CRYPTOLOGY (KRİPTOLOJİ)

Cryptology

- **Cryptology** is the science of encryption. It is the encryption of various messages and texts according to a certain system, the transmission of these messages to the recipient in a secure environment, and the deciphering of the transmitted message.
- **Kriptoloji**, şifreleme bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifre edilmesidir.

Cryptology

- Cryptology is basically divided into two main topics;
  Cryptography and Cryptanalysis.
- Kriptoloji temelde iki ana konuya ayrılmıştır; Kriptografi ve Kriptoanaliz.

Cryptography and Cryptanalysis

Cryptography : It is the process of making data hidden from open. It ensures the confidentiality, integrity and security of data. People who do this process are called cryptographers. The understandable form of the current text is called plain text or clear text.

Kriptografi : Verilerin açık halden kapalı (gizli) hale getirilmesi işlemidir. Verilerin gizliliğini, bütünlüğünü ve güvenliğini sağlar. Bu işlemi yapan kişilere kriptograf denir. Mevcut metnin anlaşılır biçimine düz metin veya açık metin denir.

Cryptography and Cryptanalysis

- The new form obtained as a result of converting plain text into a form that cannot be understood by different processes is called encrypted text.

The purpose of cryptography is to hide the contents of messages by encrypting them so as to make them unrecognizable except by someone who has been given a special decryption key.

- Düz metnin farklı işlemlerden geçirilerek anlaşılamayacak bir forma dönüştürülmesi sonucunda elde edilen yeni forma şifreli metin denilmektedir.

Kriptografinin amacı, mesajların içeriğini özel bir şifre çözme anahtarı verilen biri dışında tanınmayacak şekilde şifreleyerek gizlemektir.

Cryptography and Cryptanalysis

The main purpose of cryptography is to ensure the confidentiality of information. There are three basic methods used for this purpose :

1. Substitution Methods: The position of the letters in plain text is fixed. Encrypted text is obtained by replacing these letters with numbers, symbols or letters of another alphabet.

Kriptografinin temel amacı bilginin gizliliğini sağlamaktır. Bu amaçla kullanılan üç temel yöntemden söz edilebilir :

1. **Yerine Koyma Yöntemleri** : Düz metindeki harflerin yeri sabittir. Sayılar, semboller ya da başka bir alfabedeki harfler bu harflerin yerine yerleştirilerek şifreli metin elde edilir

Cryptography and Cryptanalysis

- **2. Transposition Methods**: Letters in plain text are replaced. No other alphabet or symbol is used, the identities of the letters in plain text are fixed; but their places change. The best example in the past is the Caesar encryption algorithm.

- 2. **Yer Değiştirme Yöntemleri** : Düz metindeki harflerin yerleri değiştirilir. Başka bir alfabe ya da sembol kullanılmaz, düz metindeki harflerin kimlikleri sabittir; fakat yerleri değişir. Geçmişteki en güzel örneği Sezar şifreleme algoritmasıdır.

Cryptography and Cryptanalysis

3. Algebraic Methods: Is done using a variety of mathematical operations and functions.

3.**Cebirsel Yöntemler** : Çeşitli matematiksel işlemler ve fonksiyonlar kullanılarak yapılır.

Cryptography and Cryptanalysis

- **Cryptanalysis** : It is a sub-science of cryptology that deals with the analysis of texts encrypted by cryptographers and the resolution of passwords. The people who do this job are called cryptoanalysts. It is the process of obtaining plain text, that is the original text, from encrypted text. In short, the purpose of the cryptoanalysis is to decrypt encrypted text.

- Kriptoanaliz : Kriptografların şifreli hale getirdiği metinlerin analizi ve şifrelerin çözümü ile ilgilenen kriptoloji alt bilim dalıdır. Bu işi yapan kişilere kriptoanalist denir. Şifreli metinden düz metni yani orijinal metni elde etme işlemidir. Kısacası, kriptoanalizin amacı şifrelenmiş metnin şifresini çözmektir.

Usage Areas of Cryptology

- Various aspects in information security such as data confidentiality, data integrity and authentication are central to modern cryptography.

- Veri gizliliği, veri bütünlüğü ve kimlik doğrulama gibi bilgi güvenliğinin çeşitli yönleri, modern kriptografinin merkezinde yer alır.

Usage Areas of Cryptology

Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Modern kriptografi, matematik, bilgisayar bilimi, elektrik mühendisliği, iletişim bilimi ve fizik disiplinlerinin kesişme noktasındadır. Kriptografi uygulamaları arasında elektronik ticaret, çip tabanlı ödeme kartları, dijital para birimleri, bilgisayar parolaları ve askeri iletişim yer alır.

Some Important Concepts in Cryptology

Cryptographer

A Cryptographer is responsible for developing security systems using algorithms and cyphers to encrypt sensitive data. They analyse and decrypt information contained within cipher texts and encrypted data.

Kriptograf: Bir Kriptograf, hassas verileri şifrelemek için algoritmalar ve şifreler kullanarak güvenlik sistemleri geliştirmekten sorumludur. Şifreleme metinlerinde ve şifrelenmiş verilerde bulunan bilgileri analiz eder ve şifresini çözer.

Some Important Concepts in Cryptology

Encryption/Decryption

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

Şifreleme / Şifre çözme

Şifreleme, normal mesajı (düz metin) anlamsız mesaja (Şifreli metin) dönüştürme işlemidir. Buna karşılık Şifre Çözme, anlamsız mesajı (Şifreli metin) orijinal formuna (Düz Metin) dönüştürme işlemidir.

Some Important Concepts in Cryptology

Cryptographic key

In cryptography, a key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

Şifreleme Anahtarı: Kriptografide anahtar, verileri rastgele görünecek şekilde değiştirmek için bir şifreleme algoritması içinde kullanılan bir karakter dizisidir. Fiziksel bir anahtar gibi, verileri kilitler (şifreler), böylece yalnızca doğru anahtara sahip biri kilidi açabilir (şifresini çözebilir).

Some Important Concepts in Cryptology

CİPHER

Cipher, any method of transforming a message to conceal its meaning. The term is also used synonymously with ciphertext or cryptogram in reference to the encrypted form of the message.

ŞİFRE

Şifre, bir mesajı anlamını gizlemek için dönüştürmenin herhangi bir yöntemidir. Terim ayrıca, mesajın şifrelenmiş biçimine atıfta bulunarak şifreli metin veya kriptogram ile eşanlamlı olarak kullanılır.