Kryptografische Methoden zur sicheren Datenübertragung

=== > Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.
Auch die Analyse der unterschiedlichen kryptografischen Verfahren, d. h ihre Stärken und Schwächen, zählt zur Kryptologie.

Zur Kryptologie gehören folglich die beiden Bereiche:

- Kryptografie
  Lehre von der Verschlüsselung von Informationen, die „Geheimschriften“
- Kryptoanalyse
  Analyse und Bewertung der Sicherheit von Kryptoverfahren (gegen unbefugte Angriffe)

Mit der Hand wurden früher mühsam Texte ver- und entschlüsselt.
Dazu zählt der **Cäsar-Code**: Cäsars Trick bestand darin, die Buchstaben des Alphabets um einige Stellen zu **verschieben**.
Beispiel:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C (um 3 Stellen nach links verschoben)

==> Aus BBS LANDAU wird dann EEV ODQGDX

Eine noch ältere Verschlüsselungstechnik ist **Atbash** (etwa 600-500 vor Chr. in Palästina benutzt).Die Buchstaben werden einfach **rückwärts** aufgelistet:
Beispiel:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A (rückwärts geschrieben)

==> Aus LANDAU wird OZMWZF !

Im 20. Jahrhundert wurden **elektromechanische Verschlüsselungsmaschinen** erfunden. Dazu zählte die im 2. Weltkrieg eingesetzte berühmte deutsche Enigma. Heute werden für Verschlüsselungen **Computer** eingesetzt.

Die Kryptologie war und ist für das Militär wichtig und auch in unserem öffentlichen und privaten Leben hat sie Einzug gehalten (Internet, Passwörtern, Kreditkartennummern).

Die Verschlüsselung bezog sich anfangs auf Wortebene (eine **Kodierung** eines Wortes), jetzt bezieht sie sich auf die Verschlüsselung der Zeichenebene (**Chiffren**). Moderne kryptologische Algorithmen operieren entweder auf **Byte-Ebene** (d.h. Zeichenebene) oder sogar auf **Bit-Ebene**. Um keine Geschwindigkeitsnachteile zu haben, wird Software in der Regel Byte-weise und Hardware Bit-weise verarbeitet.

In der Informatik wird **zwischen Code und Chiffren unterschieden**:

Ein Code legt fest wie etwa Schriftzeichen für die Datenverarbeitung als Zahlen dargestellt werden (ANSII Code). Es handelt sich hierbei jedoch nicht um eine Verschlüsselung, die der Geheimhaltung dient. Da es sich bei Codierung nicht um kryptografische Verfahren handelt, == >**spricht man in der Kryptographie von (de)chiffrieren und nicht von (de)codieren**.

Symmetrisches und asymmetrisches Verschlüsselungsverfahren

Symmetrisches Verfahren:
Anfangs waren die Schlüssel **symmetrisch**, und der Besitz eines Schlüssels konnte eine Nachricht verschlüsseln als auch entschlüsseln.. Der Schlüssel musste zwischen den Kommunikationspartnern ausgetauscht werden und **es gab nur den einen Schlüssel**. Aus diesem Grund wird für jeden Partner ein eigener Schlüssel benötigt, damit nur der seine Daten entschlüsseln kann. Mit der Anzahl der Partner steigt die Unsicherheit. Der Austausch muss aber sicher sein, unabhängig von der Anzahl der Kommunikationspartner. Dieses symmetrische Verfahren wird auch als **Secret-Key- oder „Shared Secret"-Verfahren** bezeichnet. Die erwähnten Schwächen des symmetrischen Verschlüsselungsverfahrens sollten durch das asymmetrische Verfahren beseitigt werden.

