MATH 135 — Fall 2021
Practice Problems — Chapter 9

Mark Girard

November 23, 2021

This document contains some extra notes and practice problems related to cryptography and RSA encryption.

RSA encryption

RSA encryption

- Bob's set up.
  - Bob picks distinct primes p and q and calculates $n = pq$.
  - Bob chooses numbers e and d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.
  - Bob publishes his public key (n, e) and keeps his private key (n, d) secret.
- Alice picks a message, then encrypts and sends the encrypted message.
  - Alice wants to send a message to Bob using his public key (n, e).
  - Alice picks a message $M \in \{0, 1, 2, \ldots, n-1\}$.
  - Alice encrypts the message by solving for the remainder C when M^e is divided by n:
  $$C \equiv M^e \pmod{n}$$
  - Alice sends the ciphertext (encrypted message) C to Bob.
- Bob receives and recovers the message.
  - Bob receives the ciphertext C from Alice.
  - Bob uses private key (n, d) to decrypt the message by solving for the remainder R when dividing C^d by n:
  $$R \equiv C^d \pmod{n}$$
  - Bob perfectly recovers the message $R = M$.

Note that $R \equiv C^d \equiv (M^e)^d \equiv M^{ed} \pmod{p}$.

The fact that Bob can perfectly recover Alice's message by decrypting the ciphertext is a consequence of the following theorem.

Theorem. *Suppose p and q are distinct prime numbers and define $n = pq$. Suppose $e, d \in \mathbb{Z}$ are integers such that*

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

For every $M \in \{0, 1, 2, \ldots, n-1\}$, it holds that

$$M^{ed} \equiv M \, (mod \; n).$$

Proof. Because $ed \equiv 1 \pmod{(p-1)(q-1)}$, by definition of modular congruence there exists an integer $k \in \mathbb{Z}$ such that

$$ed = 1 + k(p-1)(q-1).$$

Let $R \in \{0, 1, 2, \ldots, n-1\}$ be the remainder of M^{de} when dividing by n. That is,

$$R \equiv M^{ed} \pmod{pq},$$

where $n = pq$. Because p and q are coprime, by Splitting the Modulus this is equivalent to

$$\begin{cases} R \equiv M^{ed} \pmod{p} & (1) \\ R \equiv M^{ed} \pmod{q}. & (2) \end{cases}$$

We now prove that $R \equiv M \pmod{p}$. There are two cases to consider.

Case 1: Suppose $p \nmid M$. By Fermat's Little Theorem, it follows that $M^{p-1} \equiv 1 \pmod{p}$. Now

$$\begin{aligned} R &\equiv M^{ed} && \pmod{p} && \text{[from (1)]} \\ &\equiv M^{1+k(p-1)(q-1)} && \pmod{p} && \text{[because } ed = 1 + k(p-1)(q-1)\text{]} \\ &\equiv M \cdot (M^{p-1})^{k(q-1)} && \pmod{p} && \\ &\equiv M \cdot 1 && \pmod{p} && \text{[by Fermat's Little Theorem]} \\ &\equiv M && \pmod{p} && \end{aligned}$$

Case 1: Suppose $p \mid M$. Then $M \equiv 0 \pmod{p}$, and thus

$$R \equiv M^{ed} \equiv 0^{ed} \equiv 0 \equiv M \pmod{p}.$$

In either case, we have proved that $R \equiv M \pmod{p}$. This proves (1), which is to say, this proves that $R \equiv M^{ed} \pmod{p}$. The proof of (2) is similar. (That is, it is essentially the same proof to prove that $R \equiv M^{ed} \pmod{q}$.) So we can conclude that

$$R \equiv M^{ed} \pmod{p} \qquad \text{and} \qquad R \equiv M^{ed} \pmod{q}.$$

By Splitting the Modulus, this is equivalent to

$$R \equiv M^{ed} \pmod{pq}.$$

This completes the proof. □

Example

Suppose Alice and Bob choose to use the following encoding of letters of the alphabet into numbers:

" "	00
"A"	01
"B"	02
"C"	03
⋮	⋮
"Z"	26

The word "HELLO" would be encoded as the ten-digit number

$$0805121215$$

while the message "FROM ALICE" would be encoded as

$$06181513000112090305.$$

Bob constructs his public–private key pair by choosing primes $p = 36809$ and $q = 77377$, and defines $n = p \cdot q = 2848169993$. Bob chooses $e = 5$ and $d = 4556889293$. It can be checked (with a computer) that these numbers satisfy

$$e \cdot d \equiv 1 \pmod{2848055808},$$

where $(p-1)(q-1) = 2848055808$. We now have:

Bob's public key:	Bob's private key:
(2848169993, 5)	(2848169993, 4556889293).

Alice chooses to send the message "HELLO" which corresponds to the plaintext $M = 805121215$. Note that $0 \leq M < n$, so this is a valid message. Using a computer, we can solve the congruence

$$C \equiv M^5 \pmod{n}$$

to find the ciphertext $C = 751696144$. Alice sends this resulting ciphertext to Bob, who then decrypts it. Again, using a computer, we can check that Bob perfectly recovers the message $R = M$ when solving the congruence

$$R \equiv C^d \pmod{n},$$

and Bob finds $R = 805121215$, which he can decode to "HELLO".

Remark. What if the message that Alice wants to send is bigger than n? She can split up her message into multiple components and send each component separately. For example, to send the message "FROM ALICE" using the public key above, Alice could send messages "FROM " and "ALICE" separately as

$$M_1 = 0618151300 \qquad \text{and} \qquad M_2 = 0112090305.$$

The corresponding ciphertexts for these messages can be determined to be

$$C_1 = 1643373961 \qquad \text{and} \qquad C_2 = 2028678151,$$

which Bob would receive and decrypt separately.

Practice problems

1. Check (using a computer) that Bob perfectly recovers the messages M_1 and M_2 from the ciphertexts C_1 and C_2 using his private key from the example above.

Note. For the rest of the practice problems, you should try solving these by hand to make sure you understand how to properly solve these types of congruences. It may be useful to use a computer to check your work!

2. To generate a public–private key pair, Bob chooses primes $p = 11$ and $q = 13$ and computes $n = pq$. He then chooses $e = 23$.
   (a) What is Bob's public key?
   (b) What value for d should Bob choose to make his private key?
   (c) Suppose Alice wishes to send the message $M = 25$ to Bob. What should her ciphertext (encrypted message) be that she transmits for Bob to decrypt?
   (d) Check to make sure that $C^d \equiv M \pmod{n}$.

3. To generate a public–private key pair, Bob chooses primes $p = 23$ and $q = 13$ and computes $n = pq$. He then chooses $e = 283$.
   (a) What is Bob's public key?
   (b) What value of d should Bob choose to make his private key?
   (c) Suppose Alice picks a message $M \in \{0, 1, \ldots, n-1\}$ to send to Bob. She computes the ciphertext C by solving the congruence $C \equiv M^e \pmod{n}$ for $C \in \{0, 1, \ldots, n-1\}$ which she sends to Bob. The ciphertext she sends is $C = 7$. What is the original plaintext message she was trying to send?