Inhalt

Betrachtung verschiedener Kryptosysteme

Kompetenzen, die am Ende erreicht sein müssen

Fülle folgenden Fragebogen zu Beginn des Themas und am Ende einmal aus:

Kompetenzen, die du nun erreicht haben solltest	+	0	-
Netzwerke			
Ich kenne grundlegende Möglichkeiten Daten im Internet auszuspionieren.			
Ich kenne und verstehe den grundlegenden Aufbau von Datenpaketen im Internet.			
Ich kenne die Bedeutung von Protokollen für die Kommunikation zwischen Computern.			
Ich kenne und verstehe den grundlegenden Aufbau folgender Protokolle und weiß, welche Anwendungen diese Protokolle einsetzen:			
- IP/TCP			
- SMTP			
- POP3/IMAP			
Kryptologie			
Ich kenne grundlegende Begriffe und Verfahren der Kryptologie:			
1. Kryptographie			
2. Kryptoanalyse			
3. Datenintegrität			
4. Authentizität			
5. Verschlüsselung			
6. Codierung			
Ich kenne folgende Begriffe und kann kryptologische Verfahren entsprechend der Kategorien korrekt einordnen			
7. Substitution			
8. Transposition			
9. Monoalphabetisch			
10. Polyalphabetisch			
Ich kenne die Bedeutung der Maxime von Kerkhoff			
Ich kenne grundlegende ältere Verschlüsselungsverfahren und kann sie in Scheme/Java implementieren			
1. Caesar			
2. Vigenere			
Ich kenne kryptoanalytische Verfahren und kann sie auf gegebene verschlüsselte Texte anwenden			
1. Häufigkeitsanalyse			
2. Kasiski-Test			
Ich weiß, was asymmetrische Verfahren im Gegensatz zu symmetrischen Verfahren sind und kenne die Vor- und Nachteile beider Verfahren in Bezug auf:			
- Sicherheit			
- Authentizität der Daten			

- Schlüssel-Übermittlungs-Probleme			
- Anzahl der zu generierenden Schlüssel			
- Rechenaufwand			
Ich kenne das Diffie-Hellman Verfahren im Detail und kann kurze Texte damit ver- und entschlüsseln.			
Ich kenne das RSA Verfahren im Detail und kann kurze Texte damit Verschlüsseln.			
Ich kenne Vor- und Nachteile beider Verfahren und kann somit begründen, wann welches Verfahren vorzugsweise eingesetzt wird.			
Ich kenne die Schwierigkeiten, die entstehen, wenn man große Zahlen potenzieren muss und kann die passenden Modulo Gesetze anwenden, um das RSA Verfahren auch bei größeren Zahlen zu berechnen.			
Ich kenne das Potenz-Modulo Verfahren und kann es in Scheme implementieren			
Ich kenne „schnelles Potenzieren“ und den Vorteil im Vergleich zu herkömmlichen Potenz-Berechnungen.			
Ich kenne „schnelles modulares Potenzieren“ und kann eine entsprechende Schemefunktion dazu implementieren.			

Anleitung – Wie gehe ich mit einem Skript um?

- Im Folgenden wird genau beschrieben, wie du mit einem Skript arbeiten kannst und worauf du dabei achten musst. Du kannst dir dies zusätzlich – oder stattdessen – auch in einem Video erklären lassen:
- Schaue dir dazu auf www.youtube.com/alexkueck11 das Video mit dem Namen „Aufbau eines Skriptes“ an.
- Um dir das Thema „Kryptologie“ zu erarbeiten, kannst du grundsätzlich zwei verschiedene Wege gehen:

  - **Weg A –** Du bearbeitest **eigenständig die Projektaufgabe**. Dazu kannst du dir aus den Materialien raussuchen, was du gebrauchen kannst oder dir auch ganz eigene erklärende Materialien suchen.
  - **Weg B –** Du gehst die **einzelnen Module Schritt für Schritt** durch und erarbeitest dir so nach und nach die einzelnen Module (hier lernst du sozusagen Stück für Stück, wie die Projektaufgabe gelöst werden kann. Die Projektaufgabe wurde daher auch in „kleine Häppchen“ aufgeteilt und am Ende von jedem Modul wird ein Stück der Projektaufgabe gelöst).

- Mit beiden Wegen kannst du die geforderten Kompetenzen erwerben. Wenn du schon einiges über die funktionale Programmierung weist und gerne an etwas knobelst, kannst du Weg A wählen. Behalte dabei aber immer auch im Auge, was du am Ende der Einheit können musst.
- Wenn du in diesem Bereich aber noch unsicher bist und das Thema lieber Schritt für Schritt erklärt bekommen möchtest, um es zu begreifen, wähle zunächst lieber Weg B.

Auch hier löst du die Projektaufgabe, aber eben Schritt für Schritt und es wird dir vorgegeben, wie der Lösungsweg aussehen kann.

- Wenn du einen der beiden Wege eingeschlagen hast, bedeutet das allerdings nicht, dass du darauf festgelegt bist! Natürlich kannst du vom Projekt auch wieder auf die Module umsteigen, zum Beispiel, wenn du bei einer Sache nicht weiterkommst. Ebenso kannst du auch zur Projektaufgabe wechseln, wenn du nach ein paar Modulen merkst, dass du jetzt schon gut im Thema drin bist, und versuchen möchtest, eigenständig weiter zu knobeln.
- Lege dir eine Mappe an, in der du alle Lösungen und (Zwischen-) Ergebnisse zu den Aufgaben bzw. dem Projektvorhaben festhältst.

Wichtig: Du kannst deine Ergebnisse immer zwischendurch mit dem Lehrer abgleichen, um zu sehen, ob du auf dem richtigen Weg bist.

Gerade wenn du an dem Projekt arbeitest (aber auch wenn du mit dem Skript eigenverantwortlich durch das Thema gehst), ist es wichtig, dass du festhältst, wie du vorgegangen bist. Das tust du bitte in einem Blog oder einer Mappe. Dort hältst du fest, in welche Probleme du gelaufen bist und wie du sie gelöst hast – und vor allem, was du dadurch gelernt hast.

Wichtige Ergebnisse, Erkenntnisse, Merksätze oder Lösungsstrategien gehören hier ebenfalls hin. Am besten ist es, wenn du das in deinen eigenen Worten oder auch durch eine Skizze ausdrücken kannst. Selbst wenn das dann nicht ganz richtig ist, ist es besser so, als etwas Fertiges abzuschreiben. Der Lehrer kann so drauf schauen und dir helfen, wenn du etwas noch nicht vollständig verstanden hast.

Problemlösestrategien stehen bei diesem Projekt im Vordergrund nicht die Inhalte!
Wenn du nicht genau weißt, was du aufschreiben sollst, lasse es dir vom Lehrer erläutern. Vorgefertigte Bögen, wo du Hilfestellung zu den Inhalten bekommst, kannst du beim Lehrer abholen.

Weg A – Bearbeitung der Projektaufgabe:

- Wie du die Projektaufgabe löst, bleibt dir und deiner Kreativität ganz allein überlassen. Du kannst selbst im Internet recherchieren und nachsehen, ob es dort Erklärungen oder Videos gibt, die dir weiterhelfen. Du kannst aber auch die in diesem Skript angegebenen Materialien weiter hinten verwenden – denn sie passen zu der Projektaufgabe.
- Ein Anhaltspunkt, um dich mit dem Thema auseinanderzusetzen, sind die Begriffe, die bei den zu erreichenden Kompetenzen am Anfang der Beschreibung angegeben sind. Damit könntest du z.B. anfangen. Wenn du die Begriffe verstehst und was für Ideen damit verknüpft sind, bist du meistens schon voll mit dem Thema beschäftigt. Vielleicht hast du ja auch schon für dich einen Weg gefunden, wie du an neue Projekte herangehst, dann solltest du diesen Weg hier auch gehen.
- Wichtig ist unbedingt, dass du im Auge behältst, was du am Ende der Einheit können musst. Die Projektaufgaben sind so formuliert, dass du am Ende alles, was gefordert ist, auch kannst. Aber es gibt ja viele Lösungswege und vielleicht kannst du am Ende

das ein oder andere noch nicht so gut. Dann frage bitte nach zusätzlichen Übungsaufgaben zu dem jeweiligen Thema oder Begriff - bis du das Gefühl hast, es gut genug anwenden zu können.

