Hochschule Karlsruhe
University of
Applied Sciences

Fakultät für
Informatik und
Wirtschaftsinformatik

Digital educational Escape Game zum Thema Kryptographie

Lerninhalte

Kryptographie

Das Wort Kryptographie kommt aus dem Griechischen und besteht aus den Worten Kryptos (Verstecken) und Graphein (Schreiben).

Kryptographie = Die Kunst Codes zu schreiben und zu dekodieren.

Damit verbunden sind die Konzepte Verschlüsslung und Entschlüsselung.

Diese werden mithilfe mathematischer Mechanismen umgesetzt und erlauben die Berücksichtigung von Informationssicherheit.

Wichtige Aspekte der Informationssicherheit sind:

- Vertraulichkeit der Daten
- Datenintegrität
- Authentifizierung
- Nachweisbarkeit

Kryptographie

- Kryptografie: Ein System, das Klartext in verschlüsselten Text mit Hilfe eines Algorithmus umsetzt. Auf der Empfängerseite wird der verschlüsselte Text decodiert. Man erhält den originalen Klartext.
- Kryptanalyse: Wird von Mitlesenden des verschlüsselten Texts verwendet, um den unverschlüsselten Originaltext wiederherzustellen.

Kryptographie

- Transposition: Methode, durch die Symbole aus dem Klartext an unterschiedliche stellen im verschlüsselten Text positioniert werden.
- Substitution: Methode, durch die Symbole aus dem Klartext durch (normalerweise) andere Symbole im verschlüsselten Text ersetzt werden.
- Verschleierung: Methode, durch die zusätzliche Symbole im verschlüsselten Text positioniert werden, um den Inhalt zu verschleiern.

Kryptographie

Shannons Regeln (1949)

- das Sicherheitslevel der Nachrichten sollte sich im Verschlüsselungsaufwand widerspiegeln.
- die verwendeten Schlüssel und der Verschlüsselungsalgorithmus sollten so einfach wie möglich sein.
- die Umsetzung des Prozesses sollte so einfach wie möglich sein.
- Fehler im Verschlüsseln sollten sich nicht verbreiten, um weitere Nachrichten nicht zu zerstören.
- die Größe des verschlüsselten Texts sollte nicht grösser sein als die Größe des Klartexts.

Kryptographie

Caesar Chiffre

- Einfaches und zugleich unsicheres Verfahren zur Verschlüsselung von Texten
- Benannt nach dem römischen Kaiser Julius Caesar, der dieses Verschlüsselungsverfahren bereits genutzt haben soll
- Monoalphabetische Substitution, also jeder Buchstabe wird durch genau einen anderen Buchstaben des Alphabets ersetzt
- Basierend auf zyklischer Rotation des Alphabets um den verwendeten Schlüssel k wobei k=0 nicht sinnvoll, da keine Änderung entsteht)
- k kann für ein sinnvolles Ergebnis Werte aus der Menge $Z_{26}=\{0,1,\ldots,25\}$ annehmen

Quelle: Technische Universität Chemnitz (2024)