Trabajo Corto 4 - Sistemas Operativos

B82957

Permutar

> Frequently, we are interested in a sample space that contains elements as all possible orders or arrangements of a group of objects. For example, we may want to know how many different arrangements are possible for sitting 6 people around a table, or we may ask how many different orders are possible for drawing 2 lottery tickets from a total of 20. The different arrangements are called permutation

> A permutation is an arrangement of all or part of a set of objects.

(Ronald E. Walpole) Probability & Statistics for Engineers & Scientists

Obfuscar

> Obfuscation means to make something difficult to understand. Programming code is often obfuscated to protect intellectual property or trade secrets, and to prevent an attacker from reverse engineering a proprietary software program.

Tech Target

Llave

> Obfuscation means to make something difficult to understand. Programming code is often obfuscated to protect intellectual property or trade secrets, and to prevent an attacker from reverse engineering a proprietary software program.

Techopedia

Simétrica

En ciptografía, la encriptación simétrica se refiere a que el algoritmo de encriptar una llave y desencriptarla es el mismo a lo largo del sistema.

Un ejemplo, digamos que para encriptar un mensaje de texto, todas las 'a' las remplazo por 'b', quién recibe el mensaje cifrado sabe que para desemcriptarlo tiene que hacer el proceso en reversa.

Asimétrica

La encriptación asimétrica sirve de forma diferente, se basa en la idea de manejar una **llave privada** y una **llave pública.**

La llave privada permite descifrar todos los mensajes cifrados con la clave pública; con la pública solo podemos descifrar los mensajes cifrados con la llave privada original.

Salt / Salting

Antes de definir salting, hay que definir el concepto de hash.

> A hash value is a numeric value of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures. You can sign a hash value more efficiently than signing the larger value. Hash values are also useful for verifying the integrity of data sent through insecure channels. The hash value of received data can be compared to the hash value of data as it was sent to determine whether the data was altered.

Microsoft

> Salting is a concept that typically pertains to password hashing. Essentially, it's a unique value that can be added to the end of the password to create a different hash value. This adds a layer of security to the hashing process, specifically against brute force attacks. A brute force attack is where a computer or botnet attempt every possible combination of letters and numbers until the password is found.

> Anyway, when salting, the additional value is referred to as a "salt."

Salting

Cracked

En el contenxto de informática y encriptación, *cracked* se refiere a lograr acceder a un sistema decifrando y accediendo sus programas de seguridad

---

Cipher

> Ciphers, also called encryption algorithms, are systems for encrypting and decrypting data. A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done.

> Ciphers, also called encryption algorithms, are systems for encrypting and decrypting data. A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done.

Cipher

Esteganografría

En el contexto de computación y seguridad, esteganografía es una aréa de estudia parecida a la encriptación. Sin embargo, una diferencia importante es que la esteganografía estudia como ocultar los datos e información sensible, tratando de volverla imperceptible.