Key Distribution and Management

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 04 Jan 2022,
keys.tex, r1969

Contents

Recommended Key Sizes

Comparing Key Lengths Across Symmetric and Public Key Algorithms

- Various governments, standardisation organisations and researchers have analysed security level of cryptographic mechanisms
- Provide recommendations for:
  - Ciphers to use
  - Key lengths or hash lengths
  - Security level
- BlueKrypt website summarises recommendations: www.keylength.com
  - E.g. from NIST, German BSI, NSA, ECRYPT project, ...
- ECRYPT-CSA Project 2018 report on Algorithms, Key Size and Protocols (PDF)

The BlueKrypt website summarises recommendations from various organisations. You should visit the website and explore the different recommendations. While there are differences, you can get an approximate idea of the key lengths that should be used.

The ECRYPT-CSA project is one effort to compare algorithms. The PDF report gives a comprehensive summary of different cryptographic mechanisms, analysis of specific algorithms, and recommendations.

Recommend Key Lengths from ECRYPT-CSA 2018

Protection	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
Legacy standard level *Should not be used in new systems*	80	1024	160	1024	160	160
Near term protection *Security for at least 10 years*	128	3072	256	3072	256	256
Long-term protection *Security for 30 to 50 years*	256	15360	512	15360	512	512

Credit: BlueKrypt www.keylength.com, CC-BY-SA 3.0

The figure on slide 4 shows recommended key (or hash) lengths, in bits, for symmetric key algorithms (e.g. AES), public key algorithms based on factoring a modulus (e.g. RSA), public key algorithms based on solving discrete logarithms (e.g. the secret key and modulus/group length in Diffie-Hellman), public key algorithms based on elliptic curve cryptography, and hash functions.

Three different levels of security are given: legacy, current (near-term) and future (long-term). Current or future levels of security should be used, although legacy levels may still be secure for some cases.