r \in \{1, 2, ..., p-1\}\big\}$ includes every element of S exactly once, so it shuold be exactly the same as S, with possibly different order.

Now, first take the product of all elements of S, mod p^2, would give us:

$$1 \cdot 2 \cdots (p-1) \cdot (p+1) \cdots (2p-1) \cdot (2p+1) \cdot \cdots \cdot (p^2 - 1) = \prod_{e \in S} e \pmod{p^2}.$$

On the other hand, take the product of all elements of S', mod p^2, would give us:

$$\begin{aligned} a \cdot 2a \cdots (p-1)a \cdot (p+1)a \cdots (2p-1)a \cdot (2p+1)a \cdot \cdots \cdot (p^2-1)a &= \prod_{e \in S} ea = a^{|S|} \cdot \prod_{e \in S} e \\ &= a^{p(p-1)} \cdot \prod_{e \in S} e \pmod{p^2}. \end{aligned}$$

Thus, we have:

$$\prod_{e \in S} e \equiv a^{p(p-1)} \cdot \prod_{e \in S} e \pmod{p^2}.$$

Then, since every element of S is coprime with p^2, so they would each have an inverse mod p^2, and thus, $\prod_{e \in S} e$ would have an inverse mod p^2. Therefore, multiplying both sides of the above equation by the inverse of $\prod_{e \in S} e \pmod{p^2}$, we have that $a^{p(p-1)} \equiv 1 \pmod{p^2}$, as desired.

Q.E.D.

(b) Direct Proof

Proof. We proceed by a direct proof.

Consider the new RSA scheme where the public key is $(N = p^2q^2, e)$ with e being relatively prime to $p(p-1)q(q-1)$, and the private key being $d = e^{-1} \pmod{p(p-1)q(q-1)}$. Also, we have our message x being relatively prime to both p and q, i.e. $x^{ed} \equiv x \pmod N$. To prove that the scheme is correct, We have to show that $D(E(x)) \equiv x \pmod N$ for every possible message $x \in \{0, 1, ..., N-1\}$.

By definition of RSA, since we didn't change the definition of encyprtion/decryption functions, so the encrypted message $y = E(x) \equiv x^e \pmod N$, so $D(y) = D(E(x)) \equiv (x^e)^d \equiv x^{ed} \pmod N$. Then, since we are given that x is relatively prime to both p and q, i.e. $x^{ed} \equiv x \pmod N$, so $D(E(x)) \equiv x^{ed} \equiv x \pmod N$, as desired.

Thus, the new scheme is correct $\forall x$ relatively prime to both p and q.

Q.E.D.

(c) Direct Proof

Proof. We proceed by a direct proof. Suppose that we can break the new squared RSA scheme, i.e. if given p^2q^2, then we can deduce $p(p-1)q(q-1)$.

Then, if we're given pq, by squaring it, we can calculate $(pq)^2 = p^2q^2$. Now, we know that given p^2q^2, we can deduce $p(p-1)q(q-1)$. Since $p(p-1)q(q-1) = (pq)(p-1)(q-1)$, so dividing $p(p-1)q(q-1)$ by pq would give us $(p-1)(q-1)$. Since the information pq is given to us, so we can deduce $(p-1)(q-1)$ in this situation.

Thus, if the new scheme, squared RSA, can be broken (i.e. if given p^2q^2, then we can deduce $p(p-1)q(q-1)$), then if we're given pq, we can also deduce $(p-1)(q-1)$, which implies that the normal RSA would also be broken, as desired.

Q.E.D.