3G－1

AES暗号方式を用いた安全なWEBアクセス —iアプリ対応携帯電話への適用—*

陳　志松† 山本雅基† 矢尻えみ子†† 西尾晴久††† 神保雅一††
†(株)デンソークリエイト ††慶応義塾大学理工学部数理科学科 †††(財)ソフトピアジャパン

1. はじめに

2001年2月にアメリカ国立標準技術研究所(NIST)は、新しい共通暗号方式AESのDraft FIPS(Federal Information Processing Standard)を発表した。AESは近くFIPSとなる予定である。一方、近年携帯電話が急激に普及し、携帯電話からWEBへのアクセスが可能になった。iアプリと呼ばれるJavaアプリケーションを実行できる携帯電話も登場し、WEBサーバとの間の通信が可能になり、注目を集めている。

本研究では、AES暗号のi-アプリ対応携帯電話への実装を試み、i-アプリのファイルサイズの制限以内で暗号アルゴリズムの実装が可能であることを確認した。また、作成した暗号化クラスを利用し、iアプリ対応携帯電話からWEB上のテストページへのアクセスを行い、暗号化データ送受信が可能であることが分かった。

2. AES暗号の仕様

AESはブロック暗号である。ブロック長は128bitで、鍵長は128bit、192bit、256bitの3種類。ブロックは4×4のbyte(8bit)単位の正方行列、鍵は4×Nk (Nk=4,6,8)の長方形行列としてそれぞれ表現される。暗号化（復号化）はラウンド変換と呼ばれている一連の変換を複数のラウンドに渡って繰り返すことによって行われる。ラウンド数Nrは鍵長によって決められている。

表1 ラウンド数と鍵長

Nk	4	6	8
Nr	10	12	14

ラウンド変換は以下の4つの変換からなる：ByteSub変換、ShiftRow変換、MixColumn変換、そしてRoundKeyAddition変換。以下、これらの変換の詳細及び暗号化の手順について述べる。

2.1 ByteSub変換：

ByteSub変換は、ブロック内の各単位に対して以下の計算を行なう：

i. $GF(2^8)$における乗法的逆元を計算。（乗算は多項式の積を$x^8+x^4+x^3+x+1$でmodをとる）

ii. 上記結果に、各bitに以下のアフィン変換を行う。

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

2.2 ShiftRow変換：

下表に示したオフセット値に従って、ブロック内の各行に対して循環左シフトを行う。

表2 ShiftRow変換のオフセット値

	1行目	2行目	3行目	4行目
オフセット	0	1	2	3

2.3 MixColumn変換：

ブロック内の各列に対して、$GF(2^8)$において、各単位を係数とする多項式と下記の多項式$c(x)$との乗算を行い、その積をx^4+1でmodをとる：

$$c(x)='03'x^3+'01'x^2+'01'x+'02'$$

得られた多項式の係数を対応する単位の値とする。

2.4 RoundKeyAddition変換：

ブロック内の各単位に対して、ラウンドキーとのEXORをとる。ラウンドキーは鍵拡張アルゴリズム

---

* Safety WEB Access Using AES Code System: Apply to i-application Correspondence Cellular Phones.

†Zhisong Chen, †Masaki Yamamoto, ††Emiko Yajiri, †††Haruhisa Nishio, ††Masakazu Jimbo
†Denso Create Inc., ††Faculty of Science and Technology, Keio University, †††Softpia Japan

によって鍵を拡張し、拡張した鍵を順番に128bitずつ切り出すことによって得られる。

2.5 暗号化／復号化の手順

平文の暗号化は以下の手順で行われる：

i. RoundKeyAddition 変換。

ii. Nr-1 回ラウンド変換。

iii. MixColumn 変換なしのラウンド変換を1回行う。

暗文の復号化は平文の暗号化と逆の手順で行われる。

3. i-mode の Java 仕様

携帯電話で動作する Java の仕様では、Java2 Platform, Micro Edition の CLDC(Connected Device Configuration)を採用している。CLDC には、さらに動作する機器の特性や用途に応じた API が追加される。MIDP(Mobile Information Device Profile)は、サン・マイクロシステムズを中心に、世界各国の電話会社によって規定された、携帯電話向けの追加 API である。NTT ドコモは、MIDP に相当する追加 API を i-mode 用に提供しており、その仕様書は公開されている。

