$\boxed{\text{PSet 7 Solutions}}$

1 a) 10^{10} computers $\times 10^{9} \frac{\text{divisors}}{\text{sec}\cdot\text{computer}} \times 10^{18}$ seconds $= 10^{37}$ divisors.

So Eve could factor a number as large as $(10^{37}) = \underline{10^{74}}$ this way.

Note that $\log_2(10^{74}) \approx 246$, so this could attack a 246-bit modulus.

b) $2^{1024} \approx 10^{308}$ $(\log_{10} 2^{1024} \approx 308.2)$, so Eve's attack is too slow by a factor of $\frac{\sqrt{10^{308}}}{10^{37}} = 10^{117}$ or so. Even if Eve had one computer for every particle in the universe (there are $\approx 10^{80}$ of them), she would be way off.

2 a)

$n \equiv 2 \bmod 3$

$n \equiv 3 \bmod 5$

$n \equiv 2 \bmod 7$

$n = 2 + 3k$ (some $k \in \mathbb{Z}$)

$2 + 3k \equiv 3 \bmod 5$

$\Leftrightarrow 3k \equiv 1 \bmod 5$

$\Leftrightarrow 7\cdot 3\cdot k \equiv 7 \bmod 5$

$\Leftrightarrow k \equiv 2 \bmod 5$

ie. $k = 2 + 5h$. (some $h \in \mathbb{Z}$)

$\Rightarrow n = 8 + 15h$

ie. $n \equiv 8 \bmod 15$ (this combines the first two congruences).

Now, $8 + 15h \equiv 2 \bmod 7$

$\Leftrightarrow 15h \equiv -6 \bmod 7$

$h \equiv 1 \bmod 7$

$h = 1 + 7\ell$

$n = 8 + 15(1 + 7\ell)$

$n = 23 + 105\ell$.

So these three congruences amount to the single congruence

$n \equiv 23 \bmod 105$.

So $\boxed{23}$ is the smallest solution.

b) $23+105 = \boxed{128}$ is the only solution in $[100, 200]$.

(3) $m = 97 \cdot 101$

$\varphi(m) = 96 \cdot 100 = 9600.$

We want an ~~the~~ inverse of 211 modulo 9600.

(9600)

(211)

$[105] = (9600) - 45(211)$

$[1] = (211) - 2 \cdot [105]$

$= (211) - 2(9600) + 90(211)$

$= 91(211) - 2(9600)$

So $91 \times 211 \equiv 1 \mod \varphi(9797)$

$\Rightarrow$ decrypting exponent $\boxed{91}$.

(4) $11^1 \equiv 11$

$11^2 \equiv 121 \equiv 5$

$11^4 \equiv 5^2 \equiv 25$

$11^8 \equiv 25^2 \equiv 625 \equiv 16$

$11^{16} \equiv 16^2 \equiv 256 \equiv 24$

$$\left.\begin{aligned} 11^{21} &\equiv 11^{16} \cdot 11^4 \cdot 11^1 \\ &\equiv 24 \cdot 25 \cdot 11 \\ &\equiv (-5)\cdot(-4)\cdot 11 \\ &= 220 \\ &\equiv \boxed{17} \end{aligned}\right\} \text{all congruences modulo 29}$$

Another method: build up to 21 by either adding one or dividing by 2:

$21 \leftarrow 20 \leftarrow 10 \leftarrow 5 \leftarrow 4 \leftarrow 2 \leftarrow 1$

Then compute in turn:

$11^1 \equiv 11$

$11^2 \equiv 11 \cdot 11 \equiv 121 \equiv 5$

$11^4 \equiv 5 \cdot 5 \equiv 25$

$11^5 \equiv 11 \cdot 25 \equiv 11 \cdot (-4) \equiv -44 \equiv 14$

$11^{10} \equiv 14 \cdot 14 \equiv 196 \equiv 22 \equiv -7$

$11^{20} \equiv (-7)^2 \equiv 49 \equiv 20$

$11^{21} \equiv 20 \cdot 11 \equiv 220 \equiv 17.$

(5) We want to reduce $3^{13^{2015}} \bmod 100$.

Since $\varphi(100) = \frac{1}{2}\cdot\frac{4}{5}\cdot 100 = 40$, we can first reduce $13^{2015} \bmod 40$.

Since $\varphi(40) = \frac{1}{2}\cdot\frac{4}{5}\cdot 40 = 16$. we can first reduce $2015 \bmod 16$. Now, $16 \mid 2000$, so $2015 \equiv 15 \bmod 16$ and

$$13^{2015} \equiv 13^{15} \bmod 40.$$

Using successive squaring:

$$\begin{array}{l|l}
13^1 \equiv 13 & 13^{15} \equiv 13^1\cdot 13^2\cdot 13^4\cdot 13^8 \\
13^2 \equiv 169 \equiv 9 & \quad \equiv 13\cdot 9\cdot 1\cdot 1 \\
13^4 \equiv 9^2 \equiv 1 & \quad \equiv 117 \\
13^8 \equiv 1 & \quad \equiv 37 \bmod 40
\end{array}
\Bigg\} \text{ all mod } 40$$

Thus $13^{2015} \equiv 37 \bmod \varphi(100)$.

hence $3^{13^{2015}} \equiv 3^{37} \bmod 100$. Using successive squaring:

$$\begin{array}{l|l}
3^1 \equiv 3 & 3^{37} \equiv 3^{32}\cdot 3^4\cdot 3^1 \\
3^2 \equiv 9 & \quad \equiv 41\cdot 81\cdot 3 \\
3^4 \equiv 81 & \quad \equiv 3321\cdot 3 \equiv 21\cdot 3 \\
3^8 \equiv 81\cdot 81 \equiv 6561 \equiv 61 & \quad \equiv \underline{63} \\
3^{16} \equiv 61\cdot 61 \equiv 3721 \equiv 21 & \\
3^{32} \equiv 21\cdot 21 \equiv 441 \equiv 41 &
\end{array}
\Bigg\} \text{ all modulo } 100$$

So the last two digits are $\boxed{63}$

Alternate method: compute in turn the remainders of $3^1, 3^2, 3^4, 3^8, 3^9, 3^{18}, 3^{36}, 3^{37}$ (either squaring or ~~addi~~ mult. by 3 at each step).

(6) $n^3 \equiv 77 \bmod 100$

We can solve this by finding an inverse of 3 mod. $\varphi(100)$:

$$\varphi(100) = 40$$
$$\underline{27}\cdot 3 - 2\cdot 40 = 1$$

Hence by Euler's theorem, $n^{27\cdot 3} \equiv n \bmod 100$ (when $\gcd(n,100)=1$), and

$$n^3 \equiv 77 \bmod \iff n \equiv 77^{27} \bmod 100.$$

The remainder of 77^{27} can be found by successive squaring. It saves some labor to first work mod 4 & 100, then "merge" them with CRT.

mod 4	mod 25
$77^{27} \equiv 1^{27} \equiv 1$	$77^{27} \equiv 2^{27}$
	succ. squaring:
	$2^1 \equiv 2$
	$2^2 \equiv 4$
	$2^4 = 16 \equiv -9$
	$2^8 \equiv (-9)^2 \equiv 81 \equiv 6$
	$2^{16} \equiv 6^2 \equiv 36 \equiv 11$
	$\Rightarrow 2^{27} \equiv 2^{16}\cdot 2^8 \cdot 2^2 \cdot 2^1 \equiv 11\cdot 6\cdot 4\cdot 2$
	$\equiv 66\cdot 8 \equiv 16\cdot 8 \equiv 128 \equiv \underline{\underline{3}}$

So the solution n satisfies $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 25$.

Recombining: $n = 3 + 25k$, where $3 + 25k \equiv 1 \bmod 4$, ie. $k \equiv 2 \bmod 4$, so $n = 3 + 25(2+4h) = 53 + 100h$.

Thus $n^3 \equiv 77 \bmod 100 \iff n \equiv 53 \bmod 100$. The smallest such positive n is $\boxed{53.}$