課 題 情 報 シ ー ト

テ ー マ 名 ：	公開鍵暗号の実装				
担当指導員名：	奥秋　清次		実施年度：	28 年度	
施　設　名　：	関東職業能力開発大学校附属千葉職業能力開発短期大学校				
課　程　名　：	専門課程	訓練科名：	電子情報技術科		
課題の区分：	総合制作実習	学生数：	1	時間：	22 単位（396h）

課 題 制 作・開 発 の ポ イ ン ト

【開発（制作）のポイント】

現在、インターネットは社会のインフラとして必要不可欠です。しかし、インターネットは不特定多数のユーザが利用するため、個人情報が流出するなど社会問題が発生しています。個人情報の流出を防ぐためには、コンテンツを秘匿できる暗号技術が有効です。本総合制作では、暗号技術の最も基本的な RSA 暗号の理論を学び、実用的な鍵長で実装することにより、暗号技術を深く理解します。

【訓練（指導）のポイント】

附属短大、能開大の学生は、暗号技術の基礎である整数論、群論を習っていません。しかし、具体的な数値例を用いて説明すると、学生も良く理解できます。また、実用的な鍵長で暗号を実装するためには、多倍長演算ライブラリが必要ですが、C 言語のプログラミングが理解できていれば、問題なく学生にも作成できます。暗号技術をブラックボックスとせず、内容を理解することにより応用力が身に付きます。

学生への指導は、RSA 暗号を易しく解説した資料を渡し、学生に自ら理解してもらいます。理解が正しいかどうか、ゼミ形式でチェックします。理論が理解できたら、多倍長演算ライブラリを Linux®にインストールし、簡単なサンプルプログラムを渡します。学生はそのサンプルプログラムを応用して RSA 暗号を実装します。

課 題 に 関 す る 問 い 合 わ せ 先

施 設 名　：　関東職業能力開発大学校附属千葉職業能力開発短期大学校
住　　所　：　〒260-0025　千葉県千葉市中央区問屋町 2-25
電話番号　：　043-242-4166（代表）
施設 Web アドレス　：　http://www3.jeed.or.jp/chiba/college/

課 題 制 作・開 発 の「予 稿 」および「テーマ設 定 シート」

次のページ以降に、本課題の「予稿」および「テーマ設定シート」を掲載しています。

RSA 暗号の実装

担当教員：奥秋　清次

１．はじめに

近年,ウェブサーバーに対する不正アクセスにより,個人情報が流出する事件が発生している.個人情報が流出すると,第三者がその情報をもとに悪用し,知らないうちに犯罪に巻き込まれる場合もある.不正アクセスを防ぐためには,ファイアウォールによるアクセス制御,コンテンツを秘匿する暗号が有効である.公開鍵暗号とは,暗号化と復号に異なる鍵を用い,公開鍵で暗号化し,秘密鍵で復号する.

公開鍵暗号には代表的な方法とし Rivest,Shamir、Adleman という 3 人の研究者の頭文字をとった RSA と呼ばれる暗号がある.

本総合制作では,RSA 暗号の仕組みを理解し,RSA 暗号を実装する.

２．RSA 暗号の仕組み

RSA 暗号は素因数分解問題を用いた暗号である.大きな素数を p,q とし,その積を n とする. n が与えられても,その素因数 p,q を求める事は難しい.よって,コンピュータを用いても桁数が大きければ計算に時間がかかり,素因数を求めることができない.

また,RSA 暗号は２つの公開鍵と対となる１つの秘密鍵を必要とする.送信者は公開鍵で暗号文を作り,受信者は秘密鍵で復号する.暗号化する前のメッセージを平文 M ,暗号文を C とし,公開鍵を e,n 秘密鍵を d とする.公開鍵,秘密鍵は,以下の条件を満たす必要がある.

$$n = pq\ ,\ ed \equiv 1(\mathrm{mod}\, L)\ ,\ L = LCM(p-1, q-1)$$

暗号化は式(1),復号は式(2)である.

$$C = M^e \bmod n \quad \cdots (1)$$

$$M = C^d \bmod n \quad \cdots (2)$$

３．実装方法

実用的な RSA 暗号を作るために,多倍長演算ライブラリ GMP を用いる.GMP とは GNU Multiple Precision Library のことで,非常に大きい整数を扱うことができる算術ライブラリである.現在,鍵ｎが 1024bit あれば安全とされているので,今回はｐ,ｑを 512bit とする.鍵の生成アルゴリズムは以下の通りである.

