$\varphi(n \cdot m) = \varphi(n)\,\varphi(m)$ if $\gcd = 1$

$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \dots)$

$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2)\dots$

1a) $\varphi(45000)$

$45000 = 2^3 3^2 \cdot 5^4$

$\varphi(n) = 45000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 12000$

$\boxed{12000}$

b) $\varphi(973656247)$

$\boxed{973569880}$

c) $\varphi(\text{giant \#}) = 2^3 \cdot 13^5 \cdot 59 \cdot 173 \cdot 619 \cdot 11383 \cdot 250951 \cdot 1006433^2\ 40513627$

$\Rightarrow$

$(2 \cdot 13 \cdot 59 \cdot 173 \cdot 619 \cdot 11383 \cdot 250951 \cdot 1006433\ 40513627) *$

$\frac{1}{2} \cdot \frac{12}{13} \cdot \frac{58}{59} \cdot \frac{172}{173} \cdot \frac{618}{619} \cdot \frac{11382}{11383} \cdot \frac{250950}{250951} \cdot \frac{1006432}{1006433}\ \frac{40513627}{40513627} =$

$\boxed{996498808171813066937044132390311005224960 0}$

2) $\varphi(n) \mid n \geq 3$ is $\varphi(n)$ always even

$\varphi(n) = k \mid 1 \leq k \leq n$ & $\gcd(n,k) = 1$

$\gcd(k,n) = 1 \therefore \gcd(n-k, n) = 1$

In this way there will always be a pair, $k$ & $n-k$. $\varphi$ is even

3) $\varphi(2n) = \varphi(n)$ iff $n$ is odd

$\gcd(n,2) = 1$

$\varphi(2n) = \varphi(2)\varphi(n) \Rightarrow 1(\varphi(n)) \therefore \varphi(2n) = \varphi(n)$

$n = 2^k m \mid m, k \in \mathbb{N}$ & $\gcd(m,2) = 1$

$\varphi(2n) = \varphi(2^{k+1} m) = \varphi(2^{k+1})\varphi(m) = 2 \cdot 2^{k-1}\varphi(m) \neq \varphi(n)$

$\therefore \gcd(n,2)$ must $= 1$ if $\varphi(2n) = \varphi(n)$

4) Compute the last 2 digits of $123^{403}$

$123^{0} \bmod 100 \equiv 123^{20} \bmod 100$

$360 \bmod (20) \equiv 3$

$123^{3} \bmod (100) \equiv 67$

$\boxed{67}$

5) $(13^{13})^{13}$ last 2 digits

$13^{13} \equiv 53 \bmod 100$

$53^{0} \equiv 53^{20} (\bmod 100) \equiv 1$

$53^{13} \equiv 73 \bmod 100$

$\boxed{73}$

$13^{(13^{13})}$

$13^{13} \equiv 53 \bmod 100$

$\bmod (53, 20) = 13$

$13^{13} \equiv 53 \bmod 200$

$\boxed{53}$

6) $2019^{2020}$ last 3 digits

$2019^{0} \equiv 2019^{50} \bmod 1000$

$2020 \bmod 50 \equiv 20$

$2019^{20} \equiv 601 \bmod 1000$

$\boxed{601}$

7) last digit of

a) $3^{n}: \{1, 3, 9, 7\}$

b) $7^{n}: \{1, 7, 9, 3\}$

c) $4^{n}: \{4, 6\}$

d) $6^{n}: \{6\}$

$3^{n} \bmod 10$ reveals $3^{0} \equiv 3^{4} \bmod 10$

$7^{0} \equiv 7^{4} \bmod 10$

$4^{1} \equiv 4^{3}$ $4^{0}$ excluded $n \geq 1$

$6^{1} \equiv 6^{2}$ $6^{0}$ excluded

8) $4328^{130035}$ last 2

$4328^{1} \equiv 4328^{21} \mod 100$

$130035 \pmod{21} \equiv 3.$

$4328^{3} \pmod{100} \equiv 52$

$\boxed{32}$

9) $7 \mid 5555^{2222} + 2222^{5555}$

$5555 \equiv 4 \mod 7$
$2222 \equiv 3 \mod 7$

$4^{1} \equiv 4^{4} \quad 4^{0} \equiv 4^{3}$
$3^{1} \equiv 3^{7} \quad 3^{0} \equiv 3^{6}$

$4^{2} + 3^{5} \mod 7 \Rightarrow 2 + 5 \mod 7 \equiv 0$

$\therefore 7 \mid 5555^{2222} + 2222^{5555}$

10a) $x^{611} \equiv 605 \mod 2021$

$a^{\varphi(n)} \equiv 1 \mod n$

$m^{e} \equiv c \mod n \qquad x^{611} \equiv 605 \mod 2021$
$c^{d} \equiv (m^{e})^{d} \equiv m \pmod n \qquad 605^{d} \equiv x$

$d = mi(e, \varphi(n)) = 683$

$605^{683} \equiv 1492 \mod 2021$

$\boxed{1492}$

b) $\boxed{2020}$

c) $x^{11} \equiv c \mod n$
$d = mi(11, \varphi(n))$
$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2) = 38647551115129 68 \rightarrow P$
$d = mi(11, P) = 17567068688 69531$

$c^{d} \equiv x \mod n \Rightarrow c = \boxed{1234567}$

11) RSA: $N = 28692529$ $e = 97$ find $d$

$n = P \cdot Q$

$d = mi(e, \varphi(n)) = 26019713$

$m = 1234$ $\quad 1234^{97} \equiv 27595509 \mod N$

$27595509^{26019713} \equiv 1234 \mod N$

$m^e \equiv c \mod N$

$c^d \equiv (m^e)^d \equiv m \pmod N$

$d = mi(e, \varphi(n))$

$$\boxed{d = 26019713}$$

12) RSA: $N = 28692529$ find $e$

$d = mi(77, \varphi(n)) = 24583560$

$39 = 10295679$

$344 = 28598640$

The $\gcd(e, \varphi(n))$ must $= 1$ because otherwise a unique solution is not guaranteed

$2^3 \mod 65 \equiv 57^3 \mod 65$

$$\boxed{39}$$

13a) RSA: Security matters!... Plain text

5455377799 5515133128 1930359923 1130301528 2975000000

(encoded text)

zeros used to fill

$\downarrow$

$\text{encoded}^{123} = \text{encrypted} \mod n$

$$\boxed{627206874173,\ 2178887109512,\ 5820740544122,\ 1894810934600,\ 7537734125680}$$

encrypted text

13 b)

$d = \text{multinv}(e, \varphi(n))$

$(\text{for every encrypted Block})^d = \text{enloded} \bmod n$

40191719521524992825132129 75 encoded

Digip en ⎵ rocks! plaintext