Private Key

Return to Glossary

Definition 1

A **Private Key**[1)] is a Cryptographic Key used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public. In an asymmetric-key (public-key) cryptosystem, the private key has a corresponding public key. Depending on the algorithm, the private key may be used, for example:

1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key,
3. Decrypt keys that were encrypted by the corresponding public key, or
4. Compute a shared secret during a key-agreement transaction.

Definition 2

A **Private Key**, also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt and decrypt code. Secret keys are only shared with the key's generator, making it highly secure. **Private Keys** play an important role in symmetric cryptography, asymmetric cryptography, and cryptocurrencies.

The complexity and length of the private key determine how feasible it is for an interloper to carry out a brute force attack and try out different keys until the right one is found.

Public Key are for encrypting data by anyone with access to the Public Key. The **Private Key** is required to decrypt the data, which is why the Private key needs to be kept secret.

Source: https://searchsecurity.techtarget.com/definition/private-key

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