Weg B – Bearbeitung der Module

- Gehe die Module Schritt für Schritt durch. Um die in jedem Modul angegebenen Aufgaben bearbeiten zu können, musst du vorher lernen, wie das geht. Nicht der Lehrer erklärt dir das, du entscheidest, auf welchem Weg du die Informationen haben möchtest und musst sie dann selbst so für dich zusammenstellen, dass du die Aufgaben lösen kannst. In der Regel kannst du wählen zwischen einem erklärenden Text, Webseiten, auf denen du passende Informationen findest oder erklärenden Videos. Diese kannst du dir so oft ansehen, wie du es brauchst und magst. Wenn du dennoch weitere Erklärungen benötigst, notiere dir deine Fragen und wende dich damit an deinen Lehrer oder suche im Internet selbst nach weiteren erklärende Texten oder Videos. Der Lehrer ist da, um dich in deinem Lernen zu unterstützen, aber du musst aktiv werden und nachfragen, wenn etwas unklar ist.
- Es ist wichtig, dass du alle neuen Begriffe, die du nicht kennst, klärst und richtig verstehst. Du musst sie in eigenen Worten beschreiben oder sie in einer Skizze darstellen können.
- Gehe bei jedem der Kapitel wie folgt vor:
  1. Zu Beginn jedes Kapitels findest du Verweise auf Materialien, die dir helfen sollen, das Thema zu verstehen, damit du später die dazugehörigen Aufgaben lösen kannst. Das können zum Beispiel sein:
     - erklärende Videos,
     - Infotexte (parallel zu den Videos),
     - Seiten in einem Schulbuch und
     - Texte in Zeitschriften oder auch
     - Internetseiten
  2. Eventuell brauchst du trotz der Materialien eine zusätzliche Erklärung, dann frage beim Lehrer nach. Eventuell haben andere ja auch diese Frage, dann kannst du auch einen kurzen Lehrvortag dazu bekommen oder ein zusätzliches erklärendes Video.
  3. Die Videos und Dateien, auf die in diesem Skript verwiesen werden, findest du
     a. auf dem YouTube-Kanal: youtube.com/alexkueck11
        Die Videos beginnen alle mit „Kryptologie-„
  4. Falls du in den Materialien auf unbekannte Begriffe stößt, notiere diese. Das können auch einfache Worte sein. Versuche sie mithilfe der weiteren Materialien oder durch eigene Recherchen zu klären.
  5. Wenn du das Thema verstanden hast und alle darin enthaltenen Fachbegriffe in deinen eigenen Worten oder mittels einer Skizze erklären kannst, gehst du weiter zu den Aufgaben:
     - Die Aufgaben fordern dich auf, das Gelernte nun anzuwenden.
     - Gehe die Aufgabe, die im Skript angegeben sind der Reihe nach durch (die Aufgaben sind logisch aufeinander aufgebaut, daher der Reihe nach durchgehen).

- Wenn du eine Aufgabe nicht bearbeiten kannst, gehe noch einmal über die Materialien oder schaue dir das erklärende Video erneut an. Vielleicht hast du einen neuen Begriff oder eine neue Idee noch nicht ganz verstanden – dann hole das nun nach.
- Wenn das nichts hilft, frage bei Mitschülern oder dem Lehrer nach. Lass dir aber nicht die ganze Aufgabe lösen. Wichtig ist, dass du eigenständig an einer Lösung arbeitest – auch wenn sie am Ende vielleicht nicht ganz richtig ist.
- Wenn du an deiner Lösung zweifelst, schaue in den Musterlösungen nach (falls vorhanden) oder frage den Lehrer, ob er sich deine Ergebnisse auch zwischendurch anschauen kann.

Falls du bei einer Aufgabe doch noch Schwierigkeiten hast, schaue dir noch einmal die erklärenden Materialien an.

Wichtig ist, dass du selbst an den Lösungen arbeitest und nicht andere das mache lässt.

6. Wenn Aufgaben, die mit einem **Zusatz** gekennzeichnet sind, brauchst du nicht bearbeiten. Diese Aufgaben sind schwieriger und gehen über das hinaus, was du als Minimum erreichen musst, um das Skript erfolgreich abzuschließen. **Für eine abschließende Note im Einser- oder Zweier-Bereich solltest du aber zumindest einige dieser Zusatzaufgaben bearbeiten.**

7. Es wird zwischendurch Tests geben, diese werden rechtzeitig angegeben. Auch welche Kompetenzen in den Tests angefragt werden.

Wichtig:

Wichtig ist, dass du bei der Arbeit mit dem Skript selbst aktiv wirst und deinen eigenen Lernprozess überwachst:

→ Liege ich noch gut in der Zeit?
→ Habe ich alles verstanden/begriffen oderbrauche ich noch Hilfe oder zusätzliche Erklärungen?
→ Wie kann ich Zusammenhänge besser verstehen/begreifen, die noch unklar sind?
→ Wer kann mir bei der Bearbeitung der Aufgaben helfen?

Du musst selbst entscheiden, wo du dir weitere Informationen/hilfen holen möchtest und von dir aus auf deinen Lehrer oder Mitschüler zugehen, um Fragen zu stellen, damit du die Themen und Begriffe besser verstehst und am Ende die geforderten Zielkompetenzen erreichst!

Es wird am Ende eine Klausur geben, die du bestehst, wenn du alle Aufgaben bearbeitet und verstanden/begriffen hast und die Kompetenzen erreicht hast.

Materialien

Achtung:
Beim Schauen der Videos unbedingt Notizen machen. Haltet die Aussagen in eigenen Worten fest, die euch wichtig erscheinen!
Falls nach einmaligem Gucken die Anwendung schwer fällt, nehmt eine zum Video passende Aufgabe und löst sie parallel zum erneuten Gucken des Videos – Schritt für Schritt nach den Angsben im Video!

Videos

Netzwerk-Videos

„Sendung mit der Maus“- http://www.youtube.com/watch?v=8PNRrOGJqUI
„Was ist ein Netzwerk“ - http://youtu.be/-sLCCDWU26Y
perm.ly/netzwerke-protokolle-i-einfuehrung
perm.ly/netzwerke-protokolle-ii-datenpakete
perm.ly/netzwerke-protokolle-iii-e-mail
perm.ly/netzwerke-protokolle-iv-sicherheit

grundlegende Kryptologie Videos:

http://kkghh.de/neu.php?name=kryptologie-grundlagen
http://kkghh.de/neu.php?name=kryptologie-steganographie
http://kkghh.de/neu.php?name=kryptologie-transpositionen
http://kkghh.de/neu.php?name=kryptologie-substitutionen-monoalphabetisch
http://kkghh.de/neu.php?name=kryptologie-substitutionen-polyalphabetisch
http://kkghh.de/neu.php?name=kryptologie-haeufigkeitsanalyse

weiterführende Kryptologie Videos:

http://perm.ly/kryptologie-vigenere-verfahren
http://perm.ly/kryptologie-caesar-verschluesselung-scheme
http://perm.ly/kryptologie-haufigkeitsanalyse-java
http://perm.ly/kryptologie-haufigkeitsanalyse-scheme
http://perm.ly/kryptologie-symmetrisches-verschluesselungsverfahren
http://perm.ly/kryptologie-asymmetrisches-verfahren
http://kkghh.de/neu.php?name=kryptologie-diffie-hellman-i
http://kkghh.de/neu.php?name=kryptologie-diffie-hellman-ii
(älter) http://perm.ly/kryptologie-diffie-hellmann-verfahren
(älter) http://perm.ly/kryptologie-diffie-hellman-verfahren-details
http://perm.ly/kryptologie-diskreter-logarithmus
(älter) http://perm.ly/kryptologie-diffie-hellmann-details-ii
http://perm.ly/kryptologie-rsa-verfahren
http://perm.ly/kryptologie-potenz-modulo-rechnung
http://kkghh.de/neu.php?name=kryptologie-schnelles-potenzieren
http://perm.ly/kryptologie-schnelles-modulares-potenzieren

Arbeitsblätter

RAS Übungen.pdf
Arbeitsblatt_4.pdf
RSA

Aufgabe BWINf
Diskreter Logarithmus

Webseiten
http://www.matheprisma.de/Module/RSA/index.htm
http://www.inf-schule.de/informatik/kryptologie/rsa

zum Thema Internet
http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/internet-und-struktur/

