1) a) $y = 7x + 9 \mod 26$

	L	O	E	S	U	N	G
$x =$	11	14	4	18	20	13	6
$y =$	8	3	11	5	19	22	25
	I	D	L	F	T	W	Z

b) $7x = y - 9 \mod 26 \rightarrow x = (y-9) \cdot 7^{-1} \mod 26$

$7^{-1} = 7^{\phi(26)-1} \mod 26$

$\phi(26) = \phi(2 \cdot 13) = \phi(2) \cdot \phi(13) = 1 \cdot 12 = 12$

$7^{12-1} = 7^{11} \mod 26 = 15$

$\rightarrow x = (y-9) \cdot 15 \mod 26$

y	8	3	11	5	19	22	25
x	11	14	4	18	20	13	6

2) a) Alice: $3^3 \bmod 19 = 8$

Bob: $3^2 \bmod 19 = 9$

key: $8^2 \bmod 19 = 9^3 \bmod 19 = 7$

b) $19 = 2 \cdot 9 + 1$

not prime → 19 is not a safe prime

c) prime factors of $19 - 1 = 18 = 2 \cdot 3 \cdot 3 \Rightarrow r = 2$ & 3

$$\left.\begin{array}{l} 3^{\frac{18}{2}} \bmod 19 = 3^9 \bmod 19 = 18 \neq 1 \\ 3^{\frac{18}{3}} \bmod 19 = 3^6 \bmod 19 = 7 \neq 1 \end{array}\right\} \Rightarrow 3 \text{ is a primitive root mod } 19$$

d) key: $7_{10} = 111_2$

message: $5_{10} = 101_2$ XOR

plaintext $2_{10} = 010_2$

37a) $n = 3 \cdot 11 = 33$ $\quad 1 < c < \phi(n)$

$\phi(33) = 2 \cdot 10 = 20 = 2 \cdot 2 \cdot 5$ $\quad \gcd(c, 20) = 1$

$c \in \{3, 7, 9, 11, 13, 17, 19\}$

$\phi(20) = \phi(2^2 \cdot 5) = 2^1 \cdot 1 \cdot 5^0 \cdot 4 = 8$

b) $c = 7 \rightarrow d = 7^{-1} \bmod 20 = 7^{\phi(20)-1} \bmod 20 = 7^7 \bmod 20 = 3$

c) $E = 5: \; 5^7 \bmod 33 = 14$ $\quad I = 9: \; 9^7 \bmod 33 = 15$

d) R G A M

18 7 1 19

$18^3 \bmod 33 = 24$ X

$7^3 \bmod 33 = 13$ M

$1^3 \bmod 33 = 1$ A

$13^3 \bmod 33 = 19$ S