

ソフトウェアの名称 : Protected Communication System (ECcrypt)

1. ソフトの概要

Journal of Applied Sciences 5 (4): 604-633, 2005

ISSN 1812-5654

© 2005 Asian Network for Scientific Information

Theory and Implementation of Elliptic Curve Cryptography

Kefa Rabah

Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, via Mersin 10, Turkey

での方針に従って楕円曲線暗号でファイル全体を暗号化するものを実装してみました。
速度は、カタツムリくらいですが、もう少し速くなったら、“メールもビットマ”、“Cipher Web Mail”のセットに加えます。

貿易管理令での制限については、鍵の長さを短くするか、ソースコードを公開するかのどちらかが必要です。
HP でソースコードを公開するほうを選びました。

2. 作者への連絡先(メールアドレス、ホームページ)

メールアドレス : uyama33@yahoo.co.jp (宇山 靖政)

ホームページ : <http://uyama22.pa.land.to/> (ソースコード)

3. 取り扱い種別(フリーウェア)

(実行形式のファイルはフリーですが、ソースコードの著作権を主張します。複製の作成は許可しません。)

4. 動作環境

Windows Vista Home Premium 32 ビット

Windows 7 Home Premium 64 ビット

の上で動きます。

5. 別途必要なソフト : 特になし (暗号ソフトとして単独で動きます。メール機能はありません。)

6. インストール・アンインストール方法

インストール : EccPac.zip を解凍すると、このマニュアルの他に、EccSys.zip (暗号ソフトと関連するフォルダ、ファイル) が現れます。

さらに、EccSys.zip を解凍すると、“EccSys” フォルダが出来ます。このフォルダをデスクトップ等の適当な場所に置き、その中にある

“ECcrypt.exe” へのショートカットを作成してください。

7. アンインストール : 作成したショートカットと、フォルダを削除してください。

ECcrypt.exe について。

使い方：



通信の仕方は次のようになります。

アリスの作業

1. 素数 p のビット数を決定する。192,244,256,384,521 ビットから選ぶ。
2. 鍵を作る ボタンをクリックする。
3. 公開鍵、秘密鍵の名前、 Ao^{***} , As^{***} を決める。
4. 鍵を保存して終了する。

注意：

現在は、素数のビット数を選ぶと、楕円曲線のパラメータ $T = (p, a, b, G, n, h)$ が1組決まります。
秘密の値 m は乱数として決定されます。 m の値は、113 ビットから 392 ビットの間に設定しました。
この値 m は秘密にしておきます。

5. 相手 (ボブ) に、 (T, mG) を送る。(これが公開鍵)

ボブの作業

1. アリスから送られた公開鍵を読み込む。これで素数 p のビット数が決まる。

- 1 1. ファイルの先頭から、**kG** を取り出す。
- 1 2. 自分の持っている値 **m** を使って、**mkG** を計算する。
- 1 3. ファイルの残りの各ブロックに対して、 $(P + kmG) - mkG = P$ を計算する。
- 1 4. **P** の x 座標 (**X1+α**) を取りだして、 $X1 = (X1 + \alpha) - \alpha$ を計算して並べる。

必要となるもの

1. 多倍長整数の計算
2. ヤコビ記号の計算
3. 平方根の計算
4. 楕円曲線上の点の k 倍の計算

楕円曲線暗号を利用した公開鍵暗号のソフトです。“メールもビットマ”、“Cipher Web Mail”における共通鍵の交換のために作成しました。パラメーターに関しては、

Standards for Efficient Cryptography

SEC 2: Recommended Elliptic Curve Domain Parameters

Certicom Research

Contact: Daniel R. L. Brown (dbrown@certicom.com)

January 27, 2010

にある値を利用しました。

GF_p での p の値は、192 ビットから、521 ビットの間です。 k および m の値は、113 ビットから 392 ビットの間に設定しました。

ファイル全体を暗号化出来ませんが、とても時間がかかります。RSA 暗号が速く見えるほどです。したがって、対称鍵の暗号化にしか利用できません。もちろん貿易管理令に違反しないようにソースコードを HP で公開します。

多倍長整数の計算は、複素数の配列と多倍長整数の変換を適宜行う方法で全体を扱っています。さらに、3通りの乗法（複素数の普通の乗法、DFT による乗法、FFT による乗法）を用意して、扱う数の大きさによって切り替えて計算しています。除法と剰余は自分で考えた方法で計算しています。

ヤコビ記号の計算と平方根の計算、素数生成、最大公約数と逆数の計算は Menezes の Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) にあった方法を少し変形して使っています。べき乗計算は FFT を主に利用しています。

全体的な流れは、

Journal of Applied Sciences 5 (4): 604-633, 2005

ISSN 1812-5654

© 2005 Asian Network for Scientific Information

Theory and Implementation of Elliptic Curve Cryptography

Kefa Rabah

Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, via Mersin 10, Turkey

に沿って作成しました。ご指導いただいたことを感謝しております。

このソースコードについては、著作権を主張します。技術内容を公知の技術にするために、HP でソースファイルを公開します。