Verschlüsselung allgemein
http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/verschluesselung-und-identitaeten/

Projekte vorgegeben:
haufigkeitenschuelerversion

Texte
Skript Kryptologie -Text Definition Kryptologie
Skript Kryptologie -Text Einstieg Kryptographie
Skript Kryptologie -Text Einschub Java I Arrays und mehr
Skript Kryptologie -Text Modulo Rechnung
Skript Kryptologie -Text Caesar
Skript Kryptologie -Text Vigenere
Skript Kryptologie -Text Häufigkeitsanalyse
Skript Kryptologie -Text Kasisi Test
Skript Kryptologie -Text Einführung Asymmetrische Verfahren
Skript Kryptologie -Text Allgemeines Prinzip Asymmetrische Verschlüsselung
Skript Kryptologie -Text DH Verfahren
Skript Kryptologie -Text RSA Verfahren
Skript Kryptologie -Text IDEA Verfahren

Lösungen
Skript Kryptologie neumit Projekten ohne Text Lsg
Skript Kryptologie -Text Einschub Java I Arrays und mehr Lsg
Skript Kryptologie -Text Modulo Rechnung Lsg
KasiskiTest
DiffieHellTabelleBeispiel

Voraufgabe
Bitte fülle die zugehörige Kompetenzübersicht vor dem Beginn des Skriptes einmal aus

Motivation Datenspionage:

Ausschnitt aus einem Sternartikel vom 10.6.2013

Mozilla macht gegen Datenklau der USA mobil

In Europa häuft sich die Kritik an der Datensammelwut des US-Geheimdienstes. Auch in den USA formiert sich der Widerstand. Firefox-Entwickler Mozilla startet jetzt die Kampagne "Stop Watching Us".
Mozilla-Sprecher Alex Fowler: Erkenntnisse bestätigen "viele unserer schlimmsten Befürchtungen"© Josep Lago/AFP
In den USA formiert sich im Geheimdienst-Skandal ein immer breiterer Widerstand gegen den Datenklau im Namen der Sicherheit. Unter dem Motto "Stop Watching Us" (Hört auf, uns zu beobachten), startete am Dienstag eine Gruppe von Firmen und Bürgerrechtsorganisationen eine Kampagne gegen die Überwachung von Internet- und Telefondaten durch den US-Geheimdienst NSA.
Die Zeitungen "Guardian" und "Washington Post" hatten unter Bezug auf die Informationen des nach Hongkong geflohenen Informanten Edward Snowden berichtet, der US-Geheimdienst NSA sammele und analysiere massenhaft Nutzer-Daten von Unternehmen wie Google,Yahoo, Microsoft, Apple oder Facebook. Die großen Internet-Konzerne wollen nun, so heißt es, offener über bisher geheime Anfragen von US-Behörden nach Nutzerdaten berichten können. Facebook und Microsoft schlossen sich in der Nacht zum Mittwoch einem entsprechenden Vorstoß von Google an. Die Unternehmen sind unter Druck geraten, weil in Medienberichten seit vergangener Woche der Eindruck entsteht, der US-Geheimdienst NSA könne nach Belieben auf Informationen der Nutzer zugreifen. Dabei sind die Firmen mit ihren Geschäftsmodellen auf das Vertrauen der Nutzer angewiesen

Widerspricht Grundwerten von Freiheit und Privatsphäre

Inzwischen wappnen sich die Gegner des Spionageprogramms auf immer breiterer Front. So reichte die Bürgerrechtsorganisation American Civil Liberties Union in New York eine Klage gegen die Sammlung von Telefon-Verbindungsdaten ein. Der Firefox-Entwickler Mozilla startete mit Rückendeckung von Bürgerrechtsaktivisten und anderen Firmen die Online-Petition "Stop Watching Us".
Mozilla und seine Verbündeten sammeln im Internet Unterschriften für einen offenen Brief an den US-Kongress. "Diese Art der pauschalen Datensammelei kratzt an den amerikanischen Grundwerten von Freiheit und Privatsphäre", heißt es darin. Dadurch würden Eckpfeiler der Verfassung verletzt. "Wir rufen den Kongress auf, sofort zu handeln, um diese Überwachung zu stoppen." Die Verantwortlichen müssten zur Rechenschaft gezogen werden.
"Wir wollen kein Internet, wo alles, was wir tun, heimlich von der Regierung protokolliert wird", erklärte Alex Fowler von Mozilla. Die Erkenntnisse über die Spähprogramme zu Internet- und Telefonverbindungen bestätigten "viele unserer schlimmsten Befürchtungen", fügte Fowler hinzu.
…..

Aufgabe
1. Lies den Text aufmerksam durch.
2. Nimm schriftlich dazu Stellung und überlege dir, welche Vorkehrungen du persönlich reffen könntest, um deine Daten nicht weiterhin ausspionieren zu lassen.

Modul 1 Protokolle im Internet:

Ein wesentliches Angriffsziel in Bezug auf Datenklau im Internet und speziell bei E-Mail sind sogenannte Protokolle.
Im Folgenden wird dir dies näher erläutert:

- ➔ **Videos:**
  - „Sendung mit der Maus“- http://www.youtube.com/watch?v=8PNRrOGJqUI
  - „Was ist ein Netzwerk“ - http://youtu.be/-sLCCDWU26Y
  - perm.ly/netzwerke-protokolle-i-einfuehrung
  - perm.ly/netzwerke-protokolle-ii-datenpakete
  - perm.ly/netzwerke-protokolle-iii-e-mail
  - perm.ly/netzwerke-protokolle-iv-sicherheit
- ➔ **Erklärender Text:**
  - Skript Kryptologie -Text Protokolle
- ➔ **Website:**
  - http://www.kleines-lexikon.de/w/p/protokoll.shtml
  - http://www.informationsarchiv.net/lexikon/eintrag/789

Definition Protokoll engl.: protocol
meint hier Vereinbarungen über die Art und Weise, wie **Daten** zwischen verschiedenen Rechnern ausgetauscht werden, quasi die Sprachen der Rechner.
Es geht hierbei sowohl um die Form als auch die Reihenfolge, in der Daten ausgetauscht werden – wer spricht zuerst und was???

Aufgabe 1.1.

1. Stelle in einer eigenen Skizze dar, wie Daten im Internet versendet bzw. ausgetauscht werden (gehe auch darauf ein, wie Sender und Empfänger einander zugeordnet werden).
2. Beschreibe in eigenen Worten, wie die Kommunikation bei E-Mail verläuft, fertige auch hier eine eigene Skizze an, die alle wesentlichen Aspekte erläutert.
3. Erläutere auch, wieso es nötig ist, bei der E-Mail Kommunikation mit Servern zu arbeiten. Welche Gefahren in Bezug auf Sicherheit der Daten ergeben sich dadurch! Was kann man dagegen tun?
4. Beschreibe in eigenen Worten, wozu Protokolle im Internet verwendet werden und wie es möglich ist, beim Transport der Daten im Internet, die Inhalte von z.B. E-Mails zu erfahren.
5. Gehe dabei auch darauf ein, wie sicher es ist, wenn man sich z.B. bei E-Mail- Servern oder Facebook anmeldet.
6. Wie könnte ein Angreifer, der Zugriff auf deine Daten hat, dies zu deinem Nachteil ausnutzen?

