Alec Freeman

HW 10

1.

(a)

$p = 3 \quad n = 33$

$q = 11 \quad z = 20$

Symbolic	Numeric (m)	$c = m^e \bmod n$
D	4	$4^{13} \bmod 33 = 31$
O	15	$15^{13} \bmod 33 = 9$
G	7	$7^{13} \bmod 33 = 13$

choose $e = 13$

$ed \bmod z = 1 = 13 \cdot d \bmod 20 \qquad 13 \cdot 17 = 221$

$d = 17 \qquad 221 \bmod 33 = 1$

$15^{13} \bmod 33 = (15^8 \cdot 15^4 \cdot 15^1) \bmod 33$

$= (15^8 \bmod 33 \cdot 15^4 \bmod 33 \cdot 15^1 \bmod 33) \bmod 33$

$= (9 \cdot 3 \cdot 15) \bmod 33 = 9$

$7^{13} \bmod 33 = (31 \cdot 25 \cdot 7) \bmod 33 = 13$

The encryption for d, o, g is 31, 9, 13

(b) $d = 17 \quad m = c^d \bmod$

	c	$m = c^d \bmod$
d	31	$31^{17} \bmod 33 = 4$
o	9	$9^{17} \bmod 33 = 15$
g	13	$13^{17} \bmod 33 = 7$

$31^{17} \bmod 33 = \left((31^4 \bmod 33)^4 \cdot (31 \bmod 33) \right) \bmod 33$

$= ((16)^4 \cdot 31) \bmod 33 = 4$

$9^{17} \bmod 33 = ((9^4 \bmod 33)^4 \cdot 9 \bmod 33) \bmod 33 =$

$= (27^4 \cdot 9) \bmod 33 = 15$

$13^{17} \bmod 33 = ((16)^4 \cdot 13) \bmod 33 =$

The decryption algorithm applied to the encrypted version yields the original plaintext for d, o, g which is $\boxed{4, 15, 7}$

2.

$p=5 \quad q=11$

a. $n=55$

$z=40$

b.

$e=3$

It is an acceptable choice for e because it is a prime number relative to z or $e=3$ and $z=40$ have no common factors except 1.

c.

$3 \cdot 27 = 81$ and $81 \bmod 40 = 1$

So choose $d=27$

d.

$m=8$

$c = m^e \bmod n$

$= 8^3 \bmod 55 = (512 \bmod 55)$

$= (64 \bmod 55)(8 \bmod 55) \bmod 55$

$= 17 \bmod 55$

$= \boxed{17}$

$e(m) = \boxed{17}$

3.

a. $S = TB^{SA} \bmod p \qquad S' = TA^{SB} \bmod p$

$a \equiv b \bmod p$ then $a^e \equiv b^e \bmod p$

$a = g$

$\boxed{S} = TB^{SA} \bmod p$

$= (g^{SB} \bmod p)^{SA} \bmod p$

$= g^{SB(SA)} \bmod p \bmod p$

$= g^{SB(SA)} \bmod p$

$= g^{SB(SA)} \bmod p$

$= g^{SB(SA)} \bmod p \bmod p$ AND $TA = g^{SA} \bmod p$

$= TA^{SB} \bmod p = \boxed{S'}$

b.

b. $p = 11$

$g = 2$

$SA = 5 \qquad SB = 12$

$TA = g^{SA} \bmod p = 2^5 \bmod 11 = \boxed{10}$

$TB = g^{SB} \bmod p = 2^{12} \bmod 11 =$

$(2^6 \bmod 11)(2^6 \bmod 11) \bmod 11$

$= (9)(9) \bmod 11 = \boxed{4}$

$TA = 10$
$TB = 4$

c.

$S = 10^{12} \bmod 11 = 4^5 \bmod 11$

$= 4^5 \bmod 11 = \boxed{1}$

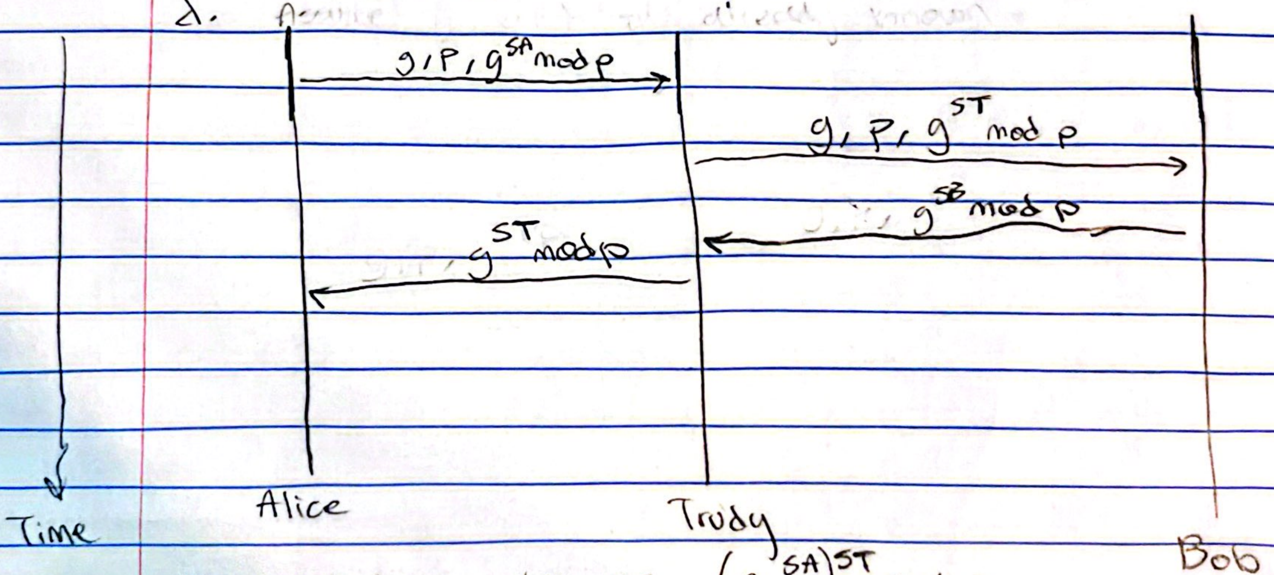
$= 10^{12} \bmod 11$

$= (10^6 \bmod 11)(10^6 \bmod 11) \bmod 11$

$= 1 \bmod 11 = \boxed{1}$

$S = 1$

d.



Alice calculates key as $(g^{SA})^{ST} \bmod p$

Trudy calculates key for Alice as $(g^{ST})^{SA} \bmod p$

Bob calculates (session) key as $g^{(ST)(SB)} \bmod p$

Trudy calculates key for Bob as $(g^{ST})^{SB} \bmod p$

Alice and Bob think they are talking with each other when Trudy is the one to least send the message or the .

One who recieves it.