The SEED Cipher Algorithm and Its Use with the SRTP

draft-ietf-avt-seed-srtp-00.txt

Yoon Seokung (KISA)

Goal / Features

- ✓ Goal : The SEED cipher algorithm would be the additional cipher in SRTP

- ✓ Features
  - ➢ RFC 4269, “The SEED Encryption algorithm”
  - ➢ RFC 4010(CMS), RFC 4162(TLS), RFC 4196(IPSec), JTC 1/SC27 N 3979(SEED)

  - ➢ 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-octets block-sizes)
  - ➢ The number of rounds is fixed 16
  - ➢ A strong round function against known attacks
  - ➢ Mixed XOR and Modular additional operation

Next Steps

- ✓ Draft adopted as WG document in Chicago
- ✓ Need for WG feedback
- ✓ A new revision accounting for WG comments to be submitted before the next meeting
- ✓ Then ready for WG last call

Thanks

Questions?