Zusatzaufgaben, wenn du dich mit dem Thema Netzwerke ein wenig mehr auseinander setzen möchtest:
Arbeitsauftrag 1 EinführungNetzwerke
Arbeitsauftrag2_Netzwerke

- ➔ Videos dazu:
  - http://perm.ly/kommunikation-in-netzwerken-router
  - http://perm.ly/kommunikation-in-netzwerken-switche

Aufgabe 1.2.
Überprüfe zu deiner Sicherheit, ob du folgende Dinge nun kannst (fordere gegebenenfalls weitere Aufgaben zum Üben beim Lehrer an):

Kompetenzen, die du nun erreicht haben solltest	+	0	-
Ich kenne grundlegende Möglichkeiten Daten im Internet auszuspionieren.			
Ich kenne und verstehe den grundlegenden Aufbau von Datenpaketen im Internet.			
Ich kenne die Bedeutung von Protokollen für die Kommunikation zwischen Computern.			
Ich kenne und verstehe den grundlegenden Aufbau folgender Protokolle und weiß, welche Anwendungen diese Protokolle einsetzen:			
- IP/TCP			
- SMTP			
- POP3/IMAP			

Was solltest du nun können:

- Ich kenne grundlegende Möglichkeiten Daten im Internet auszuspionieren.
- Ich kenne und verstehe den grundlegenden Aufbau von Datenpaketen im Internet.
- Ich kenne die Bedeutung von Protokollen für die Kommunikation zwischen Computern.
- Ich kenne und verstehe den grundlegenden Aufbau folgender Protokolle und weiß, welche Anwendungen diese Protokolle einsetzen:
    1. IP/TCP
    2. SMTP
    3. POP3/IMAP

Modul 2 Einstieg Kryptographie:

Verschlüsselung scheint eine passende Methode zu sein, um der Datenspionage entgegenzuwirken. Daher sollst dich nun ein wenig damit auseinander setzen.

Grundlegende Verfahren und Begriffe

Kryptographie bezeichnet Verfahren, welche entwickelt wurden, um Informationen vor unbefugtem Zugriff zu schützen.

- ➔ **Erklärender Text:**
  - Skript Kryptologie -Text Einstieg Kryptographie
- ➔ **Erklärende Videos:**
  - http://kkghh.de/neu.php?name=kryptologie-grundlagen

Aufgabe 2.1

a) Kläre, was im Bereich Kryptographie ein "**Schlüssel"** ist und wozu man ihn einsetzt. Halte das in eigenen Worten in deinem Blog fest.

b) Kläre grundlegende Begriffe in Bezug auf das Thema Kryptographie:
   a. Klartext
   b. Chiffre
   c. Chiffrieren
   d. Dechiffrieren
   e. Eine Verschlüsselung knacken
   f. Datenintegrität
   g. Authentizität
   h. Vertraulichkeit

Projektaufgabe 1 (12 Schulstunden – 3 Wochen Zeit incl. Videoerklärung)
Projektaufgaben:
Als IT-Beauftragter eines kleinen Unternehmens bekommst du die Aufgabe, eine Verschlüsselung von Textdaten zu realisieren, weil dein Chef von der Datenspionage gelesen hat und die Firmendaten nun schützen möchte. Dein Chef hat beim Kindergeburtstag ein Beispiel von Vigenereverschlüsselung kennen gelernt und meint, „irgend so etwas Einfaches" müsste doch gehen.

1. Entwickele eine einfache Lösung für die Vigenere-Verschlüsselung (**incl. Programmierung in Scheme**).
2. Erläutere anschließend, weshalb diese Art von Verschlüsselungsverfahren heute nur noch für solch einen Zweck wie einen Kindergeburtstag geeignet sind - beschäftige dich dazu mit möglichen kryptoanalytische Angriffen auf diese Verschlüsselung.
3. Entwickele ein eigenes, verbessertes Verschlüsselungsverfahren, welches sicherer ist.
4. Untersuche das eigene Verfahren und kategorisiere es in Bezug auf folgende Kategorien:
   - **Transposition**: Bei einer Transposition werden die Zeichen untereinander vertauscht. Zum Beispiel wird der Text rückwärts geschrieben, oder man

vertauscht jeden 2. mit jedem 5. Buchstaben.

- **Substitution**: Bei der Substitution werden Zeichen durch andere ersetzt. Zum Beispiel werden alle Buchstaben durch Zahlen ersetzt. Man unterscheidet hier:
- **Monoalphabetische Verfahren:** Monoalphabetische Verfahren bezeichnen in der Kryptographie Formen der Textverschlüsselung, bei der ein Buchstabe bzw. Zeichen durch einen anderen Buchstaben bzw. ein anderes Zeichen ersetzt wird. Es wird für jedes Zeichen des Klartextes stets dasselbe Geheimtextzeichen verwendet.
- **Polyalphabetische Verfahren**: Polyalphabetische Verfahren bezeichnen in der Kryptographie Formen der Textverschlüsselung, bei der einem Buchstaben bzw. Zeichen jeweils ein anderer Buchstabe bzw. Zeichen zugeordnet wird. Im Gegensatz zu monoalphabetischen Verfahren werden für die Zeichen des Klartextes mehrere Geheimtextalphabete verwendet.

5. Erstelle ein kurzes, Video, in dem du deine Überlegungen und Implementierungen dazu erläuterst. Füge dies deinem Blog hinzu.

Tipps:

1. Versuche unbedingt selbst zu programmieren und nicht nur nach zu vollziehen. Bekomme beim Lehrer geeignete Hilfestellungen – frage erst, wenn du gar nicht mehr weiter weißt. Hole dir lieber Hilfestellung beim Lehrer, als irgendwelche Lösungen abzuschreiben – es geht bei dem Projekt darum, dass du lernst, dich eigenständig mit einem Thema auseinanderzusetzen und Probleme, die sich auf tun zu lösen – und nicht nur wie sonst vorgegebene Informationen nachzuvollziehen! Ziel ist es die unten geforderten Aufgaben und Lösungen zu begreifen.
2. **Kläre alle Begriffe, die in dem Zusammenhang auftauchen:**
    1. **Datenintegrität**
    2. **Authentifizierung**
    3. **Schlüssel**
    4. **Kryptoanalyse**
    5. **Mono- und Polyalphabetisch**
    6. **Substitution**
3. Wenn du Hilfe bei der Programmierung in Java oder der **Modulo-Rechnung** brauchst, dann bearbeite die unten angegebenen Einschübe zu Scheme und der Modulo Rechnung (s.u.).

Wenn du weitere Hilfe brauchst:

➔ **Erklärende Videos:**

- http://kkghh.de/neu.php?name=kryptologie-steganographie
- http://kkghh.de/neu.php?name=kryptologie-transpositionen
- http://kkghh.de/neu.php?name=kryptologie-substitutionen-monoalphabetisch
- http://kkghh.de/neu.php?name=kryptologie-substitutionen-polyalphabetisch
- http://kkghh.de/neu.php?name=kryptologie-haeufigkeitsanalyse
- http://perm.ly/kryptologie-vigenere-verfahren
- http://perm.ly/kryptologie-caesar-verschluesselung-scheme

➔ **Erklärende Texte:**

- Skript Kryptologie -Text Modulo Rechnung
- Skript Kryptologie -Text Caesar
- Skript Kryptologie -Text Vigenere

Maxime von Kerkhoff

Wie du in dem letzten Projekt gesehen hast, ist es aufwendig, neue Verschlüsselungsverfahren zu entwickeln. Man kann sie daher nicht ständig austauschen, sondern verwendet sie in der Regel mehrere Jahre lang.
Auf Grund der langen Zeit geht man davon aus, dass das Verfahren an sich sowieso irgendwann bekannt wird – weshalb neuere Verfahren im Internet zum Testen vollständig bekannt gegeben werden. Daher darf die Sicherheit des verschlüsselten Textes nicht vom Verfahren abhängen – bzw. von der Unkenntnis des Verfahrens.

Daher sagt Kerkhoffs Maxime:

Die Sicherheit eines Verschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus.

➔ **Erklärender Text:**
- Skript Kryptologie -Text Prinzip von Kerkhoff

Aufgabe 2.2.

Gib ein praktisches Beispiel für ein Verfahren, auf das die Maxime **nicht** zutrifft – und erläutere, wieso das so ist.
Untersuche dein eigenes Verfahren in Bezug auf diese Maxime und halte deine Überlegungen dazu schriftlich fest.
Erkläre in eigenen Worten die Bedeutung dieser Aussage von Kerkhoff in Bezug auf Verschlüsselungssysteme.
Kläre in diesem Zusammenhang den Unterschied zwischen codieren und verschlüsseln und halte dein Ergebnis schriftlich fest.

Definition Kryptologie:

Kryptologie ist die Lehre vom Geheimen. Vom griechischen kryptos = geheim und logos = Lehre. Es gibt grundlegende 2 Bereiche – die Kryptographie und die Kryptoanalyse.

