Kriptografi Tanımı (Vikipedi)

Kriptografi, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.

Kriptografi Prensipleri

Gizlilik	Bilgiyi görme yetkisi olanlar dışındaki herkesten gizli tutmak
Bütünlük	Bilginin üzerinde hiçbir değişiklik, ekleme, yeniden düzenleme yapılmadığı garantisi
Doğruluk	Bilgi göndericisinin gerçekten gönderen kişi olduğu garantisi.
Reddedile-mezlik	Göndericinin iletilen bilgiyi inkar edememesi

Bütünlük Terimleri

Hashing	Bilginin tek yönlü bir algoritma işlemine tabi tutularak aynı boyutta bir çıktı üretmesidir
Mesaj Özeti (Message Digest)	Şifreleme sistemlerinde kullanılan hash fonksiyonlarına verilen genel addır.
MD5	Message digest (mesaj özeti) kelimelerinin kısaltmasıdır ve 5. Versiyonunu ifade etmektedir.
SHA1	Secure Hashing Algorithm (güvenli özetleme algoritması) 1. Versiyonudur.
SHA2 (SHA256)	2. yani 256 Bitlik versiyon

Farklı iki yerdeki bilgiler hash işlemine tabi tutularak çıktıları karşılaştırılır ve bütünlüğün bozulup bozulmadığı bu şekilde ispatlanır. Mesaj özetlerininn en bilinenleri MD5 ve SHA algoritmalarıdır.

Hash Hesaplama Araçları

Hashing Calculator	http://www.fileformat.info/tool/hash.htm

Online olarak ya da direkt olarak bilgisayarda çalışabilen onlarca hash hesaplama araçları bulunmaktadır.

Simetrik Şifreleme Algoritmaları

- AES
- DES
- 3DES
- IDEA
- CAST
- 2FISH
- BlowFish
- Serpents
- Rijndael
- PGP
- OTP

Asimetrik Şifreleme Algoritmaları

- Diffie Helman
- El Gamal
- RSA
- Eliptical Curve
- Knapsack
- DSA (Digital Signature Algorithm)