Using SEED Cipher Algorithm with SRTP

Seokung Yoon (KISA)

Goal / Motivation

- Goal : The SEED cipher algorithm would be the default cipher together with AES in SRTP

- Motivation
  - In Korea, many companies provide VoIP service and we predict the VoIP market could grow to as much as $10 billion by the year 2009
  - Our agency developed a VoIP phone to support secure communications for user privacy, and adopted SRTP for confidentiality to the RTP traffic
  - We add two algorithms for multimedia data encryption
    - AES – default cipher in SRTP and SEED – national standard
  - The SEED cipher algorithm is a national industrial association standard and is widely used in South Korea for electronic commerce and financial services that are operated on wired and wireless communications.

The SEED Cipher Algorithm (1/2)

- developed by KISA in 1999
- Standard status

  - TTA Standard in Korea
    - ✓ TTAS.KO-12.0004, “128-bit Symmetric Block Cipher (SEED)”
  - IETF Standard
    - ✓ RFC 4269, The SEED Encryption Algorithm
    - ✓ RFC 4010, Use of the SEED Encryption Algorithm in CMS
    - ✓ RFC 4162, Addition of SEED Cipher Suites to TLS
    - ✓ RFC 4196, The SEED Cipher Algorithm and Its Use with IPSec
  - ISO/IEC Standard
    - ✓ JTC 1/SC 27 N3979, “IT Security technique – Encryption Algorithm – Part3 : Block ciphers”

The SEED Cipher Algorithm (2/2)

- Feature

  - Block cipher with DES-like(Feistel) structure

  - The size of input/output bit is fixed 128-bit

    (Padding is required by SEED to maintain a 16-octet blocksize)

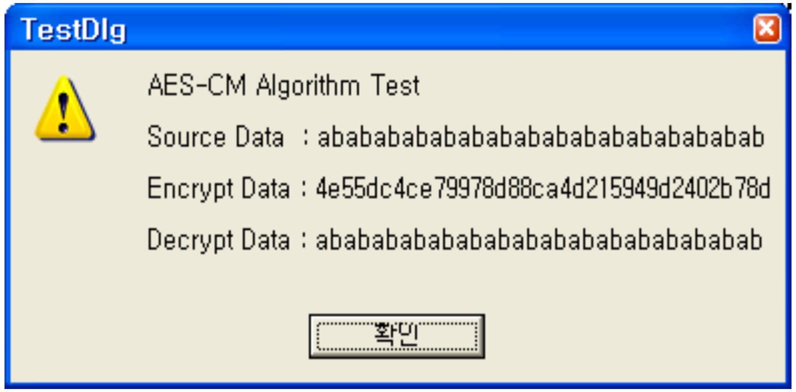
  - A strong round function against known attacks

  - The number of rounds is fixed 16

  - Mixed XOR and Modular addition operation

Example

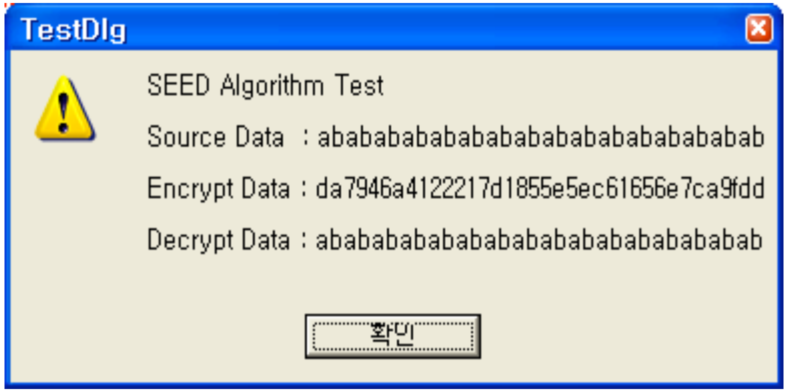
- The initial value, IV, shall be defined by the SSRC, the SRTP packet index i, and the SRTP session salting key k_s, as below:
  IV = (k_s * 2^16) XOR (SSRC * 2^64) XOR (i * 2^16)
  or shall be generated randomly



AES-CM Algorithm Test

```
Source Data  : abababababababababababababababab
Encrypt Data : 4e55dc4ce79978d88ca4d215949d2402b78d
Decrypt Data : abababababababababababababababab
```

<AES-CM>



SEED Algorithm Test

```
Source Data  : abababababababababababababababab
Encrypt Data : da7946a4122217d1855e5ec61656e7ca9fdd
Decrypt Data : abababababababababababababababab
```

<SEED>

Next Steps

- Comments or Questions ??

- Working Group Item??