

# LU05.A02 - Applikationssicherheit und Kryptographie

## Lernziele

- Ich kann wichtige Begriffe im Zusammenhang mit Applikationssicherheit in eigenen Worten erklären und anwenden.

## Rahmenbedingungen

- **Zeitbudget:** 20 Minuten
- **Sozialform:** Einzelarbeit
- **Hilfsmittel:** Dossier „LU05a - Kryptographie Basics“
- **Erwartetes Ergebnis:** Korrekt kompletter Text

## Ausgangslage

Kodierung und Kryptographie sind technisch gesehen sehr nahe beieinander. Bei der Kodierung ist das Umwandlungsverfahren bekannt. Hingegeben ist bei der Verschlüsselung das Verfahren und/oder der Schlüssel der Kodierung unbekannt.

## Arbeitsauftrag A

Vervollständigen Sie den nachfolgenden Lückentext durch die unten aufgelisteten Begriffe.

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

1. Plaintext
2. dechiffrierter Text
3. Klartext
4. Chiffertext
5. Schlüssel
6. chiffrierter Text
7. Diffusion
8. Chiffertext
9. Klartext
10. Codebuches

11. Chiffertext
12. Konfusion

- **Aufgabe 2:** Ergänzen Sie das Worddokument unterhalb der 2. Aufgabenstellung mit den beiden Begriffen und den Erklärungen zu „Kryptographie“.

## Solution

### Lösung

---



Volkan Demir

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

Permanent link:  
<https://wiki.bzz.ch/modul/m183/learningunits/lu05/aufgaben/02?rev=1754993758>

Last update: **2025/08/12 12:15**

