

LU05.L02 - Applikationssicherheit und Kryptographie

Auftrag A: Lückentext vervollständigen

Die Informationen (Ursprungstext), die geheim transportiert werden sollen, werden **A Plaintext**, **B Klartext** oder **C Ursprungstext** genannt. Der Ursprungstext wird nach der Verschlüsselung **D Chiffertext** oder **E chiffrierter Text** bezeichnet. Die Umwandlung vom lesbaren in den unlesbaren, geheimen Text wird mithilfe des **F Schlüssels** durchgeführt. Wörter oder Sätze des **G Klartextes** (7) werden durch andere Wörter oder Buchstabenfolgen ersetzt unter Verwendung eines **H Codebuches**. Wenn der Plaintext über weite Teile des **I Chiffertextes** verteilt wird nennt man das **J Diffusion**. Wenn weite Teile des Plaintext über den **K Chiffertext** verwischt werden, wird das **L Konfusion** genannt.

Auftrag B: Begrifflichkeiten

- **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/lu05/loesungen/02?rev=1754994438>

Last update: **2025/08/12 12:27**

