Cryptography

Cryptography is the practice of protecting information so that only the intended has access. Cryptography uses codes and a process that alters the original data such that it is no longer comprehendible unless you know how to undo the process. In computer science cryptography is used to secure sensitive data on many occasions, such as data stored in a database or during communication.

Cryptography has four primary aims:

- Confidentiality: Protect the information from any who should not see it
- Integrity: The data must be recoverable without any alterations
- Non-repudiation: The creator of encrypted information's should be identifiable from the information.
- Authentication: the sender and recipient should be able to verify the information's source.

The process of securing data, transferring and recovering goes like so:

Data->Encrypt->Transfer->Decrypt>-Data

Approaches to cryptography

Symmetric Encryption

One key is used to encode both encode and decode the data. Symmetric encryption can be faster than asymmetric encryption. Symmetric encryption is suitable where both the encrypter and decrypter can be trusted with the key. A good use case is for encrypting database data where only the server has access to the key.

Asymmetric encryption

One key is used for decryption and another of encryption. The encryption key is known as the public key and the decryption key the private key. Because the public key only encrypts information it can be shared freely as it does not represent a security risk.