Homework 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.

- (1) Give an example of p (prime), $c \neq 0$ much p, $e \geq 1$
- Give an example of p corine), $C \neq 0$ much P, $e \geq 1$ such that $g(d(e,p+) \neq 1)$ and $\chi^{e} = 0$ much P has at least two solutions.

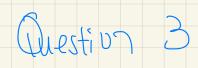
Bob	Alice
Key creation	
Choose secret primes p and q .	
Choose encryption exponent e	
with $gcd(e, (p-1)(q-1)) = 1$.	
Publish $N = pq$ and e .	
Encryption	
	Choose plaintext m .
	Use Bob's public key (N, e)
	to compute $c \equiv m^e \pmod{N}$.
	Send ciphertext c to Bob.
Decryption	
Compute d satisfying	
$ed \equiv 1 \pmod{(p-1)(q-1)}.$	
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 $3d = 1 \mod 0$ (m). Then we can find $0 \pmod 2$ easily.

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

(a) N = 17693317, e = 3, d = 12544187(b) N = 61853041, e = 3, d = 41224875

Hmt () ((N) | Bd-1 Let N' = 3d-1 We 'know (ech) is a factor of N N'is a small multiple of N. $(N \simeq (N)) \leftarrow N \Rightarrow (-9) \leftarrow Q \qquad 21 \quad (N) \bigcirc$ N' 15 a "small" multiple of UN. Find K S, t K divides N', and compute NIK, which is a potential value of QW). Use 3 to chert it WIK is actually equal to (P-1)(9-1) for some primes Guen Nard (la), Fird P, q, (a) compute ptq using Q(N) = (P-)(9-1) = Pq - (P+q) + 1 (b) compute P, q, by friding roots of

 $\chi^2 - (P+q) \times + Pq = 0$