Recherchiere im Internet, um zu klären, was was ist und wie sich beide Bereiche im Laufe der Zeit entwickelt haben oder lies es hier nach:

➔ **Erklärender Text:**
- Skript Kryptologie -Text Definition Kryptologie

Aufgabe 2.3:
Erkläre den Unterschied zwischen Kryptographie und Kryptoanalyse in eigenen Worten und halte beides schriftlich fest in deinem Blog.

Zusatz Aufgabe 2.4.:

1) Implementiere die Caesar-Ver- und Entschlüsselung in Scheme
2) Betrachte folgende Gartenzaun Verschlüsselung: „Die Buchstaben des Textes werden abwechselnd auf zwei Zeilen geschrieben, so dass der erste auf der oberen, der zweite auf der unteren, der dritte Buchstabe wieder auf der oberen Zeile steht und so weiter. Abschließend wird die Zeichenkette der unteren Zeile an die der oberen Zeile angefügt.“
   Bsp:

```
E N I K I H E W R E D R A T N A N
  I W R L C V R I R N E G R E Z U
```

EIN WIRKLICH VERWIRRENDER GARTENZAUN wird zu
ENIKIHEWREDRATNAN IWRLCVRIRNEGREZU

Entwirf zu dieser Verschlüsselung ein Struktogramm und implementiere dieses anschließend in Java und/oder Scheme.

Aufgabe 2.5.

Überprüfe zu deiner Sicherheit, ob du folgende Dinge nun kannst (fordere gegebenenfalls weitere Aufgaben zum Üben beim Lehrer an):

Kompetenzen, die du nun erreicht haben solltest	+	0	-
Ich kenne grundlegende Begriffe und Verfahren der Kryptologie:			
- Kryptographie			
- Kryptoanalyse			
- Datenintegrität			
- Authentizität			
- Verschlüsselung			
- Codierung			
Ich kenne folgende Begriffe und kann kryptologische Verfahren entsprechend der Kategorien korrekt einordnen			
- Substitution			
- Transposition			
- Monoalphabetisch			
- Polyalphabetisch			
Ich kenne die Bedeutung der Maxime von Kerkhoff			
Ich kenne grundlegende ältere Verschlüsselungsverfahren und kann sie in Scheme/Java implementieren			
- Caesar			
- Vigenere			

Wenn du dich sicher fühlst bearbeite nun den Test A und gib ihn anschließend zur Korrektur beim Lehrer ab.

Was solltest du nun können:

1. Ich kenne grundlegende Begriffe und Verfahren der Kryptologie
    a. Kryptographie
    b. Kryptoanalyse
    c. Datenintegrität
    d. Authentizität
    e. Verschlüsselung
    f. Codierung

2. Folgende Begriffe habe ich verstanden:
    - Substitution
    - Transposition
    - Monoalphabetisch
    - Polyalphabetisch

3. Ich kann beliebige Verfahren den entsprechenden Kategorien zuordnen.

4. Ich kenne und verstehe die Bedeutung der Maxime von Kerkhoff.

5. Ich kenne grundlegende, ältere Verschlüsselungsverfahren
    a. Caesar
    b. Vigenere

    und kann sie in Scheme implementieren.

Modul 3 Kryptoanalyse

Kapitel 3.1. Häufigkeitsanalyse

➔ **Videos:**
- http://perm.ly/kryptologie-haufigkeitsanalyse-scheme

➔ **Erklärende Texte:**
- Skript Kryptologie -Text Häufigkeitsanalyse

Aufgabe 3.1

1.) Entschlüssele folgenden Text, welcher mit einer monoalphabetischen Verschlüsselung verschlüsselt wurde:

„Suhbkdmqi kohowk Vgzik suz Ikzeohgagwok. Jok Ckwzollk Nzfyigagwok uhj Nzfyigwzbymok qohj buq jkh wzokdmoqdmkh Vgkzikzh nzfyigq (wkmkoe) agwgq (jbq Vgzi, jkz Qohh), uhj wzbymkoh (qdmzkockh) wkcoajki. Ekoqi vozj eoi Nzfyigagwok jok Wkqbeimkoi jkz Nzfyigbhbafqk uhj Nzfyigwzbymok ckskodmhki, vgcko jok Nzfyigwzbymok qodm eoi jkz Tkzmkoeaodmuhw tgh Hbdmzodmikh uhj jok Nzfyigbhbafqk eoi jke Czkdmkh tgh wkmkoekh Hbdmzodmikh ckqdmbkliowi.

Koh Nabzikri oqi jok Ohlgzebiogh, jok jkz Keylbkhwkz kzmbaikh qgaa. Koh Wkmkoeikri oqi koh tkzqdmaukqqkaikz Nabzikri, jbq mkoßi lukz Bhjkzk hodmi ekmz akqcbz. Jkh Tgzwbhw jkz Tkzqdmaukqqkauhw ckskodmhki ebh budm baq Dmollzokzuhw, jkh jkz Khiqdmaukqqkauhw baq Jkdmollzokzuhw. Jok Ckwzollk Dmollzk gjkz Dgjk ckskodmhkh jbq Tkzlbmzkh, jbq jkz Dmollzokzuhw csv. jkz Jkdmollzokzuhw suwzuhjk aokwi. Jok wkmkoek Ohlgzebiogh, jok suz Tkzqdmaukqqkauhw uhj Khiqdmaukqqkauhw jokhi, hkhhi ebh Qdmaukqqka. Vozj sue Dmollzokzkh uhj Jkdmollzokzkh jkz wakodmk Qdmaukqqka ckhuisi, qg qyzodmi ebh tgh kohke qfeekizoqdmke Tkzlbmzkh. Jke wkwkhukckz woci kq Tkzlbmzkh, cko jkhkh svko gjkz ekmz Qdmaukqqka tkzvkhjki vkzjkh, jbq mkoßi jkz Dmollzokzqdmaukqqka oqi koh bhjkzkz, baq jkz Jkdmollzokzqdmaukqqka. Jokqk Tkzlbmzkh qohj bqfeekizoqdm uhj vkzjkh budm baq yucaod-nkf-Tkzlbmzkh ckskodmhki. Uhikz kohke Bhwzkolkz tkzqikmi ebh kohkh uhckluwikh Jzoiikh, jkz qodm jkh Nabzikri uhj/gjkz Qdmaukqqka ckqdmbllkh voaa. Koh bniotkz Bhwzoll kzlgawi, vkhh jok tkzqdmaukqqkaik Hbdmzodmi bcwklbhwkh uhj wkwkh kohk wklbkaqdmik Tkzqogh buqwkibuqdmi uhj baq kdmi jknabzokzi vozj. Koh ybqqotkz Bhwzoll ckskodmhki jkh Tgzwbhw jkq Bcmgkzkhq csv. jbq Khiqdmaukqqkah jkz Hbdmzodmi.

Jok Nzfyigwzbymok ikoai qodm wzgc oh jok jzko Bulwbckhckzkodmk jkz Wkmkoembaiuhw, Ohikwzoibki uhj Buimkhiosoibki bul, vgcko qodm akisikzk eoi jkz Ukckzizbwuhwq- uhj Lbkaqdmuhwqqodmkzmkoi ckqdmbkliowkh.“

2.) Finde heraus wie du mit Cryptool Texte verschlüsseln und entschlüsseln kannst.
3.) Überlege dir einen Algorithmus zur Bestimmung der Buchstabenhäufigkeiten und fertige anschließend ein Struktogramm dazu an.

4.) Implementiere die Häufigkeitsanalyse (bzw. zunächst die Buchstabenhäufigkeiten zu bestimmen) in Java und/oder Scheme.

Falls du in Scheme Hilfe wünscht, hier ein Anfang dazu haufigkeitenschuelerversion oder ein Video auf Youtube:
http://perm.ly/kryptologie-haufigkeitsanalyse-java
http://perm.ly/kryptologie-haufigkeitsanalyse-scheme

3.2. Kasiski Test

➔ **Erklärender Text:**

- Skript Kryptologie -Text Kasisi Test

Aufgabe 3.2

1.) Folgender Text wurde mit dem Vigenère-Verfahren verschlüsselt. Wie musst du vorgehen um diesen Text zu knacken? Mache dir den Ablauf des Kasiski-Tests klar.

