RIVEST-SHAMIR-ADLEMAN (RSA)

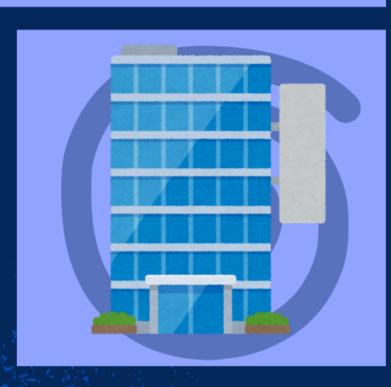


WAS IST RSA?

RSA (Rivest-Shamir-Adleman) ist ein asymmetrisches Verschlüsselungsverfahren, das weltweit für sichere Datenübertragung eingesetzt wird.

ECHTE ANWENDUNGSBEREICHE

- ProtonMail Sichere E-Mail-Verschlüsselung
- TLS/SSL (Amazon, Google) Verschlüsselte Webverbindungen
- Microsoft Windows Digitale Signaturen für Software-Authentifizierung
- Bitcoin Schlüsselverwaltung für Kryptowährungs-Wallets





UNSERE IMPLEMENTIERUNG: VON GRUND AUF IN C++

Unsere modular aufgebaute RSA-Implementierung umfasst grosse Ganzzahlen, Schlüsselgenerierung, Verschlüsselung, Entschlüsselung und Laufzeitanalysen.

Highlights:

- Effiziente Primzahlgenerierung
- Sauberer Code (Google C++ Style Guide)