Asymmetrisches Verfahren:
Werden für Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet, dann wird das Verfahren als **asymmetrisch** bezeichnet.
Es gibt einen öffentlichen Schlüssel und einen privaten Schlüssel.
Bei der **Public Key Cryptography** (**P**retty **G**ood **P**rivacy (PGP), von Phil Zimmermann entwickeltes Programm zur Verschlüsselung von Daten), wird ein Paar zusammenpassender Schlüssel eingesetzt, **ein eindeutig zugeordnetes Schlüsselpaar**.
Der eine Schlüssel ist ein **öffentlicher** Schlüssel der zum **Verschlüsseln** von Nachrichten für den Schlüsselinhaber benutzt wird.
Der andere Schlüssel ist ein privater Schlüssel, der vom Schlüsselinhaber **geheim** gehalten werden muss und zur **Entschlüsselung** eingesetzt wird. Je nach verwendetem Schlüssel entstehen bei der Verschlüsselung derselben Daten bei einem anderen Kommunikationspartner unterschiedliche verschlüsselte Daten, die ja eigentlich gleich sind.
Trotzdem: Mit diesem Verfahren wird nur ein einziges Schlüsselpaar für jeden Teilnehmer benötigt und das bedeutet ein mehr an Sicherheit.
Der Besitz des öffentlichen Schlüssels setzt die Sicherheit nicht aufs Spiel, weil es noch einen weiteren privaten und geheimen Schlüssel bei dem anderen Partner gibt.
Diese **Public-Key-Verfahren** können zur

Authentifizierung in einer interaktiven Kommunikation und auch zur Erstellung einer **elektronischen Signatur** (sicheren Abwicklung von Geschäften im Internet) verwendet werden.

E-Mail-Verkehr: Zusammen mit S/MIME gehört der OpenPGP-Standard zu den wichtigsten Standards für E-Mail-Verschlüsselung

OpenPGP: OpenPGP ist in der EDV ein Standard für Verschlüsselungs-Software. OpenPGP ist ein Internet-Standard. Das Dokument beschreibt das Datenformat, um Informationen verschlüsselt zu speichern und digitale Signaturen zu erzeugen. OPenPGP ist solch ein Hybrid, d.h. eine Kombination aus asymmetrischer und symmetrischer Verschlüsselung.

S/MIME: S/MIME bedeutet Multipurpose Internet Mail Extensions und wird auch Multimedia Internet Message Extensions genannt. MIME ist ein Kodierstandard, der

die Struktur und den Aufbau von E-Mails und anderer Internetnachrichten festlegt. Zwischen Sender und Empfänger werden Informationen über den Typ der übermittelten Daten ausgetauscht (Content-Type) und gleichzeitig eine für den verwendeten Übertragungsweg sichere Kodierung festgelegt.
Weitere bekannte **Kryptografische Protokolle** sind:
SSH: SSH oder Secure shell ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man sich über eine verschlüsselte Netzwerkverbindung auf einem entfernten Computer einloggen und dort Programme ausführen kann. SSH ermöglicht eine sichere, authentifizierte und verschlüsselte Verbindung zwischen zwei Rechnern über ein unsicheres Netzwerk.
SSL/TLS: SSL oder Secure Sockets Layer oder auch Secure Server Line ist ein Netzwerkprotokoll zur sicheren Übertragung u. a. von Internetseiten (Bankgeschäfte), welches zur sicheren Kommunikation eines Browsers mit dem Server dient, wird als Verfahren eingesetzt. TLS: Transport Layer Security, ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet

Ob die Signatur echt ist- und damit die Integrität und Authentizität der Daten - kann durch entsprechende Operationen mit dem öffentlichen Schlüssel überprüft werden.
Diese Operation wird bei der elektronischen Unterschrift genutzt, da nur der Besitzer des geheimen Schlüssels einen so genannten **Hash-Wert**, der das Dokument identifiziert, chiffrieren kann. Der Hash-Wert des Dokumentes wird vom Empfänger der Nachricht errechnet und mit dem chiffrierten Hash-Wert, der mit dem öffentlichen Schlüssel des Absenders dechiffriert werden kann, auf Übereinstimmung geprüft. Sind beide Hash-Werte gleich, ist sichergestellt, dass der Absender im Besitz des geheimen Schlüssels ist und das Dokument signiert hat.

Die Public-Key-Kryptografie wurde zuerst vom Militär **zwischen 1960 und 1970 entwickelt**.
Ein wichtiger Fortschritt war 1976 die Veröffentlichung des Artikels New Directions in Cryptography von Whitfield Diffie und Martin Hellman.
Dieser Aufsatz stellte eine radikal neue Methode (Idee) der Schlüsselverteilung vor und gab den Anstoß zur Entwicklung von **Public-Key-Verfahren**. Dennoch bleibt der Schlüsselaustausch ist eines der fundamentalen Probleme der Kryptografie.

Moderne Verschlüsselungsalgorithmen sind z. B.:

- **RSA** (1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard M. **A**dleman entwickelt, Patent ist 2000 ausgelaufen) und
- **AES** (**A**dvanced **E**ncryption **S**tandard, 128 Bit Blocklänge, der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt).

