Kryptographie

Die Wissenschaft der Verschlüsselung von Informationen

Name: Kacper Bohaczyk

Date: 08.03.2022

Inhaltsverzeichnis

Zusammenfassung 4.1.1

4.1.1.1: Was ist Kryptographie?

Kryptographie ist die Kunst des Erstellens und Knacken der Geheimcodes. Das Ziel ist es die Daten so zu speichern, sodass nur der Empfänger sie sehen und bearbeiten kann. Es werden dabei Algorithmen benutzt. Die Daten werden verschlüsselt und chiffriert (es wird ein Klartext in Chiffretext umgewandelt). Die Person die ein Schlüssel besitzt kann dann die Nachricht in ein Klartext umwandeln.

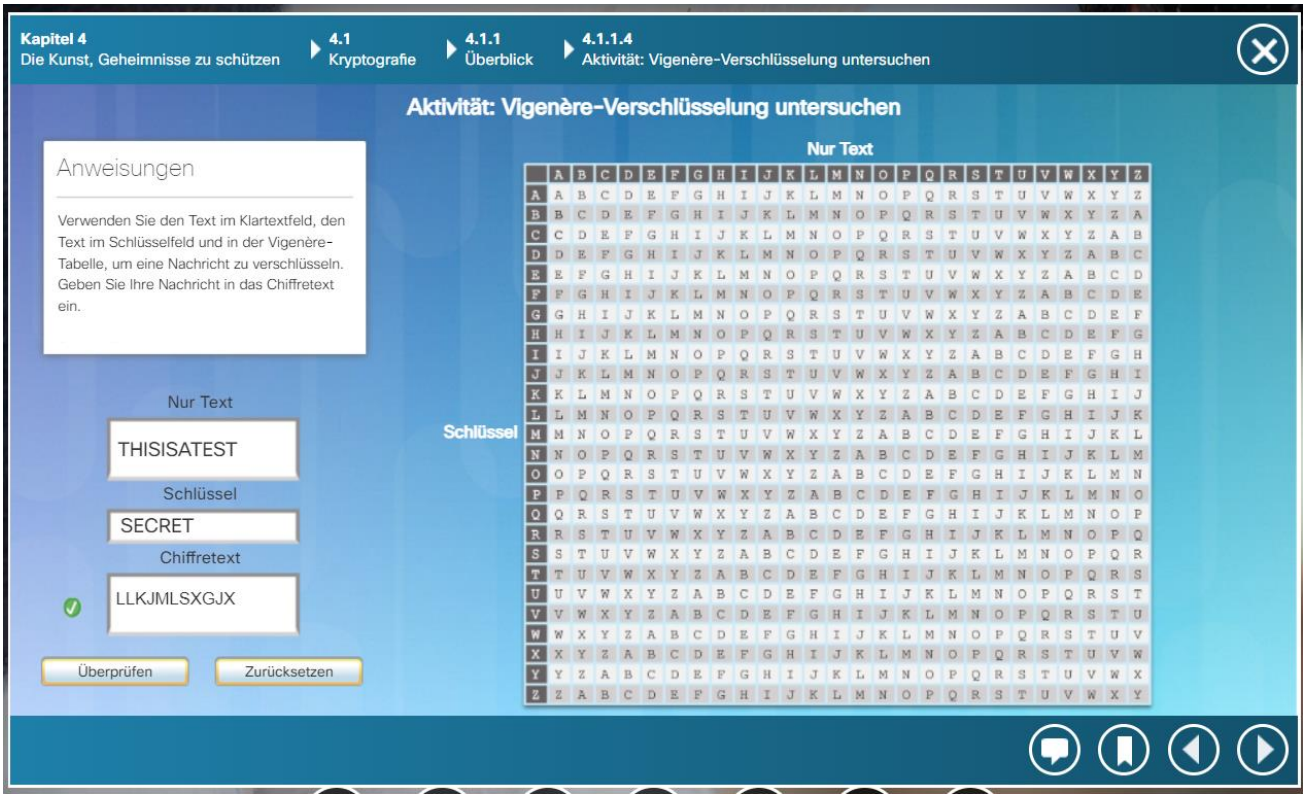
4.1.1.2: Die Entwicklung der Kryptographie

Es wurden schon immer Verschriftungen benutzt um sicher sich vor einem Königreich zu verteildigen. Es gab mehrere Geräte bzw. Varianten , mit denen man Verschlüsselt hat. Beispielsweise Skytale, Cäsar-Verschlüsselung, Vigenère-Verschlüsselung oder Enigma-Chiffriermaschine.