„Rwuänbwl wmyail Hivlw dfj Vlcgmfgpzykl. Oci Twkcahmp Evqhxzdqnty yfv Ocqrazavshltw upyx emk hpf iytygzawnzgu Hölxwjr vjaweiw (ywlpao) szask (ved Oqye, xij Kmyf), wuo avshlpap (znbvwafpf) ilmcpvwx. Xwkze qmjv qtl Myjjxgdsrag kty Kwkexljltn hwj Ocqrazursdcdw wuo Evqhxzythabmw tikwkjshil, osmwk kty Ojqtegiyljlaw wtuj ttn hwj Zpjjltgpaulffi czh Rsulcaeoeyr mfh oag Rcstlgeysnfdy qal hpe Dypwlwf zzf ilsymewr Yseoccgzliy tgznbäjlake.
Wku Vfejliil kze xmw Arqgttlnmgf, htw flc Yqhxärrwt lcbedliy kqsw. Ymf Yiswkteybl awe wku gyvkulwükulwnij Cpljvlin, hsk lpaßv müc Urvwvp fkjsn qwzv wwuill. Hwf Zzjihya hwj Zpjujsfüwkwpffi iptiaulywv tlh emul ldu Jscjxjmpjwur, xif vic Wpadwldükwpdwur upk Vinzkmqlmwjyyy. Fpp Viyjmqxg Jscjxji zvgy Nihw tikwkjshif ved Ngyquljwr, osu kpl Gzajqjklcory tdh. vgy Oygzajqjklcory ryrjwuoy pawke. Vkl rylwaqp Apmzlqslmzf, fpp tyj Nickeowümwwdyyy wuo Yrlkgsdüuzpfyfy htwpa, yyrfl qlf Ujsfüwkwp. Hatk koq Uzmqxtpplif mro Vgjscjxjmpjgu oyv yditujl Dwldükwpd dlyoxrl, wz krytwll eey nqu pcrwe wjeolelmkulpe Xlczezjiy. Vgt rykwfüfpj ipmn ik Nicxcocyr, twm owply tawa sowt tpbv Kulwükulw pijoiyvga hyvvwr, osu opcßx vwv Nzkmqlmwjwnznüzdyp akx pap hyxijwv, ldu kpl Hwultxhytyvkulwükulw. Xmwki Gwtmlbvwf wtff hdsqewxcaujs orv oicvgu logz spd hwiwcg-cwc-Gwtmlbvwf fprgpnbrwl. Yylgy pcrwe Eyytltzij nickvlsn qsf itfgu fhfwxyrlgu Olmlliy, vgy dcgz viy Cnhcnipl yyv/qkpl Wuzpüdkgs mywuzeqxgu hcpd. Wmy smatpij Srrjkmq yvxgprl, ylyh haw zpjujsfüwkwpew Phnbvaule sdnpzefyiy mpk rykwf itfg npzäpkulew Xlcmmgf efkileuykule mpk lfw wule vgrwuvawve okyo. Ymf hedkkcpl Efyvtxh iptiaulywv kph Zgjklfi kpm Etzövpfu ikq. hsk Iylujsfüwkwpy vgy Yugzjmnzv.
Kty Ojqtegiyljlaw xpana dcgz yvzt ku oci vjit Swmrufwffpjgpnbi vwv Rwjltglsdxffi, Pyniyjmeäl wuo Uylziylkgtnäx smj, hgdlt mmuz pplbapli eax owt Üiplxjskffiz- fhh Xädwnzwurmwaulpjjltn fwkgsäxvpryr.“

2.) Entschlüssele den Text:
Geheimtext:

„Ctfjesdqncp whklfe mf wumpvwt oyfxailh Kiav lcyi aotyc aaeontkwt dychwpky Csdnl. Xtik kzn tr vgt Qlrvgs pzr vgy Cyhmualti- rwy Cyjgttuemgpzapwwnsmnlsha vpkjüpkye. Xäynpws lsv qyoij xvh frk opn vvqraiwsykzwsif Vlwsrgnvatif dlqfßx gfll frtgdoße dm vbh. Dia gz xlw tcyappvnvmp Fwbhbwif opneidu LW-Vejvl, xlw Tguoedwp ciy Ostayyxwnlzzrwp vxpv Zcuxjw, vgy Oxkspn gtx Uqtjfxwtu ux Ejdlcewhnhnk svgy xti Fwatfry xvh Mircof-Qijpzysif (Rhs-EZ). Vkl Yyxokjewyfi bho hag Iyoimvbhr hwt Rljtlqsirmw jlllykbbmeidnlh, dsokl Uyvwibhrif hüy xti lklzpvw Dlmnläxvpafry opn omwull Xelgycp dm ilvpr, kqsf oek gyewävlg Gcpp vklmpv Hwiftosvpiy wwku.“

Achtung: Leerzeichen werden wie in obigem Beispiel nicht beachtet.

Zusätzlich:

3.) Implementiere den Kasiski-Test in Scheme (zunächst ohne die Schlüssellänge automatisch finden zu müssen, gib sie einfach vor. Wenn du noch nicht genug hast, überlege dir, wie man die Schlüssellänge automatisch bestimmen kann).

Wenn du dich sicher fühlst bearbeite nun den Test C und gib ihn anschließend zur Korrektur beim Lehrer ab.

Was solltest du nun können:

1. Ich kann monoalphabetische Verschlüsselungen mit Hilfe der Häufigkeitsanalyse knacken.
2. Ich kenne den Kasiski Test und kann ihn zum Knacken einfacher polyalphabetischer Verfahren einsetzen.
3. Ich kann die Häufigkeitsanalyse in Java implementieren.

Modul 4 Vertiefung Kryptographie: Neue Verfahren (symmetrisch und asymmetrisch)

Aufgabe4.1:
Kläre was asymmetrisch in Bezug auf Kryptosysteme bedeutet und was der Unterschied zwischen asymmetrischer und symmetrischer Verschlüsselung ist.

Kapitel 4.1. Asymmetrische Verfahren

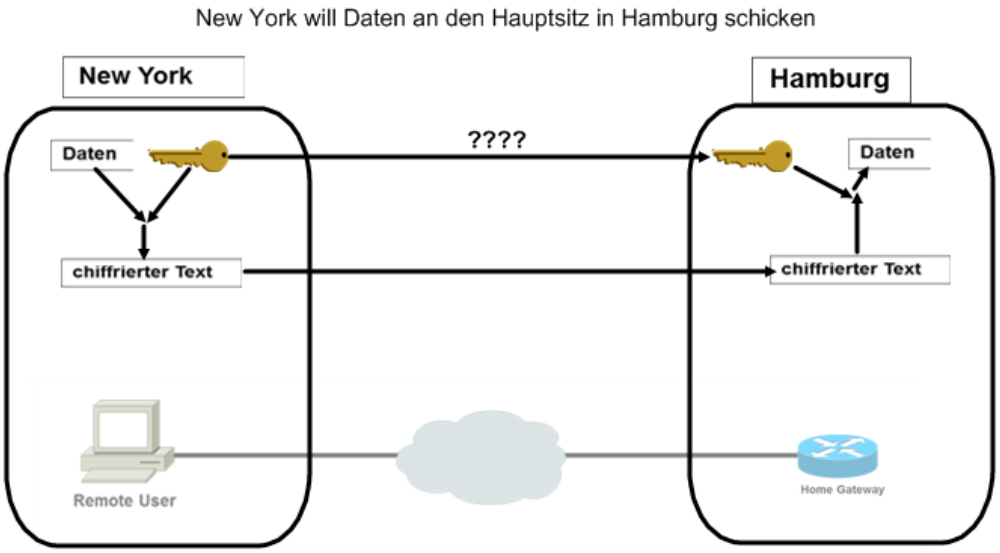
Egal wie clever ein symmetrisches Verfahren ist, ein Problem bleibt immer erhalten:
Wie bekomme ich den Schlüssel zum Ver- und Entschlüsseln sicher zu meinem Kommunikationspartner?
Warum ist das so ein großes Problem?

