## Honework 7 Question 1

The congruence

X = C mod P

has a unique solution congruence modulo prime pWhen gcd(e, p-1) = 1.

JU 1

In this question, you are asked to explore what happen when  $gcd(e,p+) \pm 1$ .

Consider p prime. c \$ 0 mod P. e > 1.

- Such that  $x_6 = C$  mod b has no solution.

  (1) Give an example of b (blume),  $C \not\equiv 0$  mod b, 6 > 1
- G) Give an example of p (prime),  $C \neq 0$  mod P,  $e \geq 1$ sum that  $g(d(e, p-1) \neq 1)$  and  $X^e = 0$  mod Phas at least two solutions.

Prove that if  $X^6 \equiv C$  and P has a solution, then it has QCd(e, P-1) distant solutions.

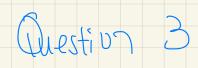
Bob	Alice
Key creation	
Choose secret primes $p$ and $q$ .	
Choose encryption exponent $e$	
with $gcd(e, (p-1)(q-1)) = 1$ .	
Publish $N = pq$ and $e$ .	
Encryption	
	Choose plaintext $m$ .
	Use Bob's public key $(N, e)$
	to compute $c \equiv m^e \pmod{N}$ .
	Send ciphertext $c$ to Bob.
Decryption	
Compute d satisfying	
$ed \equiv 1 \pmod{(p-1)(q-1)}.$	
Compute $m' \equiv c^d \pmod{N}$ .	
Then $m'$ equals the plaintext $m$ .	

Table 3.1: RSA key creation, encryption, and decryption



Section. The RSA public key cryptosystem

- **3.6.** Alice publishes her RSA public key: modulus N=2038667 and exponent e=103.
- (a) Bob wants to send Alice the message m=892383. What ciphertext does Bob send to Alice?
- (b) Alice knows that her modulus factors into a product of two primes, one of which is p = 1301. Find a decryption exponent d for Alice.
- (c) Alice receives the ciphertext c = 317730 from Bob. Decrypt the message.



**3.8.** Bob's RSA public key has modulus N=12191 and exponent e=37. Alice sends Bob the ciphertext c=587. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message. (*Hint. N* has a factor smaller than 100.)



**3.13.** Alice decides to use RSA with the public key N=1889570071. In order to guard against transmission errors, Alice has Bob encrypt his message twice, once using the encryption exponent  $e_1=1021763679$  and once using the encryption exponent  $e_2=519424709$ . Eve intercepts the two encrypted messages

$$c_1 = 1244183534$$
 and  $c_2 = 732959706$ .

Assuming that Eve also knows N and the two encryption exponents  $e_1$  and  $e_2$ ,

Can Eve find out the plaintext without finding p, a ?

Question 5

The following question is an experiment to the following statement:

If N = pq is a product of two district odd primes. If e = 3 and d is given such that  $3d = 1 \mod \Phi(n)$ .

Then we can find  $\Phi(n)$  easily.

For each of the following values, find  $\emptyset(N)$ :

(a) N = 17693317, e = 3, d = 11789931(b) N = 61853041, e = 3, d = 41224875

Additival Questions

1) Double encyption RSA.

Public parioreters: N, e, e2

private parameters: d,, d=, p, q,

To encrypt = C= m ond N

C== C, = mud N

To decorpt : [TO DO]

[TODO] Argue Whether Dande encyption RSA is equal | less / more secure than RSA.

2) Multi prime RSA N=Pgr Where Plane are distinct odd primes. Public parameters: N, e. private parameters: d, P, 9, To except: me mad N To decompt: Cd mad N How to feed of? e g = / ung 55 Argue whether multiprine RSA is equal/ more less secure than RSA. Arque unetre there is an advantage of using Multipame.