# 스마트폰을 위한 모바일 데이터 암호화 기능 구현

## Implementation of Mobile Data Encryption Technique for Smart Phones

진영훈*, 김재양*, 한상훈*, 이소희*, 최준석*, 추영열*
동명대학교*

Jin Young-hoon*, Kim Jae-yang*, Han Sang-hoon*
Lee So-hui*, Choi Jun-seok*, Choo Young-yeol*
Tongmyong University*

요약

스마트폰 보급의 증가로 인해 모바일 환경의 보안이 중요한 이슈로 부각되고 있으며 이에 본 논문에서는 스마트폰 환경에 적합한 암호화 알고리즘을 기존 암호화 기법들의 성능 비교를 통해 제시하고자 한다.

## Ⅰ. 서론

최근 스마트폰의 급격한 확산은 사회전반에 패러다임을 변화시키고 있다. 특히 누구나 개발하고 사용할 수 있는 어플리케이션으로 인해 금융, 교육, 교통, 의료등의 산업 간의 융합이 촉진되어 새로운 IT 혁명을 유도하고 있다. 하지만 이러한 팽창에 따른 보안에 대한 대비책은 미비한 실정이며 이는 스마트폰을 통한 기존 구축된 사회적 IT 인프라의 정보 유출과 같은 문제점을 야기한다. 따라서 이러한 문제점들을 해결하기 위한 백신 등의 보안 솔루션들에 대한 많은 연구가 진행되고 있으며 이를 견인할 보안정책의 중요성이 부각되고 있지만 현재 어플리케이션에서의 암호화 방식은 SSL(Secure Socket Layer)에 치중되어 있다. 이러한 배경에서 본 논문에서는 스마트폰을 통한 정보유출을 방지하기 위한 보안 솔루션으로써 필수적인 암호화 알고리즘에 대해 언급한다. 또한 기존 성능이 증명된 RC5, AES-128, SEED의 암복호화 속도 비교를 통하여 스마트폰에 적합한 암호화 알고리즘을 제시한다.

본 논문은 서론에 이어 2장에서 관련 암호화 알고리즘에 대해 알아보고, 3장에서 암호화 알고리즘을 적용하여 시뮬레이션 한다. 이어서 분석된 결과를 4장에서 설명하고, 5장에서 결론을 맺는다.

## Ⅱ. 관련연구

본장에서는 스마트폰 환경에 적용하기 위한 암호화 알고리즘과 암호화모드에 대해 간단히 알아보고자 한다.

### 1. RC-5

RC-5는 다양한 크기의 키, 블록, 라운드를 적용가능하며, 이를 입력으로 사용할 수 있는 알고리즘이다. 블록의 크기는 32, 64, 128bit를 사용 가능하며 키의 크기는 0~2040bit까지 가변적이다. 라운드 역시 0~255 까지 가변적임에 따라 암호화 강도와 속도를 조정 가능하며 이를 통한 성능과 안전성을 환경에 적절하게 적용하여 사용할 수 있는 장점을 가진다.

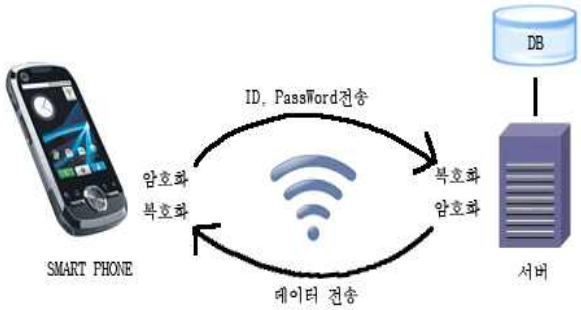
### 2. AES-128

미국 정보 표준으로 지정된 블록 암호 형식으로 128bit가 미국 표준으로써 사용되고 있다. AES에서 사용하는 구체적인 알고리즘은 Rijndael 알고리즘이며, 정보를 암호화 및 해독할 수 있는 대칭적 블록 암호이다. 블록 크기는 128, 192, 256bit이며, 키의 크기도 역시 128, 192, 256bit이다.