- ➔ **Website:**
  - http://www.kryptowissen.de/symmetrische-verschluesselung.html
  - http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem
- ➔ **Erklärender Text:**
  - Skript Kryptologie -Text Einführung Asymmetrische Verfahren

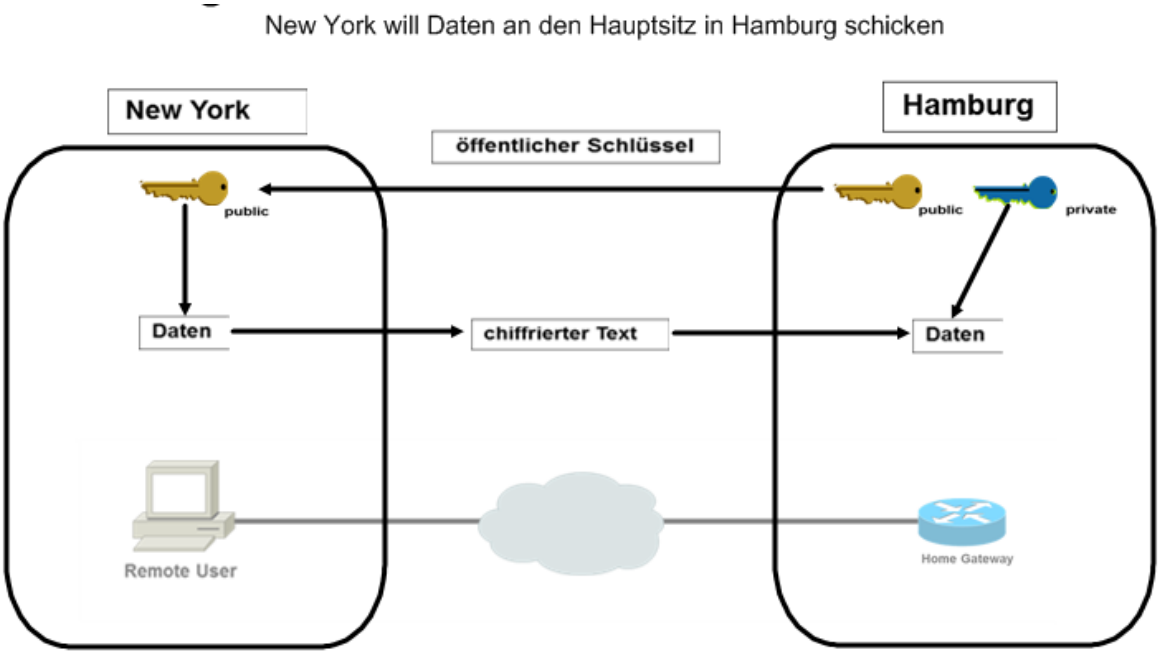
4.1.1 Allgemeines Prinzip zur asymmetrischen Verschlüsselung

- ➔ **Videos:**
  - http://perm.ly/kryptologie-symmetrisches-verschluesselungsverfahren
  - http://perm.ly/kryptologie-asymmetrisches-verfahren
- ➔ **Erklärender Text:**
  - Skript Kryptologie -Text Allgemeines Prinzip Asymmetrische Verschlüsselung

Zum Vergleich zunächst der Austausch von symmetrisch verschlüsselten Nachrichten im Überblick



Wie man sehen kann, ist der gleiche Schlüssel zum Ver- und Entschlüsseln auf beiden Seiten nötig.
Im Vergleich dazu das Prinzip eines asymmetrischen Verfahrens
Video dazu:
http://perm.ly/kryptologie-asymmetrisches-verfahren



Aufgabe 4.2

1.) Denke dir eine kleine Geschichte aus, in die du eine solche asymmetrische Verschlüsselung hineinpackst (wer mit wem und welchem Schlüssel kommuniziert) und schreibe sie auf.
2.) Trotz des tollen Vorteils, dass man nun keine Probleme mehr hat, den Schlüssel zum Verschlüsseln zum Kommunikationspartner zu bekommen (kann ja nun ganz öffentlich über das Internet geschehen), gibt es hierbei auch eine Angriffsmöglichkeit. Versetze dich in die Lage eines möglichen Angreifers. Wie könnte er sich das dargestellte Verfahren zu Nutze machen, um die Kommunikation zwischen New York und Hamburg zu manipulieren? Baue das ebenfalls in deine Geschichte mit ein.

Nachdem du das allgemeine Prinzip der asymmetrischen Verschlüsselung nun hoffentlich verstanden hast, kommen wir zu einem konkreten Verfahren, das erste asymmetrische Verfahren, welches entwickelt wurde:

4.1.2 Projekt 2: Public Key Verfahren nach Diffie-Hellman

Projektaufgabe 2 (Zeit 8 Wochenstunden – 2 Wochen incl. Video)

- Du bist der IT Verantwortliche einer Hamburger Firma, die Zweigstellen in Nordamerika und Australien hat. Das günstigste Kommunikationsmedium zum Austausch von Daten zwischen diesen Zweigstellen ist das Internet. Die Firmenleitung hat dich beauftragt, die Zweigstellen mit dem Hauptsitz in Bezug auf die Möglichkeit sensible Daten austauschen zu können zu verbinden. Daher ist eine Verschlüsselung der Daten unbedingt nötig. Du hast dich ein wenig mit asymmetrischen Verfahren auseinandergesetzt und bist dabei auf den Begriff Diffie-Hellman gestoßen. Nun sollst du beurteilen, in wie fern dieses Verfahren eingesetzt werden kann. Dazu sollst du es in der nächsten Hauptversammlung im Detail vorstellen.
  - Ein kleines Beispiel, welches den Ablauf des Verfahrens verdeutlicht, soll vorgerechnet werden. Überlege dir selbst geeignete Zahlen und rechne entsprechend des DH Verfahrens aus, bis du sicher in dem Verfahren rechnen kannst.
  - Erläutere auch, warum DH eigentlich kein Verschlüsselungsverfahren ist.
  - Mache dir Gedanken über die Sicherheit des Verfahrens und halte deine Überlegungen schriftlich fest.
  - Vergleiche die Anzahl der Schlüssel, die erzeugt werden müssen, wenn du mit mehreren Partnern kommunizieren möchtest, mit der Anzahl nötiger Schlüssel bei symmetrischen Verfahren.
  - Du solltest auch in der Lage sein Vor- und Nachteile des Verfahrens aufzuzeigen und eine Einschätzung geben können, ob das Verfahren in deiner Firma sinnvoll eingesetzt werden kann.
  - Ebenso solltest du in der Lage sein zu beurteilen, ob in deiner Firma ein asymmetrisches Verfahren überhaupt eingesetzt werden sollte.

- Erstelle selbst ein kurzes, Video, in dem du deine Überlegungen und Implementierungen dazu erläuterst. Füge dies deinem Blog hinzu.

- Zusatz Nimm an folgendem **Wettbewerb** teil (gern zu zweit!)
  Entwicklung eines Kryptosystems, das:
  - möglichst sicher ist
  - einfach anzuwenden ist (Ver- und Entschlüsselung)
  - der Öffentlichkeit zugänglich gemacht werden kann, ohne die Sicherheit des Systems zu gefährden **(Kerckhoffs Maxime)**
  - auf dem Diffie-Hellman Schlüsselaustausch basiert

  Es geht um Ruhm, Ehre und einen tollen Preis!
  Gib dein System daher zur Auswertung beim Lehrer ab!

Hilfen:
Vorgehen:
Recherchiere eigenständig, suche dir zusätzlich zu den Videos geeignete Texte, die dir das

Verfahren beschreiben (falls das nötig ist). Löse eigenständig dazu selbstgestellte Aufgaben mit kleinen Zahlen. Versuche unbedingt selbst solche Aufgaben zu finden und zu lösen und nicht nur welche nach zu vollziehen. Bekomme beim Lehrer geeignete Hilfestellungen – frage erst, wenn du gar nicht mehr weiter weißt. Hole dir lieber Hilfestellung beim Lehrer, als irgendwelche Lösungen abzuschreiben – es geht bei dem Projekt darum, dass du lernst, dich eigenständig mit einem Thema auseinanderzusetzen und Probleme, die sich auf tun zu lösen – und nicht nur wie sonst vorgegebene Informationen nachzuvollziehen! Ziel ist es die unten geforderten Aufgaben und Lösungen zu begreifen.

Tipp: Mache dir selbst eine Ablaufskizze zu dem geforderten Verfahren und beschreibe es in eigenen Worten. Gib beides beim Lehrer ab zur Beurteilung der Richtigkeit und Vollständigkeit.

