

LU03.L02 - Applikationssicherheit und Kryptographie

1. Lückentext vervollständigen

Die Informationen (Ursprungstext), die geheim transportiert werden sollen, werden Plaintext (1), Klartext (2) oder Ursprungstext (3) genannt. Der Ursprungstext wird nach der Verschlüsselung Chiffertext (4) oder chiffrierter Text (5) bezeichnet. Die Umwandlung vom lesbaren in den unlesbaren, geheimen Text wird mithilfe des Schlüssels (6) durchgeführt. Wörter oder Sätze des Klartextes (7) werden durch andere Wörter oder Buchstabenfolgen ersetzt unter Verwendung eines Codebuches (8). Wenn der Plaintext über weite Teile des Chiffertextes (9) verteilt wird nennt man das Diffusion (10). Wenn weite Teile des Plaintext über den Chiffertext (11) verwischt werden, wird das Konfusion (12) genannt.

2. Bereiche der Vertraulichkeit und Authentizität

- **Vertraulichkeit:** Beschränkter Datenzugriff, Passwort an bestimmte Personen, Bankkonten, Useraccounts
 - Vertraulichkeit bezieht sich auf den Schutz von Informationen, sodass nur autorisierte Personen Zugriff darauf haben. Dies ist besonders wichtig bei persönlichen Daten, Bankinformationen oder bei der Zugriffskontrolle auf Useraccounts.
- **Authentizität:** ID, Unterschrift (digital), Persönliche Fragen bei Passwortrecovery, digitale Signaturen, Retina, Fingerabdruck
 - Authentizität gewährleistet, dass eine Person oder ein Objekt das ist, was es zu sein behauptet. Im digitalen Bereich sichert dies zum Beispiel durch digitale Signaturen, biometrische Verfahren wie Retina-Scans oder Fingerabdrücke die Identität einer Person.

From:

<https://wiki.bzz.ch/> - BZZ - Modulwiki



Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu03/loesungen/kryptographie?rev=1711631267>

Last update: 2024/03/28 14:07