Sie gelten als „sicher“. Ohne den entsprechenden Schlüssel können verschlüsselte Daten nur mit hohem Aufwand dechiffriert werden.
Eine Kryptoanalyse solcher Verfahren ist bei einem komplexen Schlüssel selbst für Strafverfolgungsbehörden oder Geheimdienste „aussichtslos“.

Vor- und Nachteile der zwei Verfahren:
Der Schlüsseltausch ist ein grundsätzliches Schwachstelle bei allen Verfahren.
Asymmetrische Kryptosysteme haben den Vorteil, dass sie das Geheimnis möglichst klein halten, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Bei einem symmetrischen Kryptosystemen muss jeder Benutzer alle Schlüssel geheim halten.

Mit steigender Teilnehmerzahl wird der Aufwand immer größer und eine große Zahl an Schlüsseln ist erforderlich und die Schlüssel müssen auf einem sicheren Weg übermittelt werden (Schlüsselverteilungsproblem). Dies kann sehr aufwändig werden.
Im Gegensatz dazu kann mit dem öffentlichen Schlüssel dieses Problem ignoriert werden, da nicht er, sondern der private Schlüssel das Geheimnis trägt. Voraussetzung dafür ist aber, dass der öffentliche Schlüssel echt ist und nicht vorgetäuscht wird. Dies versucht man entweder mit dem Einsatz von zentralen Zertifizierungsstellen oder durch Etablierung eines Web of Trust zu gewährleisten.

Asymmetrischen Algorithmen arbeiten langsam. Durch so genannte hybride Verfahren wird in der Praxis das Problem minimiert. Hybride Verfahren sind eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung.
Wird bei dem asymmetrischen Verfahren eine verschlüsselte Nachricht an **mehrere Empfänger** zugestellt, dann erfolgt eine Verschlüsselung mit dem **öffentlichen Schlüssel**. Die Nachricht müsste aber für jeden Empfänger einzeln verschlüsselt und versandt werden. In der Praxis wird dieses Problem ebenfalls mittels hybrider Verfahren umgangen.

Die Sicherheit vieler asymmetrischer Kryptosysteme ruht laut wikipedia auf unbewiesenen Annahmen: „Es wird lediglich stark vermutet, dass die den verschiedenen Verfahren zugrunde liegenden Einwegfunktionen nur mit enormen Rechenaufwand umkehrbar sind. Es kann also nicht ausgeschlossen werden, dass noch unbekannte Algorithmen existieren, die die Umkehrung der „Einwegfunktion“ mit vertretbarem Aufwand leisten.“

Auch die Frage: „Ist der öffentliche Schlüssel tatsächlich echt?“ bleibt und ist es nicht ein Angriff vom so genannten Mittelsmann, dem **Man-In-The-Middle-Angriff**.
Täuscht ein Mittelsmann den öffentlichen Schlüssel eines Kommunikationspartners nur vor? Vertrauenswürdigen **Zertifizierungsstellen** versuchen dieses Problem zu umgehen.

Die Verschlüsselung mit dem **Elliptische-Kurven-Kryptosystem (EKK)** wird immer populärer, da sie mit wesentlich kleineren Schlüsseln auskommt. Bei diesem asymmetrischen Verfahren sollen Schlüssellängen mit160 Bit genauso sicher wie eine frühere 1024 Bit Verschlüsselung sein.

Beispiel A:

Die Kopplung aus asymmetrischer und symmetrischer Verschlüsselung bezeichnet man als hybrides Verschlüsselungsverfahren.

a) Nennen Sie ein Anwendungsbeispiel!
b) Erläutern Sie wie diese Kopplung funktioniert!

zu Frage a): SSL
Verschlüsselung

zu Frage b):

- Ein Schlüsselpaar (asymmetrisch) ist vorhanden und wird nur am Beginn des Prozesses benötigt.
- Die eigentliche Verschlüsselung erfolgt mit einem Session-Key (symmetrisch).

- Dieser Session-Key wird für jede Verbindung neu erzeugt.
- Der Session-Key wird für die Übermittlung von der Client-Seite mit dem öffentlichen Schlüssel verschlüsselt und danach von der Server-Seite wieder entschlüsselt.
- Das Schlüsselpaar ist durch ein Trust-Center verifiziert.