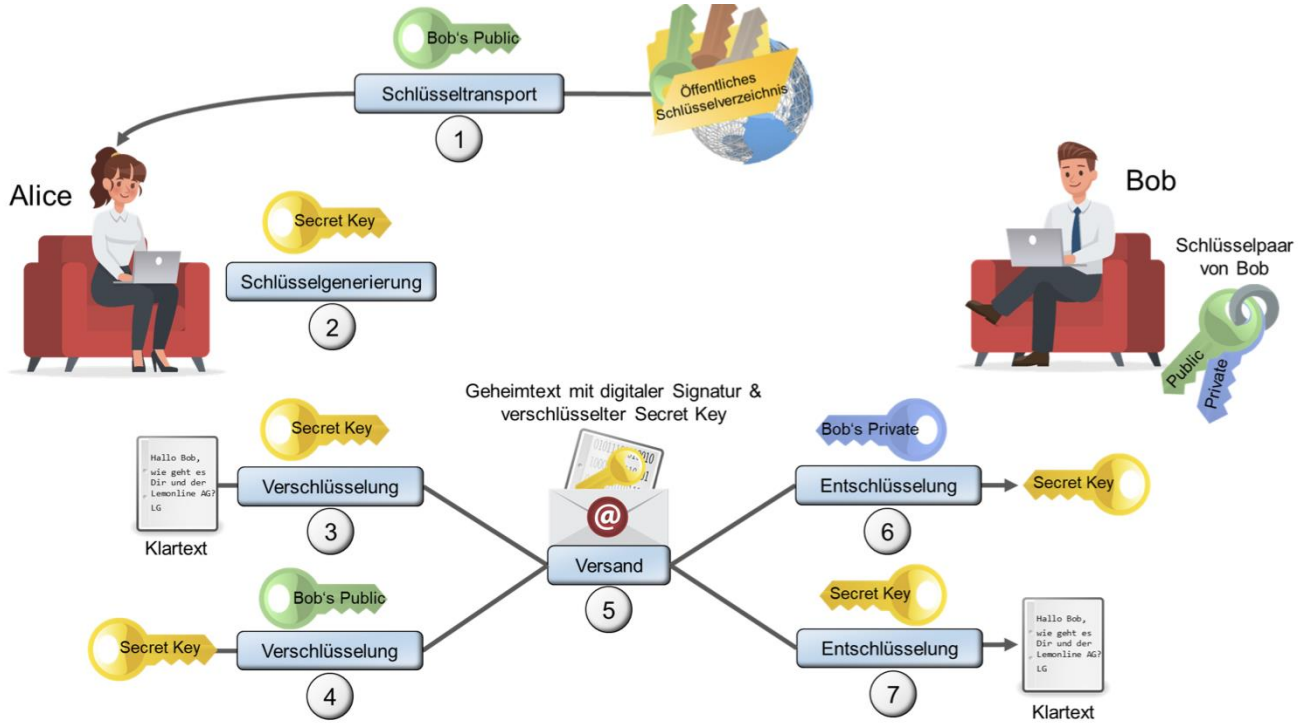
Daniel Niederhauser, Julian Madersbacher 5AHW

Hybride Verschlüsselung

Die hybride Verschlüsselung kombiniert das asymmetrische und symmetrische Kryptoverfahren. Eine Kombination dieser beiden Verfahren bringt erhebliche Geschwindigkeitsvorteile gegenüber dem asymmetrischen Verschlüsselungsverfahren. Grundidee beim hybriden Verfahren ist es, den Klartext zuerst mit einem zufällig generierten Schlüssel zu verschlüsseln (symmetrisch). Dann wird nur der zufällig generierte Schlüssel asymmetrisch verschlüsselt und übertragen.



Schritt 1: Alice beschafft sich den öffentlichen asymmetrischen Schlüssel von Bob aus einem öffentlichen Schlüsselverzeichnis.

Schritt 2: Alice generiert einen geheimen symmetrischen Schlüssel für die zukünftige Kommunikation mit Bob.

Schritt 3: Alice schreibt eine Nachricht in Klartext. Sie erstellt auch ihre digitale Signatur (schlüsselabhängige Prüfsumme) und fügt diese bei. Alice verschlüsselt die Nachricht mit dem generierten, geheimen Schlüssel. Die Nachricht wird in Geheimtext umgewandelt.

Schritt 4: Alice verschlüsselt den geheimen Schlüssel mit dem öffentlichen Schlüssel von Bob.

Schritt 5: Alice versendet die verschlüsselte Nachricht zusammen mit ihrer digitalen Signatur und dem verschlüsselten geheimen Schlüssel per E-Mail an Bob.

Schritt 6: Bob entschlüsselt den geheimen Schlüssel mit seinem privaten Schlüssel. Bob überprüft auch die digitale Signatur von Alice.

Schritt 7: Danach entschlüsselt Bob die Nachricht von Alice mit dem geheimen Schlüssel.

Das hybride Verfahren sorgt dafür, dass Alice und Bob einen symmetrischen Session-Key für ihre verschlüsselte Kommunikation verwenden können. Mithilfe des asymmetrischen RSA-Verfahrens kann der symmetrische Schlüssel, mit dem die Nachricht verschlüsselt wurde, von Alice zu Bob transportiert werden. Das RSA-Verfahren hat jedoch einen Nachteil. Die privaten Schlüssel könnten von unbefugten Personen oder von Angreifern entnommen werden. Wenn eine Person den privaten Schlüssel von Alice oder Bob in die Hände bekommen sollte, würde er damit den geheimen Session-Key entschlüsseln können. Aus diesem Grund werden einmalig erstellte RSA-Schlüsselpaare für den Transport des geheimen symmetrischen Session-Keys nicht mehr empfohlen.

Das Diffie-Hellman-Verfahren ergänzt daher das RSA-Verfahren mit einer notwendigen Methode, vergängliche Schlüssel für den Transport zu vereinbaren und keine starren RSA-Schlüsselpaare zu verwenden.

Vorteile:

+ Die Diffie-Hellman-Schlüsselvereinbarung erzeugt einen geheimen, symmetrischen Session-Key und bietet mehr Vertraulichkeit.

+ Das RSA-Signatursystem bestätigt die Identität von Personen und prüft Informationen auf Richtigkeit.

+ Hohe Geschwindigkeit bei der Ver- und Entschlüsselung des Session-Keys durch das symmetrische Verfahren.

Nachteile:

– Die Bedrohung durch potenzielle Man-in-the-Middle-Attacken wird durch digitale Signaturen zwar erschwert, ist jedoch nicht immer zu vermeiden.

– In der Praxis möglicherweise anfällig für Anwendungs- und Implementierungsfehler durch die hohe Komplexität.

Anwendungsgebiete:

Das hauptsächliche Anwendungsgebiet für die hybride Verschlüsselung besteht bei E-Mails. Neben E-Mails kommt diese Form von Verschlüsselung auch in diversen Netzwerkprotokollen zu Einsatz. Hierzu zählen beispielsweise TLS und SSL.