

Homework 7

Question 1

The congruence

$$x^e \equiv c \pmod{p}$$

has a unique solution congruence modulo prime p

when $\gcd(e, p-1) = 1$.

In this question, you are asked to explore what happens when $\gcd(e, p-1) \neq 1$.

Consider p prime, $c \not\equiv 0 \pmod{p}$, $e \geq 1$.

- ① Give an example of p (prime), $c \not\equiv 0 \pmod{p}$, $e \geq 1$ such that $x^e \equiv c \pmod{p}$ has no solution.
- ② Give an example of p (prime), $c \not\equiv 0 \pmod{p}$, $e \geq 1$ such that $\gcd(e, p-1) \neq 1$ and $x^e \equiv c \pmod{p}$ 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

Question 2

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.

Question 3

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.)

Question 4

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

$$c_1 = 1244183534 \quad \text{and} \quad c_2 = 732959706.$$

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, q ?