RSA

**Wo wird RSA noch angewendet**

RSA ist ein Verfahren, welches auch heute noch zum Einsatz kommt. Oft wird RSA gebraucht um die Schlüssel von symmetrischen Verfahren wie 3DES und AES zu verschlüsseln. Dass grosse Problem von RSA ist die Geschwindigkeit. Wenn man RSA sicher anwenden möchte, braucht es eine Schlüssellänge von fast 2000 bit, was jeden Prozess sehr langsam macht.   
RSA kommt heute vor allem bei Übertragungs-Protokollen wie: IPsec, TLS, SSH und WASTE zum Einsatz.  
Weiter wird RSA auch im EBanking gebraucht.   
Der grosse Vorteil von RSA ist die Anwendung von einem öffentlichen und privaten Schlüssel, also ein asymmetrisches Verfahren. Oft werden dann symmetrische und asymmetrische Verfahren zu einem hybriden Verfahren kombiniert.   
Damit können die Vorteile beider Systeme vereint werden: Der einfache Schlüsselaustausch und eine schnelle und effiziente Verschlüsselung.

**Warum wird RSA heute weniger angewendet**

Damit RSA sicher angewendet werden kann, braucht es Schlüssellängen von fast 2000 bit. Bei solch langen Schlüsseln leidet die Effizienz und insbesondere die Geschwindigkeit. Der verschlüsselte Geheimtext wird deutlich länger als der ursprüngliche Text.  
Reine RSA Verfahren sind daher bei grossen Mengen von Daten zu langsam.

RSA wird aber bei vielen hybriden Verfahren angewendet um den Schlüssel symmetrischer Verfahren auf einem öffentlichen Kanal versenden zu können und dann nur mit dem privaten Schlüssel zu dem symmetrischen Schlüssel zu kommen, der geheim gehalten werden muss.

**Einige Verschlüsselungsverfahren und deren Vorteile gegenüber RSA**

AES: Advanced Encryption Standard

AES ist ein symmetrische Verschlüsselungsverfahren, wo es entscheidend ist, den Schlüssel geheim halten zu können.  
Die Vorteile von AES ist die Geschwindigkeit und die Effizienz. Geschwindigkeit dadurch, dass die verschlüsselte Nachricht nicht länger wird. Beeindruckend ist, dass bei diesem Verfahren auf eigentlich einfache Weise jede bit verändert wurde.   
Es werden verschiedene Verschlüsselungsrunden angewendet, die jeweils einen anderen Schlüssel haben, der aus dem ursprünglichen Schlüssel generiert werden.  
In jeder Runde werden verschiedene Operationen angewendet wie

-ShiftRow: Die bits werden nach links oder rechts geschoben,   
-MixColumns: Die in Tabellenform abgelegten Daten werden untereinander vertauscht,  
-SubBytes: Jedes bit wird zuerst einmal verändert.

AES bedarf der Geheimhaltung vom ursprünglichen Schlüssel. Daher wird AES dort angewendet, wo es keinen Schlüsselaustausch bedarf.  
Oder AES wird mit RSA oder anderen asymmetrischen Verfahren zu einem hybriden Verfahren kombiniert.

AES überzeugt durch eine einfache Implementierung und eine hohe Geschwindigkeit.

Anwendung findet AES bei WPA2, SSH und IPSec.

DES: Data Encryption Standard 3DES : Triple DES

DES ist der Vorgänger vieler symmetrischen Verschlüsselungsverfahren. Es wurde bereits in den siebziger Jahren von IBM entwickelt.  
Ein grosser Vorteil, DES ist frei von Patentrechten. DES wurde für die Hardware-Verschlüsselung geschaffen und ist für Software zu langsam.

Die Schwachstelle von DES ist seine Blocklänge von 64 Bit und da 8 Bit als Prüfsumme verwendet werden, sind es eigentlich nur 56 Bit.

Dadurch entstand die Idee mehrere Blöcke hintereinander zu platzieren. Es entstand so das Triple DES.

Heute wird DES noch bei der Sprachverschlüsselung angewendet. Beispielsweise bei der Funkkommunikation von Spezialeinheiten der Polizei.

Twofish

Twofish ist der Nachfolger von Blowfish. Die Schlüssellänge kann 128, 192 oder 256 Bit betragen.Twofish war auch ein Kandidat für AES und schaffte es unter die besten drei.

Twofish ist ein symmetrisches Verfahren, welches auch aus dem ursprünglichen Schlüssel verschiedene Schlüssel für jede Verschlüsselungsrunde generiert.  
In jeder Runde werden dann Operationen wie XOR, ROT und MOD angewendet.  
Im Vergleich zu AES ist Twofish etwas weniger sicher.   
Twofish überzeugt aber auch durch Effizienz und Geschwindigkeit.

Da auch Twofish ein symmetrisches Verfahren ist, muss der Schlüssel geheim gehalten werden können. Wie AES bedarf wird auch Twofish zusammen mit asymmetrischen Verfahren verwendet.