Ciphers in Use in the Internet

David McGrew

Sean Shen

draft-irtf-cfrg-cipher-catalog-00

- a catalog of the ciphers in use on the Internet, and/or defined or referenced in IETF RFCs.
- not a standards document
- aim to capture the consensus of the Cryto Forum Research Group at the time of publication
- Aim to provide technical guidance to standards groups, other implementers, engineers and researchers.

draft-irtf-cfrg-cipher-catalog-00

1. Introduction
2. Background
    - 2.1. Attack Models

      Popular known attack model
    - 2.2. Security Goals

      Some designing goals for ciphers

draft-irtf-cfrg-cipher-catalog-00

3. Guidance

general guidance such as cipher mode, combination with authentication, block size.

draft-irtf-cfrg-cipher-catalog-00

4. 128-bit Block Ciphers

   ARIA, CLEFIA, SMS4, SEED, Camellia, CAST-256, AES, Twofish, Serpent

5. 64-bit Block Ciphers

   MISTY1, SKIPJACK, RC2, CAST-128, BLOWFISH, IDEA,
   GOST 28147-89, 3DES, DES

6. Stream Ciphers

   Kcipher-2, Rabbit, RC4

For each cipher:

- reference, inventors, related RFCs, key sizes, rounds, IPR claims, known attacks, etc.
- lists ciphers in decreasing order of the year of their publication.

draft-irtf-cfrg-cipher-catalog-00

- This is the initial version of this note; it’s a work in progress, will improve in content and readability.
- Should not yet be considered as representative of any consensus.
- Comments are solicited and should be sent to the authors and to cfrg@irtf.org

Thank you!