### 3. SEED

한국정보보호진흥원의 기술진이 개발한 블록 암호화 방식으로 미국에서 수출되는 웹브라우저 보안 수준이 40bit로 제한됨에 따라 128bit 보안을 위해 별도로 개발된 알고리즘이다. 전자상거래, e-mail, 인터넷 뱅킹, 데이터 저장, VPN, 지적재산권 보호 등 다양한 분야에서 사용되고 있으나 SEED기반 보안 프로그램은 ActiveX Plug-in으로 배포될 수밖에 없는 단점을 가지며 공인인증서와 함께 대한민국의 웹 호환성 문제와 가장 밀접하게 연관되어 있다[1,2].

## Ⅲ. 시스템 구성




▶▶ 그림 1. 시스템 구성

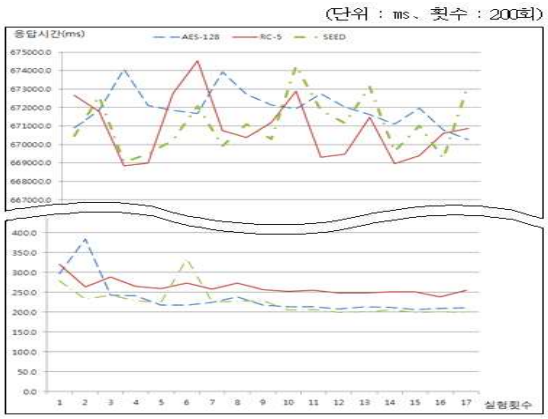
그림 1은 스마트폰과 서버간에 Wi-Fi를 통한 암복호화 시스템 구성도이다.

## Ⅳ. 시뮬레이션 결과분석

### 1. 시뮬레이션 환경 및 결과분석

표 1. 시뮬레이션 환경[3]

| 변인 | 구분 | 내용 |
|---|---|---|
| 통제변인 | CPU | AMD ATHLON ii x4 630 Processor 2.80㎓ |
| | RAM | 2.00G |
| | OS | Windows7 Professional K |
| | Eclipse ver. | eclipse Helios |
| | Key 길이 | 128bit |
| | 블록 크기 | 128bit |
| | 암호모드 | CBC모드 |
| | 패딩기법 | PKCS#5padding |
| 종속변인 | IV | abcdefghijklmnop |
| | Key | What time is it? |
| | 평문 | android android |




▶▶ 그림 2. 암복호화 측정 결과

그림 2는 200개의 암복호화 측정 결과를 가지고 10개씩의 평균값을 구해, 20개의 값을 그래프로 나타낸 것이다.

## Ⅴ. 실험결과

표 2. 실험결과

| 구분 | 종류 | 속도(ms) |
|---|---|---|
| 암호화 | AES-128 | 671,978 |
| | RC5 | 670,934 |
| | SEED | 671,119 |
| 복호화 | AES-128 | 3,598 |
| | RC5 | 3,668 |
| | SEED | 3,584 |

측정결과는 암호화 평균속도는 RC5가 가장 우수하였으며, 복호화 평균속도는 SEED가 가장 우수하였다. 그리고 가장 평균적인 값을 가진 암호화 알고리즘은 AES-128인걸로 결과가 나왔다.

## Ⅵ. 결론

스마트폰을 통한 무선 네트워크 어플리케이션의 사용이 증가되고 있음에 따라 스마트폰 환경의 보안이 이슈로 부각되고 있다. 이에 본 논문은 스마트폰 환경에 적합한 암호화알고리즘을 제시하기 위해 AES-128과 RC5, SEED 암호화 알고리즘을 구현하여 각각의 알고리즘들의 성능을 비교하였다. 암호화 평균속도는 RC5가, 복호화 평균속도는 SEED가 우수하였다. 하지만 3가지 알고리즘 모두 암복호화의 성능 차이가 크지 않았다. 향후 연구에서는 암복호화가 적용된 스마트폰 시스템을 구성하여 다양한 외부공격 환경에 대한 실험이 필요할 것이다.

본 연구는 부산테크노파트 산학공동기술혁신사업(2010B030) 지원으로 수행되었음.

## ■ 참 고 문 헌 ■

[1] http://seed.kisa.or.kr/kor/seed/seedInfo.jsp
[2] William Stallings, "Network Security Essentials 3rd", SciTech, 2007
[3] Deepika Mulani, "HOW SMART IS YOUR ANDROID SMARTPHONE?", San José State University, 2010.