4.1.1.3: Erstellen eines verschlüsselten Textes

Bei jeder Verschlüsselung wird ein Algorithmus benutz. Es gibt verschiedene Möglichkeiten zur erstellen von Chiffren: Transposition , Substition, One Time Pad

4.1.1.4:



4.1.1.5: Zwei Verschlüsselungsarten

Es gibt die Symmetrische- und die Asymmetrische- Verschlüsselung. Bei der Symmetrischen verwendet man denselben Key bei der Verschlüsslung und der Entschlüsselung, im Gegensatz zur Asymmetrischen. Da ist ein Schlüssel öffentlich und der andere ist privat. Ein Nachteil bei den Asymmetrischen ist das sie mehr Ressourcen verbrauchen und länger dauern.

Zusammenfassung 4.1.2

4.1.2.1: Die Symmetrische Verschlüsselung

Symmetrische Algorithmen verwenden denselben Pre-Shared Schlüssel, um Daten zu verschlüsseln und entschlüsseln. Ein Nachteil dabei ist das, wenn man sicher sein will muss man je Kommunikation ein neuen Schlüssel erstellen

4.1.2.2: Arten der Kryptographie

Die meistverwendeten Arten der Kryptografie sind Blockchiffren und Stromchiffren. Im Blockchiffren wird ein Klartextblock fester Länge auf einen Chiffretextblock mit 64 oder 128 Bit abgebildet. Um es zu entschlüsseln wird dasselbe Verfahren benutzt nur umgekehrt. Bei Stromchiffren variiert die Umwandlung kleinerer Klartexteinheiten je nach Verschlüsselungsprozess. Komplexere Systeme können Blockchifferen und Stromchifferen kombinieren

4.1.2.3: Die Symmetrische Verschlüsselung

Es gibt 3DES (Triple DES), das IDEA (International Data Encryption Algorithm) und das AES (Advanced Encryption Standard. Bei dem 3DES werden symmetrische Blockchiffre mit 64-Bit-Blockgrößemit einem Schlüssel von 56 Bit. Bei der IDEA wird ein 64-Bit-Blöcke und 128-Bit-Schlüssel verwendet. Es gibt 8 Transformationsrunden. AES hingegen hat eine feste Blockgröße von 128 Bit mit einer Schlüsselgröße von 128,192 oder 256 Bit

4.1.2.4:

4.1.3.1: Die Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung, wird ein Schlüssel für die Verschlüsselung und ein anderer für die Entschlüsselung verwendet. Diese nennt man public und private key. Der public key ist jedem bekannt und der private key hat nur die person an die die Nachricht ankommen soll.

4.1.3.1: Die Asymmetrische Verschlüsselung

Es gibt verschiedene Algorithmen wie zum Beispiel das RSA (River-Shamir-Adleman) , Diffe- Hellman, ElGamal oder das Elliptische-Kurven-Kryptografie (Elliptic Curve Cryptography, (ECC)) Diese Unterscheiden sich Grundsätlich vom Preis und Anzahl an Primzahlen und Verwendung.

4.1.3.1:

4.1.4.1: Key Management (Schlüsselverwaltung):

das Generieren, Austauschen, Speichern, Nutzen und Ersetzen der Schlüssel, die in einem Verschlüsselungsalgorithmus verwendet werden, gehören zum Schlüsselmanagement. Die Schlüsselverwaltung ist die wichtigste und auch schwierigste Aufgabe. Meistens wird bei angriffen die Schlüsselverwaltung angegriffen und nicht der Algorithmus selbst. Die Schlüssellänge und das Keyspace sind dabei essenziel. Desto länger die Schlüssellänge desto größer ist der Keyspace

