1) a) $\gcd(14039, 1528)$

$= \gcd(1529, 278)$

$= \gcd(278, 139)$

$= \gcd(139, 0)$

$= 139$

$14039 = 9 \cdot 1529 + 278$

$1529 = 5 \cdot 278 + 139$

$\Rightarrow 139 = 1529 - 5 \cdot 278$

$= 1529 - 5 \cdot (14039 - 9 \cdot 1529)$

$= 1529 + (45)1529 - (5)14039$

$= 46(1529) - 5(14039)$

$s = -5 \quad t = 46$

b) $1528x \equiv 1 \pmod{14039}$

$x \equiv \overline{1528} \pmod{14039}$

$x \equiv 1528^{-1} \pmod{14039}$

$\Rightarrow 14039 = 1528(9) + 287$

$1528 = 287(5) + 93$

$287 = 93(3) + 8$

$93 = 8(11) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$\Rightarrow 1 = 3 - 2$

$= 3 - (5 - 3)$

$= 2 \cdot 3 - 5$

$= 2 \cdot (8 - 5) - 5 = 2(8) - 3(5)$

$= 2(8) - 3(93 - 11(8))$

$= 2(8) - 3(93) + 33(8)$

$= 35(8) - 3(93)$

$= 35(287 - 3(93)) - 3(93)$

$= 35(287) - 108(93)$

$= 35(14039 - 9(1528)) - 108(1528 - 5(287))$

$= 35(14039) - 315(1528) - 108(1528) + 540(287)$

$= 35(14039) - 423(1528) + 540(287)$

$= 35(14039) - 423(1528) + 540(14039 - 9(1528))$

$= 35(14039) - 423(1528) + 540(14039) - 4860(1528)$

$= 575(14039) - 5283(1528)$

$1528^{-1} \pmod{14039} \equiv -5283 \equiv 8756$

$1528x \equiv 1 \pmod{14039}$

$x = 8756$ 953

C) $2x \equiv 3 \pmod 5$

$5x \equiv 2 \pmod 6$

CRT $4x \equiv 7 \pmod{11}$

$\Rightarrow x \equiv 4 \pmod 5$

$x \equiv 4 \pmod 6$

$x \equiv 2 \pmod{11}$

1. $2x \equiv 3 \pmod 5$

$2x \equiv 3+5 \pmod 5$

$x \equiv \frac{8}{2} \pmod 5$

$\because \gcd(2,5) = 1$

$x \equiv 4 \pmod 5$

2. $5x \equiv 2 \pmod 6$

$6x - 1x$

$-1x \equiv 2 \pmod 6$

$x \equiv -2 \pmod 6$

$x \equiv 4 \pmod 6$

3. $4x \equiv 7 \pmod{11}$

$x \equiv \frac{7}{4} \pmod{11}$

$\because \gcd(4,11) = 1$

$x \equiv 2 \pmod{11}$

1) $m = 5 \cdot 6 \cdot 11 = 330$

2) $M_1 = \frac{m}{m_1} = 66$

$M_2 = 55$

$M_3 = 30$

3) $y_1 = M_1^{-1} \equiv 1 \pmod 5$

$y_2 = M_2^{-1} \equiv 1 \pmod 6$

$y_3 = M_3^{-1} \equiv 7 \pmod{11}$

4) $X = 1 \cdot 4 \cdot 66 + 1 \cdot 4 \cdot 55 + 7 \cdot 2 \cdot 30$

$= 904 \equiv 244 \pmod{330}$

$X = 244 + 330y$

2) 1) Paris
2) Bordeaux
3) Lyon
4) Marseille
5) Nice
6) Cannes

3) 1) Argo
2) Alien
3) Chicago
4) Grease
5) Titanic

4) Eve has: c & a message r to encrypt as $z = r^e \pmod n$ and given to Bob; Bob will return $X^d \pmod n$
$m^e \pmod n$

let $X = c \cdot z$

- $a^b \bmod c = (a \bmod c)^b \bmod c$
- $xy \bmod z = x \bmod z \cdot y \bmod z$
- $\phi(n) = \phi(pq)$
$= \phi(p)\,\phi(q) = (p-1)(q-1)$
- $\gcd(e, (p-1)(q-1)) = 1$
- $de \equiv 1 \pmod{(p-1)(q-1)}$

$$X^d \pmod n = (m^e \pmod n \cdot r^e \pmod n)^d \pmod n$$
$$= (m^e r^e)^d \pmod n \quad \cancel{\pmod n}$$
$$= (mr)^{de} \pmod n$$
$$= (mr)^{1 + k(p-1)(q-1)} \pmod n$$
$$= (mr)(mr)^{k(p-1)(q-1)} \pmod n$$
$$= (mr)(mr)^{k\phi(n)} \pmod n$$
$$= (mr)\cancel{(mr)^{\phi(n)^k}} \pmod n$$
$$= mr \pmod n, \text{ we know } r \text{ so}$$
$$\Rightarrow \frac{mr \pmod n}{r} = m \pmod n$$

she can get m from this since she has the public key n

⇒ Eve should construct X to be Alice's ciphertext times some ciphertext z of a message r using Bob's encryption method.

5) let vertex = room
let edge = door

-> The degree-sum formula states that the sum of the degrees (# times each vertex is touched) is equal to twice the number of edges (doors). This means that there is an even net degree of the rooms in the mansion. Since there is a given singular entrance to the mansion (one degree to a room (vertex) of the mansion), at least one room in the mansion must have an odd degree to even out the first single odd degree provided by the entrance, and thus contain no ghost.

I pledge my honor that I have abided by the stevens honor system. UwU

Issac Zheng
Rohan Kallur