RSA
Solutions.

Problem 1 [DPV] 1.11

We can use Euler's Theorem. Notice that $35 = 5 \times 7$ hence $\phi(35) = 24$. Since $g.c.d.(4, 35) = g.c.d.(9, 35) = 1$ we have that $4^{24k} \equiv 9^{24t} \equiv 1(mod\ 35)$ for all natural numbers k, t. From this observation we have:

$$4^{1536} = 4^{24\times 64} \equiv 1 \equiv 9^{24\times 201}(mod\ 35)$$

so we conclude the given difference is divisible by 35.

Problem 2 [DPV] 1.12

By Fermat's theorem $2^{2k} \equiv 1(mod\ 3)$ for any natural number k, hence the given power is also congruent to 1, since the exponent is even.

Problem 3 [DPV] 1.13

Apply Fermat's theorem dividing first each exponent by $30 = 31 - 1$. For the second, you need to compute $6^6(mod\ 31)$ which is equal to 1. Answer: YES.

Problem 4 [DPV] 1.14

There are many ways to do this problem, since it asks for an efficient solution only. If you want to use problem 0.4: it shows how to get the n^{th} Fibonacci term in time $O(\log(n))M(n)$ where $M(n)$ is the running time of your favorite multiplication algorithm. Since we are computing $(modp)$ on each step we can reduce numbers $(mod\ p)$ leading to a running time of $O(\log(n)M(\log(p)))$.

Problem 5 [DPV] 1.18

Just a simple practice problem. Any calculator will tell you that $210 = 2 \times 3 \times 5 \times 7$ and $588 = 2^2 \times 3 \times 7^2$. Euclid's Algorithm will gives you

$$g.c.d.(588, 210) = g.c.d.(210, 168) = g.c.d.(168, 42) = g.c.d.(42, 0) = 42$$

.

Problem 6 [DPV] 1.20

Solutions:
$20^{-1}(mod\ 79) = 4$
$3^{-1}(mod\ 62) = 21$.
$21^{-1}(mod\ 91) = DNE$ because the two share a divisor bigger than one.
$5^{-1}(mod\ 23) = 14$

Problem 7 [DPV] 1.22

a has an inverse $(mod\ b)$ if and only if $g.c.d.(a, b) = 1 = g.c.d.(b, a)$ if and only if b has an inverse $(mod\ a)$.

Problem 8 [DPV] 1.24

This problem asks to compute $\phi(p^n)$ for p prime and n a natural number. Note that only those numbers divisible by p share a factor with p^n. There are $p^n/p = p^{n-1}$ multiples of p in the set $\{1, 2, \ldots, p^n\}$ so e conclude that

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1).$$

Problem 9 [DPV] 1.25

Since 127 is prime we know that $2^{125} \times 2 = 2^{126} \equiv 1(mod\ 127)$, hence we are looking for the inverse of 2 $(mod\ 127)$! This is an easy task since $127 + 1 = 2 \times 64$.

Problem 10 [DPV] 1.26

Because the last digit is the reminder in the division by 10, we need to compute $17^{17^{17}}$ $(mod\ 10)$. To apply the hint, we need to find 17^{17} $(mod 4)$ (here $4 = (5-1)(2-1)$ from $10 = 5 \times 2$). Since $17 \equiv 1$ $(mod\ 4)$ then also $17^{17} \equiv 1$ $(mod\ 4)$. This means we can write $17^{17} = 4q + 1$ for a natural number q and then

$$17^{17^{17}} = 17^{4q+1} = 17 \times 17^{4q} \equiv 7 \times 1 = 7\ (mod\ 10).$$

The last relation uses that $17^{4q} \equiv (17^4)^q \equiv 1^q \equiv 1$ $(mod\ 10)$. Answer: 7.

Problem 11 [DPV] 1.27

Recall that d is the inverse of e $(mod\ (p-1)(q-1))$ for $N = pq$. In this case $N = 391 = 17 \times 23$ and $e = 3$. The inverse of 3 $(mod\ 352)$ is $d = 235$. For message 41, the encryption is 41^3 $(mod\ 391)$ which is 105.

Problem 12 [DPV] 1.28

In other words: find integers d and e such that $de \equiv 1 (mod\ 60)$. We cannot use $e = 3$ or $e = 5$ but $e = 7, 11, 13$ will do it. The values of d are $43, 11, 37$ respectively.

Problem 13 [DPV] 1.42

To decrypt, we need a number d such that $m^{ed} \equiv m (mod\ p)$. By Fermat's theorem we know it is enough to find an inverse of e $(mod\ p-1)$, which we can find efficiently using Euclid's Algorithms, for example.