3.1　公開鍵ｎの生成

512bit の素数ｐ,ｑをつくるプログラムは以下のとおりである.ただし、変数の宣言、初期化は省略する。

```
int GeneratePrime(mpz_t p,gmp_randstate_t state)
{
    for (i = 0 ; i < 1000 ; i++) {
        mpz_urandomb(P,state,512);
        result = mpz_probab_prime_p(P,15);
        if(result == 1 || result == 2){
            return OK;
        }
    }
    return NG;
}
```

この関数GeneratePrimeは,乱数を生成させp,ｑが素数かどうかを判定する.乱数は,mpz_urandombで生成し,素数判定はmpz_probab_prime_pを用いる.実行する度,異なる乱数系列にする為に,stateにシード値として現在時刻を与える.素数が生成するまでこの処理を繰り返す.公開鍵ｎは,生成したp,ｑの乗算であるのでmpz_mul(n,p,q)で計算する.

3.2　公開鍵eと秘密鍵dの生成

公開鍵eを作る為,Lを作成する.Lはｐ-1とｑ-1の最小公倍数なので,mpz_lcm(L,p_1,q_1)を用いる.公開鍵eと秘密鍵dを生成するプログラムは以下のとおりである.

```
int CreateKeys(mpz_t n,mpz_t e,mpz_t d)
{
    mpz_sub_ui( p_1, p,1L);
    mpz_sub_ui( q_1, q,1L);
    mpz_lcm(L ,p_1, q_1);
    for (i = 0 ; i < 1000 ; i++) {
        mpz_urandomb(E,state,512);
        mpz_gcd(gcd, E, L);
        result = mpz_cmp_ui(gcd , 1L );
        if(result == 0) {
            mpz_invert( d, E, L);;
            mpz_mul(n, p, q);
            mpz_set(e,E);
            return OK;
        }
    }
    return NG;
}
```

eとLが互いに素となる大きいランダムな素数を作る為に,eとLの最大公約数をmpz_gcdで求め,その

値が1であるかをmpz_cmp_uiで判定する.eが生成するまでこの処理を繰り返す. d はeの逆数なのでmpz_invert(d,e,L)を用いて計算する.

3.3　暗号化と復号

暗号化と復号は,べき乗を計算する関数でmpz_powmを用いる.

暗号化の場合

```
mpz_powm(C ,M ,e ,n);
```

復号の場合

```
mpz_powm(M2 ,C ,d ,n);
```

である.

3.4　文字列を整数に変換

文字列を大きな整数 N に変換する.os2ip は,文字列 s,文字列の長さ len を受け取り大きな整数 N に変換する.

```
void os2ip(mpz_t N,char s[],int len)
{
        for(i = 1;i <= len;i++){
        mpz_ui_pow_ui(exp,256L,(unsigned long)(len-i));
        mpz_mul_ui(tmp,exp,(unsigned long)s[i-1]);
        mpz_add(N,N,tmp);
        }
}
```

入力された文字数をlenとする.1文字は8bitなので,8bitを1つの箱とする.Mを256進数で表すとlenの数だけ箱ができる.最下位bitから最上位bitに向けて文字を整数値として配置する.mpz_ui_pow_uiで256進数の箱をlneの数だけつくる.mpz_mul_uiで,できた箱に入力した文字を順番通りに入れる.そしてmpz_addを用いて,1つの大きな整数Nに変換する.

