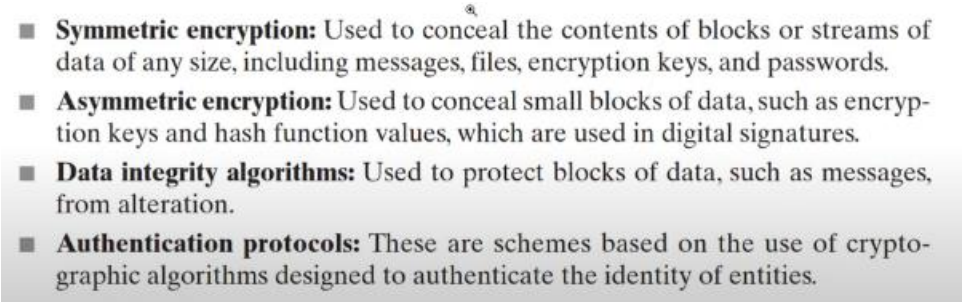
Kriptografik algoritmalar ve protokoller verilerin güvenliğini sağlamak için kullanılan matematiksel işlemlerdir. Bu algoritmalar, verilerin şifrelenmesi, şifrelerin çözülmesi ve güvenli veri iletişimi gibi işlemlerde kullanılır. Aşağıda, kriptografik algoritmaların ve protokollerin genel açıklamalarını ve bazı türleri:



- **Symmetric encryption:** Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.
- **Asymmetric encryption:** Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.
- **Data integrity algorithms:** Used to protect blocks of data, such as messages, from alteration.
- **Authentication protocols:** These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

- Şifreleme Algoritmaları: Bu algoritmalar, verileri şifrelemek için kullanılır. Şifreleme, verilerin anlaşılamaz hale getirilmesini sağlar ve sadece yetkili kullanıcıların şifreyi çözebilmesini mümkün kılar. Simetrik ve asimetrik şifreleme olmak üzere iki temel türü vardır.
- Simetrik Şifreleme: Aynı anahtarın hem şifreleme hem de şifre çözme işlemlerinde kullanıldığı bir şifreleme türüdür. AES (Advanced Encryption Standard) ve DES (Data Encryption Standard) gibi algoritmalar simetrik şifreleme örnekleridir.
- Asimetrik Şifreleme: Farklı anahtar çiftlerinin kullanıldığı bir şifreleme türüdür. Bir anahtar (genellikle "halka açık anahtar" olarak adlandırılır) verileri şifrelerken kullanılırken, diğer anahtar (genellikle "özel anahtar" olarak adlandırılır) şifreleri çözmek için kullanılır. RSA ve ElGamal gibi algoritmalar asimetrik şifreleme örnekleridir.
- Karma Fonksiyonları: Karma fonksiyonları, verilerin benzersiz bir karmasını (hash) oluşturan algoritmalardır. Bu algoritmalar, parola saklama, dijital imzalar ve veri bütünlüğü doğrulama gibi birçok uygulamada kullanılır. MD5, SHA-1 ve SHA-256 gibi karma fonksiyonları örnek verilebilir.
- Sayı Üreteçleri: Sayı üreteçleri, rastgele sayıların oluşturulması için kullanılan algoritmalardır. Güvenli rastgele sayı üretimi, şifreleme ve kimlik doğrulama protokollerinde önemlidir. Pseudorandom sayı üreteçleri (PRNG) ve gerçek rastgele sayı üreteçleri (TRNG) olmak üzere iki tür sayı üreteci bulunur.
- İmza Algoritmaları: İmza algoritmaları, bir mesajın doğruluğunu ve bütünlüğünü sağlamak için kullanılır. Mesajın gönderici tarafından imzalandığı ve imzanın alıcı tarafından doğrulandığı bir güvenlik mekanizmasıdır. RSA ve DSA (Digital Signature Algorithm) gibi algoritmalar imza oluşturma ve doğrulama için kullanılır.

- Anahtar Değişim Protokolleri: Anahtar değişim protokolleri, iletişimde kullanılan şifreleme anahtarlarının güvenli bir şekilde paylaşılmasını sağlar. Diffie-Hellman anahtar değişimi protokolü, güvenli anahtar değişimi sağlamak için yaygın olarak kullanılan bir örnektir.
- SSL/TLS Protokolü: Secure Socket Layer (SSL) ve Transport Layer Security (TLS), web tabanlı iletişimde kullanılan güvenli bir protokol çiftidir. Bu protokoller, sunucu ile istemci arasındaki verilerin şifrelenmesini ve kimlik doğrulamasını sağlar. Bu şekilde, güvenli bir şekilde veri alışverişi yapılabilir.

Bu liste, kriptografik algoritmaların ve protokollerin sadece birkaç örneğini içermektedir. Kriptografi alanı sürekli gelişmekte olup, yeni algoritmalar ve protokoller ortaya çıkmaktadır. Güvenlik ihtiyaçlarınıza ve uygulamanıza en uygun algoritmayı ve protokolü seçmek için güvenlik uzmanları ve kriptografi standartlarına başvurmanız önemlidir.