Cryptographic Key

Return to Glossary

Cryptographic Key [1] is a parameter used in conjunction with a Cryptographic Algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce, reverse or verify the operation while an entity without knowledge of the **Cryptographic Key**, cannot.

Examples include:

1. The transformation of Plaintext data into cyphertext data,
2. The transformation of cyphertext data into Plaintext data,
3. The computation of a Digital Signature from data,
4. The verification of a Digital Signature on data,
5. The computation of an Authentication Code from data,
6. The verification of an Authentication Code from data and a received or retrieved authentication code, and
7. The computation of a shared secret that is used to derive keying material.

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

1)

Elaine Barker, NIST, Recommendation for Key Management: Part 1 - General, NIST Special Publication 800-57 Part 1, Revision 5, May 2020, Accessed 18 January 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf