**Kryptographie**

1. Was ist Kryptographie ?

Definition:

Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen, um diese vor unbefugtem Zugriff zu schützen.

Ziel:

Sicherstellung von Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit von Informationen

*~Zu deutsch: Verschlüsselung~*

Anwendungsbereiche:

Kommunikation, Datenspeicherung, Authentifizierung

1. Geschichte der Kryptographie

Antike:

Einfache Verschlüsselungstechniken z.B. Caesar-Verschiebung

Mittelalter:

Vereinfachte Methoden z.B. Substitutionsverschlüsselung

Moderne:

Einführung von Maschinen (z.B. Enigma) und komplexe mathematische Algorithmen

Heutige Zeit:

Einsatz in digitalen Systemen, Internetkommunikation, E-Commerce

1. Grundlegende Konzepte der Kryptographie

Vertraulichkeit:

Schutz der Daten vor unbefugtem Zugriff

Integrität:

Sicherstellung, dass Daten nicht unbemerkt verändert werden

Authentizität:

Nachweis der Identität der Kommunikationspartner

Nicht-Abstreitbarkeit:

Sicherstellung, das der Sender einer Nachricht diese nicht leugnen kann

*~Heißt so viel wie: Verschlüsselung sollte tatsächlich verschlüsseln~*

1. Symmetrische Verschlüsselung

Definition:

Ein einzelner Schlüssel wird sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet

Vorteile: Schnell

Nachteile: Schlüsselverteilung

Beispiele:

A(dvanced)E(ncryption)S(tandard), D(ata)E(ncryption)S(standard)

DES ist defunc

1. Asymmetrische Verschlüsselung

Public key für verschlüsselung, Private key für Entschlüsselung

Vorteile: schnellere Schlüsselverteilung, sehr Sicher

Nachteile: langsamer als symmetrische verschlüsselung

Beispiele:

RSA (Rivest-Shamir-Adleman) => eines der ersten asymmetrischen Algorithmen

ECC (Elliptic Curve Cryptography) => modern, genauso sicher aber kürzere Schlüssel

1. Anwendungen

Sichere Kommunikation (SSL/TLS) => sichere Internetverbindung

Digitale Signaturen => Verifizierung von Authentizität und Integrität von Nachrichten

Datenspeicherung => Verschlüsselung von Datenträgern

Kryptowährungen => Blockchain und Sichere Transaktionen

1. Asd
2. Asd
3. asd