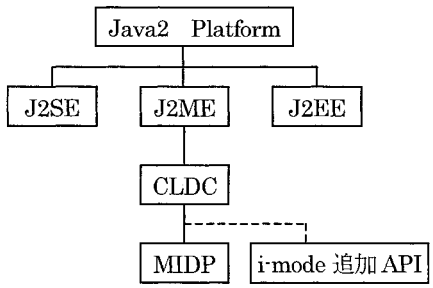


図 1 i-mode で動く Java の位置付け

i-mode 対応 Java には、セキュリティ上の配慮などの理由から、種々の制約事項がある。いくつかを列挙すると、以下のようなものがある：

i. 同時に起動できる i アプリは1つだけ。

ii. i アプリで利用できるデータ通信プロトコルは HTTP もしくは HTTPS のみ。

iii. ダウンロード元のサーバとしか通信できない。

iv. アプリケーションは Jar ファイルで 10KB 以内。

4. AES 暗号の実装

本研究では、AES アルゴリズムの検証と i-mode 携帯電話における動作を確認するために、i-アプリで実装を行った。

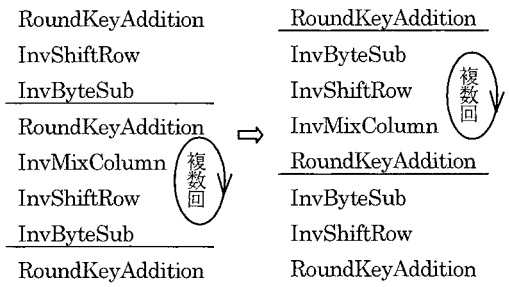
i-mode 対応 Java の制限事項を踏まえて、実装では、以下の設計方針を定めた：

i. 暗号化（復号化）はルックアップテーブルを使用

AES では、暗号化（復号化）は、ラウンド変換と呼ばれている変換を繰り返し使う。ラウンド変換は、ByteSub 変換、ShiftRow 変換、MixColumn 変換と RoundKeyAddition 変換からなる。各変換の処理単位は、単位(byte)から列、行までそれぞれ異なる。実装では、ラウンド変換の処理単位を32bit にし、4つのルックアップテーブルを引くことと4回の EXOR で暗号化（復号化）を行う。

ii. 復号化を暗号化と同じ手順で処理する

AES では、復号化は暗号化と逆の手順で処理を行う。以下のように復号化の手順を変えることによって、復号化は暗号化と同じ手順で処理することができる。このとき、ラウンドキーはそれに応じて変更する必要がある。



実装した結果、AES 暗号クラスを Jar ファイルに圧縮すると 2.4KB になり、i-mode に規定されている 10KB サイズより小さい。作成した AES 暗号クラスを利用して、携帯電話から慶応大学の就職 DB へアクセスするアプリケーションを開発し、送信データの暗号化及び受信データの復号化を実現した。

5. 今後の課題

今回は AES 暗号を実装してみたが、鍵配送問題が解決しなければ、実用的ではない。今後は、公開鍵暗号 RSA を i-mode に実装し、AES 暗号とあわせて、実用的な暗号化データ送受信を実現したいと考えている。

参考文献

[1]藤原良, 神保雅一：符号と暗号の数理（情報数学基礎講座），共立出版（1994）

[2]Joan Daemen：AES Proposal：Rijndael, http ://www.esat.kuleuven.ac.be/~rijmen/ （1999）

[3]Sun Microsystems,Inc: Java2 SDK Document Ver1.3