**Computer Algorithm**

**Chapter 04**

**RSA Algorithm**

**[실습] RSA 암호화 알고리즘**

**실습 목표**

* **RSA 암호화 알고리즘의 작동방식에 대해 자세히 학습한다.**
* **RSA 암호화 알고리즘을 이용하여 문자열을 암호화 & 복호화를 구현할 수 있다.**

**요구사항**

* **실습과제 1) (100점)**

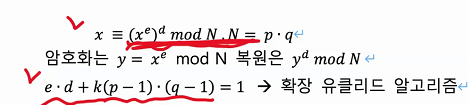
문자열 “Hello Dongguk. My name is Woongsup Kim”을 RSA 암호화 알고리즘으로 암호화 및 복호화 하는 프로그램을 구현한다.

//이름은 내껄로

P = 11, q = 17, e = 3 으로 주어진다. 입력은 C언어 표준 라이브러 리를 이용한다. (배경지식에 있는 구현순서 참고가능)

**배경지식**

RSA 암호화 알고리즘은 공개키와 비밀키의 2 종류 키를 사용하여 메시지를 암호화하고 복호화 하는 알고리즘으로, 메시지를 암호화/복호화를 하는 데 비밀키만을 사용하는 알고리즘에 비해 암호키 업데이트가 용이하여 메시지 역추적을 무력화할 수 있다는 장점을 가져 더 안전한 암호화 알고리즘으로 간주된다.



RSA 알고리즘을 통해 메시지를 암호화하고 복호화하는 방법은 다음과 같다.

1. 주어진 두 소수를 사용하여 공개키와 비밀키를 설정한다.
   1. 두 개의 임의의 큰 소수 와 를 선택한다.
   2. 공개키는 로 정한다. 여기서 이고 는 과 서로 소의 관계에 있는, 즉 gcd() = 1인 임의의 숫자를 로 잡는다. 일반적으로 3이나 5 정도의 값을 잡을 수 있다.
   3. 비밀키는 의 역수가 되는 값 즉 에 대해

의 관계를 가지는 값 를 찾아 비밀키로 잡는다. 여기서 비밀키의 (혹시 d?)는 지난 실습에 구현하였던 확장 유클리드 알고리즘에 의해 찾을 수 있다.

1. 단계1에서 찾은 공개키를 사용하여 문자열을 암호화한다.
   1. 문자열의 문자 각각에 대해서 (각각의 문자를 ch라고 할 경우) mod N을 계산하여 암호화한 후 저장한다.
2. 단계 1에서 찾은 비밀키를 사용하여 문자열을 복호한다.
   1. 암호화된 문자열의 문자 각각에 대해서 (각각의 문자를 이라고 할 경우) 을 계산하여 암호화한 후 저장한다.

위 알고리즘을 참고하고 아래의 예제 코드를 활용하여 주어진 메시지를 RSA알고리즘을 사용하여 암호화, 복호화하는 프로그램을 구현할 수 있다.

다음은 위 알고리즘을 구현한 예제코드이다. 아래를 참고하여 구현하도록 하라.

**예제 코드)**

#**define** MESSAGE\_LENGTH 35

**char** message[] = {'H','e','l','l','o',',',' ','P','l','e','a','s','e',

' ','l','o','v','e',' ','W','o','o','n','g','s','u','p','!','!',

'!','\0'};

// Hello, Please, love Woongsup! 에 대한 문자열 정의

**unsigned** **int** encryption[MESSAGE\_LENGTH];

// 암호화된 문자들은 정수형 배열로 선언,저장

**char** decryption[MESSAGE\_LENGTH];

// 복호화된 문자들은 문자형 배열로 선언, 저장

...

**struct** \_*node {*

*// extended*\_Euclid 함수 사용을 위한 구조체

**int** first;

**int** second;

**int** third;

};

// ckey mod N 값을 구한다.

// 아래함수의 매개변수 key 값은 암호화할 때는 공개키 (e,N)의

e 값으로 하고 할 때는 비밀키 (d, N)의 d값으로 한다.

**unsigned** **int** do\_exp(**int** c, **int** key, **int** N){

// do\_exp()는 ckey mod N 해준 값을 리턴한다.

// 단 c를 key 번 곱하게 되면 그 값이 정수형으로 감당할 수 없을 정도로 커지므로

// c를 곱해줄 때 마다 mod 연산 (%연산)을 구행하여 그 값을 충분히 작은 값으로

// 유지시킬 필요가 있다. 물론 수업시간에 배운 내용을 적용하여 ckey mod N 을 구할

// 수도 있다.

**return** prod; // ckey mod N을 리턴

}

// encryption 배열은 정수형으로 되어 있으므로 아래 함수를 사용하여 출력하도록 한다.

**void** print\_encryption(**int** e[]) {

**for** (**int** i = 0; i < MESSAGE\_LENGTH; i++)

printf("%d", e[i]);

printf("\n");

}

**void** main(void){

...

1. 주어진 p, q, e 값으로 extended\_euclid함수를 사용하여 비밀키 d를 얻는다.
2. message의 문자들을 한자 씩 읽는어 읽은 문자들을 암호화한다.
3. 읽은 문자를 문자 변수 ch에 할당한다.
4. c = (unsigned int) ch; // ch를 정수형으로 변환한다.
5. c를 public key에 따라 암호화(do\_exp(c, e, N)를 사용권장)한 후 이를 encryption[i]에 저장한다.
6. print\_encryption()함수를 사용하여 암호화된 정수배열 encryption의 내용을 출력한다.
7. 배열 enctyption의 숫자들을 하나씩 읽는다.
8. 읽은 숫자를 정수 변수 c에 할당한다.
9. c를 private key에 따라 복호화 (do\_exp(c, d, N)를 사용) 한 후, 이를 decryption[i]에 하나씩 저장한다. 단 decryption의 경우 문자형 배열이므로 형변환후 저장한다. (예, decryption[i] = (char)do\_exp(...);)
10. 복호화된 문자열 decryption의 내용을 출력한다.

}

**제출방법**

* 보고서 작성방법: 실습문제 번호별로 결과가 나온 화면의 내용을

캡쳐하여 보고서에 붙여 놓는다.

* 소스코드의 파일이름에 연습문제 번호를 붙이는 것을 잊지 않는다. 예) ex-1.c, ex-2.c
* 결과 보고서에 이름과 작성 날짜를 기입하는 것을 잊지 않는다. 예) 김웅섭\_2020\_09\_01.doc
* 실행결과를 보고서에 작성하여 소스코드와 함께 제출한다.
* 제출 마감 : e-class 제출 마감시간까지