3.5　数字を文字列に変換

大きな整数 N を文字列に変換する.i2osp は,大きな整数 N を受け取り文字列の長さ len の文字列 s に変換する.

```
void i2osp(char s[],mpz_t N,int len)
{
        for(i = len-1;i >= 0;i--){
                mpz_fdiv_qr(q,r,N,BASE);
                mpz_set(N,q);
        s[i] = (char)mpz_get_ui(r);
        }
}
```

M を 256 で割ることにより,商と余りを計算し,余りを最下位の箱に格納する.その商をまた 256 で割ることにより,次の下位の箱に格納する値が求まる.この処理を len 回繰り返す.

mpz_fdiv_qrで,Nから商 q と余り r を求める.この r は,文字列の1文字に相当する.mpz_setで,次の文字を求める為に,N に q を代入する.mpz_get_uiにより多倍長の整数をlong型の整数に変換する.この処理をlen回繰り返す.

４．結果

平文を msg とし,msg を数で表した値を M1 とする.M1 を暗号化した値を C とし,C を復号した値を M2 とする.そして M2 を文字に表したものを dmsg とする.結果は以下の通りである.

```
msg = Sougou Seisaku!

M1 = 43322128843111008827198503117307625 7

C = 37280419346888064782405332867545866427963431188155 9
    74438086525011884409871899191241626842953066850955 0
    21235579257246407707042521939274211853267001728022 4
    23731174636626212182491063074449353088833763193804 9
    85745694190885789349599641573264288373166401477612 3
    73468975531928493028450689825760028352148930937913553

M2 = 43322128843111008827198503117307625 7

dmsg = Sougou Seisaku!
```

実際に復号することができた.

５．まとめ

RSA 暗号を実用的な鍵長 1024bit で実装することができた.オイラーの定理,フェルマーの小定理,Euclid の互除法について学び,RSA 暗号の仕組みを理解した.

参考文献

[1] D,R.Stinson,CRYPTOGRAPHY Teheory and Practice,Chapman&Hall/CRC,2006

[2」The GNU Multiple Precison Arithmrtic Library Edition6.1.1

[3] Jonsson&Kaliski,RSA Cryptography specifications,February 2003

課題実習「テーマ設定シート」

科名：　　電子情報技術科

教科の科目	実習テーマ名	
総合制作実習	RSA 暗号の実装	
担当教員	担当学生	
電子情報技術科　奥秋　清次		

課題実習の技能･技術習得目標

公開鍵暗号の代表的な方式である RSA 暗号を理論から学習し、実用的な鍵長で実装します。

実習テーマの設定背景･取組目標

実習テーマの設定背景

現在、インターネットは社会のインフラとして必要不可欠です。しかし、インターネットは不特定多数のユーザが利用するため、個人情報が流出するなど社会問題が発生しています。個人情報の流出を防ぐためには、コンテンツを秘匿できる暗号技術が有効です。本総合制作では、公開鍵暗号の最も基本的な RSA 暗号の理論を学び、実用的な鍵長で実装することにより、暗号技術を深く理解します。

実習テーマの特徴･概要

附属短大、能開大の学生は、暗号技術の基礎となっている整数論、群論を習っていません。しかし、具体的な数値例を用いて説明すると、学生も良く理解できます。また、実用的な鍵長で実装するためには、多倍長演算ライブラリが必要ですが、C 言語のプログラミングが理解できていれば、問題なく学生にも作成できます。暗号技術をブラックボックスとせず、内容を理解することにより応用力が身に付きます。

No	取組目標
①	公開鍵暗号と共通鍵暗号について違いを理解します。
②	RSA 暗号の理論を理解します。
③	Linux と多倍長演算ライブラリをインストールします。
④	Linux のシステム管理について習得します。
⑤	サンプルプログラムにより多倍長演算ライブラリの使用方法をを習得します。
⑥	RSA 暗号のプログラムを作成します。
⑦	文字列と数値を変換する手法を理解し、プログラムを作成します。
⑧	報告書の作成、パネル展示・発表会を行います。
⑨	５Ｓ(整理・整頓・清掃・清潔・躾)の実現に努め、安全衛生活動を行います。
⑩	