1. Decrypt using the Playfair cipher:

M	I/J	N	E	W
A	S	B	C	D
F	G	H	K	L
O	P	Q	R	T
U	V	W	Y	Z

QT → PR	IY → EV	GK → FH	TM → OW	BS → SA
WE → EN	CM → AE	VZ → UY	CY → ER	ME → WN
UM → OU	EC → YE	BV → SX		

Intermediate value is:
I = PREVFHOWSAENAEUYERWNOUYES (X is removed from end)

Since there are 25 characters, and no padding was necessary, then the transposition cipher most likely has 5 × 5 rows/columns:

I = PREVF HOWSA ENAEU YERWN OUYES

or

P	H	E	Y	O
R	O	N	E	U
E	W	A	R	Y
V	S	E	W	E
F	A	U	N	S

Consider the first character of each block: PHEYO.
How can those letters be re-arranged to make a 4-letter word? Since the last letter of *m* is not a vowel, then of "FAUNS" the last character of the first row must end with 'P', 'Y' or 'O'.

If it ends with 'P' we have 'HEYO' remaining. The 4 letter words: ?
If it ends with 'Y' we have 'PHEO' remaining. The 4 letter words: 'hope', ?
If it ends with 'O' we have 'PHEY' remaining. The 4 letter words: ?
So, if the first 5 characters are 'HOPEY' then the key must be 25134 giving:

H	O	P	E	Y
O	U	R	N	E
W	Y	E	A	R
S	E	V	E	W
A	S	F	U	N

Message *m* = HOPE YOUR NEW YEARS EVE WAS FUN

2. Proof: We will prove this by Mathematical Induction
As a base case, clearly $4^1 \equiv 4 \bmod 12$.
Now suppose that $4^k \equiv 4 \bmod 12$. Then $4^{k+1} \equiv 4(4^k) \bmod 12$.
By assumption, $4^k \equiv 4 \bmod n$, so $4^{k+1} \equiv 4^2 \bmod 12$. And $4^2 \equiv 16 \equiv 4 \bmod 12$.
This shows that for any $n \in N$, $4n \equiv 4 \bmod 12$.

3. Proof: Let $d = \gcd(z, x)$, then $z = dc$ and $x = da$, where $\gcd(a, c) = 1$
$\therefore \gcd(z, xy) = \gcd(dc, day) = d \times \gcd(c, ay) = d \times \gcd(c, y)$
because $\gcd(a, c) = 1$
$$\therefore \gcd(z, xy) = \gcd(z, x)\gcd\left(\frac{z}{d}, y\right) = \gcd(z, x)\gcd\left(\frac{z}{\gcd(z, x)}, y\right)$$

4. The key space of the affine is $24 \times 45 = 1080$

5. If the key length is small i.e. 3 or 4 characters, then Kasiski method can be used for Hill cipher also.

6. $P(a) = 1/2$, $P(b) = 1/3$, therefore $P(c) = 1/6$. $P(k_1) = 3/4$, $P(k_2) = 1/4\cdot$
$P(x/a) = P(k_1)\cdot P(x/E_{k1}(a)) + P(k_2)\cdot P(x/E_{k2}(a)) = 3/4\cdot 0 + 1/4\cdot 0 = 0$,
Similarly, $P(x/b) = 0$, $P(x/c) = 1$.
$P(y/a) = P(k_1)\cdot P(y/E_{k1}(a)) + P(k_2)\cdot P(y/E_{k2}(a)) = 3/4\cdot 0 + 1/4\cdot 1 = 1/4$,
$P(y/b) = 3/4$, $P(y/c) = 0$.
$P(z/a) = P(k_1)\cdot P(z/E_{k1}(a)) + P(k_2)\cdot P(z/E_{k2}(a)) = 3/4\cdot 1 + 1/4\cdot 0 = 3/4$,
$P(z/b) = 1/4$, $P(z/c) = 0$.

$P(x) = P(k_1)\cdot P(c) + P(k_2)\cdot P(c) = 3/4\cdot 1/6 + 1/4\cdot 1/6 = 1/6$
$P(y) = P(k_1)\cdot P(b) + P(k_2)\cdot P(a) = 3/4\cdot 1/3 + 1/4\cdot 1/2 = 3/8$
$P(z) = P(k_1)\cdot P(a) + P(k_2)\cdot P(b) = 3/4\cdot 1/2 + 1/4\cdot 1/3 = 11/24$

By Bayes theorem
$$P(a/x) = \frac{P(a)P(x/a)}{P(x)}$$

$$P(a/x) = \frac{(1/2) \times 0}{1/6} = 0, \quad P(b/x) = 0 \ and \ P(c/x) = 1$$
$P(a/y) = 1/3, \quad P(b/y) = 2/3, \quad and \ P(c/y) = 0$
$P(a/z) = 9/11, \quad P(b/z) = 2/11, \quad and \ P(c/z) = 0$
So, there is no perfect secrecy.

7. Total characters = 26(a-z) + 26(A-Z) + 10(0-9) = 62
Passwords which can be formed without using any digit = 62 - 10 (0-9) = 52
Passwords must be between 5 characters to 7 characters with at least one digit
Possible number of passwords is

$$\sum_{k=5}^{7} 62^k - \sum_{k=5}^{7} 52^k = 3.5 \times 10^{12} - 1.048 \times 10^{12} = 2.45 \times 10^{12}$$

Time required to crack = Total number of possible passwords × rate × accuracy

$$= 2.45 \times 10^{12} \times \frac{1}{2500000} \times 0.75 = 735000 \text{ Secs} = 8.5 \text{ days}$$

8. Let r be the remainder on dividing n by $\lambda(n)$. i.e. $n = r + u\,\lambda(n)$.
We also know $\lambda(n)$ divides $\varphi(n)$. Therefore let $\varphi(n) = v\,\lambda(n)$.
$n - \varphi(n) = r \bmod \lambda(n)$. i.e. $p + q - 1 = r \bmod \lambda(n)$.
Therefore, p and q are roots of $x^2 - (r + 1)\,x + n = 0$
Here $r = 589 \bmod 90 = 49$.
$x^2 - 50\,x + 589 = 0 \Rightarrow x = 31, 19$ which are the factors of 589.

9. We have that $(xy/q) = (x/q)\,(y/q)$. Since each of the Legendre symbols in this equality assumes the value 1 or −1, it follows that at least one of them must be equal to 1. Hence at least one of x, y, or xy must be a quadratic residue modulo q.

10. $c^{e^k} \bmod n = c \Longrightarrow \left(c^{e^{k-1}}\right)^e \bmod n = m^e \quad \because c = m^e$

$$\Longrightarrow c^{e^{k-1}} = m \bmod n$$

11. The Diophantine equation $x^2 + py + a = 0$ is equivalent to the quadratic congruence $x^2 \equiv -a \pmod{p}$. This quadratic congruence has a solution if and only if $(-a/p) = 1$.

12. Here, in this question lg means $\lceil \lg \rceil$ which is very fast on a computer.
Using Divisions Primes $p_1, \ldots, p_t <$ B divide x. Divide x by all the p_i .
Also, p_i^2, p_i^3, etc. until does not work.
When you are done you've B-factored the number or not.
Using Subtraction Primes $p_1, \ldots, p_t <$ B divide x.
Do $d = \lg(x) - \lg(p_1) - \lg(p_2) - \cdots - \lg(p_t)$
If d ∼ 0 then we think x is B smooth.
If far from 0 then declare DO NOT DIVIDE!