所属実験室	計算機システム	指導教員	佐藤 寿倫
学籍番号	TL081328	氏　名	宇栄原 佑
論文題目	Android 用暗号化アプリケーションの検討		

1. 序論

最近では Android や iPhone などのスマートフォンが普及している。スマートフォンは従来の携帯電話と比較して、インターネットも見やすく、PC メールを送受信できるなどの機能も実装されており、インターネットへのアクセスも盛んになっている。こうした高機能化が進み、スマートフォンがビジネスツールとして活用され、業務端末の役割も果たすようになった今、情報の漏洩や流出などの危険性に厳重に対処する必要がある。その対策の一つとして暗号化を取り上げる。

2. スマートフォンとセキュリティ

暗号化とは第三者に通信内容を知られないように行う特殊な通信（秘匿通信）方法のうち、通信文を見ても特別な知識なしでは読めないように変換する表記法（変換アルゴリズム）のことである。暗号化には、暗号化と復号に同じ鍵を使う共通鍵暗号と、異なる 2 つの鍵を使う公開鍵暗号があり、本論文のアプリケーション開発では、公開鍵暗号の代表的な方式の一つである RSA 暗号方式を用いる。

3. RSA 暗号方式

RSA 暗号方式は現在ではもっとも安全性の高い暗号方式の一つで、素因数分解の難解さに安全性を依存している。現在最良の素因数分解アルゴリズムとされている数体ふるい法でも、大きな 2 つの因数をもつ数の素因数分解を解読するには天文学的な時間を要する[1]。素因数分解アルゴリズムの効率化には、高性能の超並列演算コンピュータを開発して計算速度を速める他ない。

4. 暗号化アプリケーション

Java には暗号認証機能を実装するための Java Security パッケージがある。Java Security パッケージには鍵ペア生成や暗号化を行う際に必要なクラスが用意されている。これらのクラスに独自の仕様を持たせたサブクラスを組み込むことで、RSA 暗号方式を実現し、入力された文字列を公開鍵で暗号化、秘密鍵(個人鍵)で復号するプログラムを作成した。

5. Android アプリケーション

統合開発環境は Eclipse を使用し、JDK(Java 開発キット)、ADT(Android 開発ツール)、Android SDK(ソフトウェア開発キット)をインストールする。開発言語には Java を用いる。4 章で作成した暗号化プログラムを Android 用アプリケーションとして開発した[2]。

6. まとめ

本研究では、Android 用暗号化アプリケーションを開発し、エミュレータ上で動作確認まで行った。今後は Android 上での暗号化アプリケーションの動作確認、Android 同士の端末間での暗号化通信を課題とする。

参考文献

[1]安生 真, “初歩からわかる Android 最新プログラミング”, 株式会社インプレスジャパン, 2010.

[2]鳥居 直哉, “素因数分解の困難性に基づく暗号の技術的評価に関する研究開発”, 2006.