16 RSA Asymetrische Verschlüsselung

Peter Rutschmann

03.12.2025

Asymetrische Verschlüsselung

Unterschied Symetrische und Asymetrische Verschlüsselung

Bei der symetrischen Verschlüsselung verwenden Sender und Empfänger den gleichen Schlüssel zum Ver- und Entschlüsseln der Nachricht. Beispiel: AES, DES, 3DES Bei der asymetrischen Verschlüsselung verwenden Sender und Empfänger ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Beispiel: RSA

Aufgabe Symetrische und Asymetrische Verschlüsselung

- Schauen Sie sich dieses Video zum Unterschied zwischen symetrischer und asymetrischer Verschlüsselung an.
  - https://www.youtube.com/watch?v=QFjlwsAL9BY
- Erklären Sie Ihrem Lernpartner die beiden Verfahren.

Aufgabe: Anwenden der Asymetrischen Verschlüsselung

- Ausgangslage: Alice hat ein Schlüsselpaar aus einem privaten und einen public Schlüssel erstellt.
- Stichworte: Public Key, Private Key, Verschlüsseln, Entschlüsseln, Signieren, Signatur überprüfen
- Fall 1: Bob will Alice eine geheime Nachricht senden.
  - Erklären Sie Ihrem Lernpartner, wie Bob die Nachricht verschlüsselt und wie Alice die Nachricht wieder entschlüsselt.

- Fall 2: Alice will Bob eine Nachricht senden, die Bob eindeutig als von Alice stammend erkennen kann.
  - Erklären Sie Ihrem Lernpartner, wie Alice die Nachricht signiert und wie Bob die Signatur überprüft.
- Fall 3: Eve kennt den public key von Alice.
  - Erklären Sie Ihrem Lernpartner, welche der beiden Fälle Eve damit nutzen kann.
- Fall 4: Bob und Alice möchten sich geheime Nachrichten zusenden.
  - Erklären Sie Ihrem Lernpartner, welche die beiden vorgehen müssen.

RAS - Asymetrische Verschlüsselung

RSA (Rivest-Shamir-Adleman) ist ein weit verbreitetes asymetrisches Kryptosystem, das auf der mathematischen Schwierigkeit basiert, grosse Zahlen in ihre Primfaktoren zu zerlegen. Es wurde 1977 von Ron Rivest, Adi Shamir und Leonard Adleman entwickelt und ist eines der ersten praktischen Public-Key-Kryptosysteme.

RAS - das Prinzip

Das Prinzip von RAS zeigt dieses Arbeitsblatt. Laden Sie es herunter und lösen Sie es zusammen mit der Lehrperson.

Das Prinzip von RSA

RAS - praktische Anwendung

Aufgabe: Anwenden der RSA Asymetrischen Verschlüsselung

- Sie finden unter diesem Link eine Online-Version für die RAS Verschlüsseltung: https://www.devglan.com/online-tools/rsa-encryption-decryption
- Aufgabe 1)
  - Die Lehrperson hat eine Nachricht für alle Lernenden verschlüsselt.
  - Entschlüsseln Sie die Nachricht mit dem public key der Lehrperson.
  - Key-Size: 1024bit
  - Public-Key: RSA Public Key Lehrperson
  - Verschlüsselte Nachricht (Base64): tjeyUglifabTTrXGNm5Qw3R7QUau0SIXsPAI8FziCVokn
  - Encryption Algorithmus: RSA

- Aufgabe 2)
  - Erstellen Sie selber einen Schlüsselpaar (public und private key) mit einem Key-Size von 1024bit.
  - Tauschen Sie den Public-Key mit Ihrem Lernpartner aus. (und umgekehrt)
  - Verschlüsseln Sie eine Nachricht und geben Sie die verschlüsselte Nachricht an Ihren Lernpartner weiter. Er soll die Nachricht entschlüsseln. (und umgekehrt)