Asymmetrische Verschlüsselung

Grundlagen

Informationen unverständlich machen
Dazu wird ein Codebuch verwendet
Nur Personen mit Schlüssel haben Zugriff

Originaltext	Verschlüsselter Text (Codebuch)
A	1
B	2
C	3
Ich heiße David	837 483831 38392

Verschlüsselungsverfahren

RSA (Rivest–Shamir–Adleman) eines der wichtigsten
Diffie Hellmann
Elliptische Kurven Kryptographie

Asymmetrische Verschlüsselung

Verwendet zwei Schlüssel
Public Key verschlüsselt Daten (jedem bekannt)
Private Key entschlüsselt Daten (nur Empfänger bekannt)

Ablauf einer Verschlüsselung

1.Schlüsselerzeugung
    Jeder Benutzer generiert ein Schlüsselpaar welches Public und Private Key enthält.
2.Benutzer1 schickten Daten zu Benutzer21
    Daten werden mit öffentlichem Schlüssel von Benutzer2 verschlüsselt
3. Benutzer2 empfängt Daten
    Benutzer2 kann mit seinem privaten Schlüssel empfangene Daten entschlüsseln

SSH-Ablauf

1.Client fragt bei Server um Verbindung an
2.Server sendet dem Client seinen Public Key
3.Beide verhandeln über mögliche Parameter und den richtigen Channel
4.Client loggt sich auf Server ein

Use-Cases

Sichere Übertragen von Daten (SSH)
Schlüsselaustausch (symmetrische Verschlüsselung)
Digitale Signaturen (Handy-Signatur)
Authentifizierung von Server und Client
E-Mail-Verschlüsselung
VPN
Kryptowährungen

Vergleich zwischen der symmetrischen und asymmetrischen Verschlüsselung

Asymmetrische Verschlüsselung	Symmetrische Verschlüsselung
Zwei Schlüssel	Einen Schlüssel
Empfänger benötigt nur einen Schlüssel	Sender und Empfänger benötigen privaten Schlüssel
Langsamere Geschwindigkeit	Schnellere Geschwindigkeit
Sicherer	Unsicherer
Für Kommunikationen verwendet	Für große Datenmengen verwendet