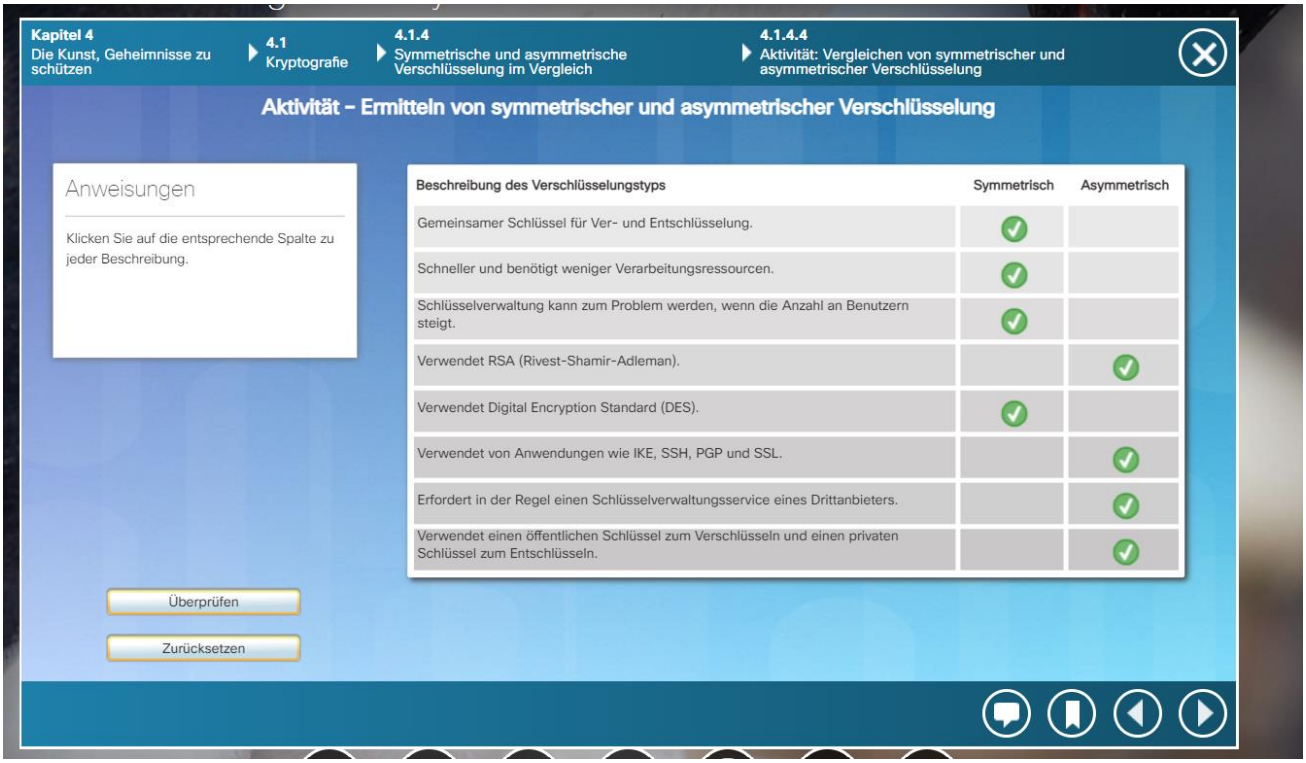
4.1.4.2: Vergleich zwischen verschiedenen Verschlüsselungarten

Die Unterschiede zwischen der Symmetrischen Verschlüsselung und der Assymetrischen sind, dass die Symmetrische Verschlüsselung effizienter ist und kann größere Datenmengen bewältigen. Asymmetrische Verschlüsselung kann hingegen zum Schutz der Vertraulichkeit kleiner Datenmengen besser benutzt werden. Sie bietet mit ihrer Größe und Geschwindigkeit eine höhere Sicherheit für Aufgaben wie den elektronischen Schlüsselaustausch,

4.1.4.3: Anwendung

Sie wird beispielsweise bei folgenden Protokollen verwendet IKE (Internet Key Exchange) , bei der Secure Socket Layer (SSL) , beim (SSH) Secure Shell oder beim Pretty Good Privacy (PGP). Bei VPN wird auch oft die Kryptographie benutzt.

4.1.4.4: Anwendung


Kapitel 4
Die Kunst, Geheimnisse zu schützen
4.1
Kryptografie
4.1.4
Symmetrische und asymmetrische Verschlüsselung im Vergleich
4.1.4.4
Aktivität: Vergleichen von symmetrischer und asymmetrischer Verschlüsselung
Aktivität – Ermitteln von symmetrischer und asymmetrischer Verschlüsselung
Anweisungen
Klicken Sie auf die entsprechende Spalte zu jeder Beschreibung.
Beschreibung des Verschlüsselungstyps
Symmetrisch
Asymmetrisch
Gemeinsamer Schlüssel für Ver- und Entschlüsselung.
Schneller und benötigt weniger Verarbeitungsressourcen.
Schlüsselverwaltung kann zum Problem werden, wenn die Anzahl an Benutzern steigt.
Verwendet RSA (Rivest-Shamir-Adleman).
Verwendet Digital Encryption Standard (DES).
Verwendet von Anwendungen wie IKE, SSH, PGP und SSL.
Erfordert in der Regel einen Schlüsselverwaltungsservice eines Drittanbieters.
Verwendet einen öffentlichen Schlüssel zum Verschlüsseln und einen privaten Schlüssel zum Entschlüsseln.
Überprüfen
Zurücksetzen