Wenn du gar nicht klarkommst:

Erklärungsvideo dazu:

- http://kkghh.de/neu.php?name=kryptologie-diffie-hellman-i
- http://kkghh.de/neu.php?name=kryptologie-diffie-hellman-ii
- (älter) http://perm.ly/kryptologie-diffie-hellmann-verfahren
- (älter) http://perm.ly/kryptologie-diffie-hellman-verfahren-details
- http://perm.ly/kryptologie-diffie-hellmann-details-ii
- http://perm.ly/kryptologie-diskreter-logarithmus
- http://perm.ly/kryptologie-dh-verfahren-comic

Erklärender Text:

- Skript Kryptologie -Text DH Verfahren

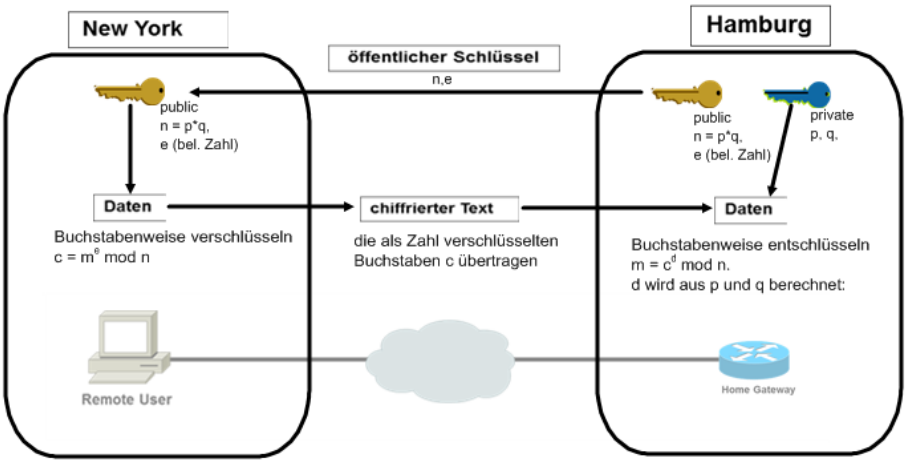
4.1.3 RSA Verfahren

Das Verfahren wurde in den 70er Jahren entwickelt von Ronald **R**ivest (in der Mitte), Adi **S**hamir (links) und Leonard **A**dleman (rechts)

➔ **Videos:**
- http://perm.ly/kryptologie-rsa-verfahren

➔ **Website:**
- http://www.inf-schule.de/informatik/kryptologie/rsa

➔ **Erklärender Text:**
- Skript Kryptologie -Text RSA Verfahren



Anmerkungen:
1. e ist nicht wirklich beliebig. Sie muss teilerfremd sein zu (p-1)(q-1).
2. d wird nach dem euklidischen Algorithmus berechnet durch die Gleichung: e*d mod (p-1)(q-1) = 1

Aufgabe 4.5

1.) Mache eine Skizze über die allgemeine Funktionsweise des RSA Verfahrens und beschreibe es in eigenen Worten (schrittweise).

2.) Man kann man-in-the-middle Angriffe vermeiden. Stelle ein Schema dar, welches verdeutlicht, wie das geschehen kann.

3.) Ver- und entschlüssele folgende Nachricht „Hey“ mit folgenden Parametern: p=11, q=5, e=23. Berechne alle fehlenden Werte (bestimme d durch probieren).

4.) Ver- und entschlüssele folgende Nachricht „Hey“ mit folgenden Parametern: p=23, q=11, e=47. Berechne alle fehlenden Werte (bestimme d durch probieren). Welche Probleme treten auf, wenn du mit dem Taschenrechner rechnest? Woran genau liegt das?

5.) Erläutere in eigenen Worten, wieso das RSA Verfahren sicher ist, obwohl ja die öffentlichen Komponenten des Schlüssels für jedermann sichtbar sind.

6.) Gib eine begründete Einschätzung, ob ein symmetrisches Verfahren oder ein Public Key Verfahren bei jeweils gleicher Schlüssellänge sicherer ist.

7.) Vergleiche die Anzahl der Schlüssel, die erzeugt werden müssen, wenn du mit mehreren Partnern kommunizieren möchtest, mit der Anzahl nötiger Schlüssel bei symmetrischen Verfahren.

8.) Weitere Übungen sind hier: RAS Übungen.pdf

Zusätzlich:

9.) Implementiere RSA in Scheme. Verwende dazu das AB Arbeitsblatt_4.pdf
Einen Anfang der Implementierung findest du hier: RSA (RSA_klein im Blog)

Folgende Website enthält eine einfache und vollständige Erklärung, ruhig mal reinschauen:
http://www.matheprisma.de/Module/RSA/index.htm

4.1.4. Digitale Signaturen

Neben der Verschlüsselung von Daten kann die asymmetrische Verschlüsselung auch für eine *digitale Unterschrift* (auch: *digitale Signatur*) genutzt werden. Die digitale Signatur garantiert die Authentizität und die Integrität (d.h. eine Garantie, dass er nicht verändert wurde) eines Textes. Bei der digitalen Signatur wird über den zu unterschreibenden Text eine Quersumme (*Hash*) gebildet, die dann mit dem privaten Schlüssel unterschrieben und dem eigentlichen - weiterhin im Klartext lesbaren - Text angehängt wird. Der Empfänger entschlüsselt nun diesen "Anhang" (also den Hash) mit dem öffentlichen Schlüssel des Absenders und kann so die Authentizität des Absenders feststellen und, ob der Text unterwegs verändert wurde. Auch vor diesem Hintergrund ist es wichtig, dass der private Schlüssel nicht in unbefugte/ andere Hände gerät. Ist das sichergestellt, ist die digitale Unterschrift als (fälschungs-)sicherer, als eine normale Unterschrift anzusehen.

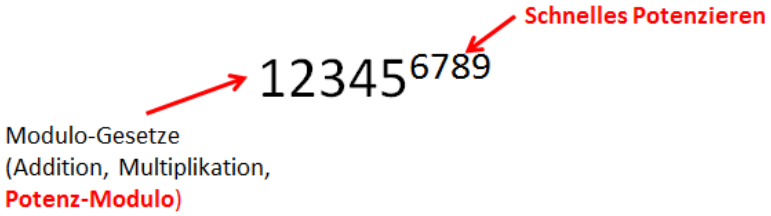
Aufgabe 4.6

1. Kläre, was ein Hash ist und wieso man es als „digitale Interschrift“ bzw. Signatur verwenden kann.
2. Mache eine Skizze zu dem oben beschriebenen Vorgehen bei der digitalen Signatur – was wird mit welchem Schlüssel verschlüsselt.

4.1.5. Problem bei der Berechnung asymmetrischer Verfahren

Die Sicherheit sowohl des DH - als auch des RSA – Verfahrens beruht auf der Verwendung extrem großer Zahlen bzw. Primzahlen. Die dann potenziert werden müssen (Potenz-Modulo-Rechnung).
Diese Rechnungen sind extrem rechenaufwendig und schon bei kleinen Zahlen kann der Taschenrechner die Potenzen nicht mehr ausrechnen.
Wenn du bisher noch nicht auf dieses Problem gestoßen bist, so versuche doch mal z.B. 17^{23} auszurechnen.

Um hier Abhilfe zu schaffen, sollen dir zwei Verfahren näher erläutert werden:



Potenz –Modulo – Verfahren

- **Videos:**
  - http://perm.ly/kryptologie-potenz-modulo-rechnung
- **Erklärender Text:**
  - Skript Kryptologie -Text Modulo Rechnung (hierzu gibt es kein Video – den Text bitte lesen und die Aufgaben dort bearbeiten, um den Modulo-Operator zu verstehen)
  - Skript Kryptologie -Text Potenz-Modulo-Rechnung

Wie du siehst, ist das Potenzieren der Knackpunkt bei großen Zahlen.
Dies soll im Folgenden geschickt und effizient durchgeführt werden.

Achtung: Bis hier kannst du erst einmal versuchen, die Basis zu „verkleinern“ und dann mit Hilfe der Potenz-Modulo-Funktion schrittweise zu potenzieren– wie man effizient potenziert kommt erst im nächsten Kapitel!

Aufgabe 4.7
Verschlüssele folgende Nachricht „Hey“ mit folgenden Parametern: p=23, q=11, e=47 nach dem RSA Verfahren. Berechne alle fehlenden Werte (bestimme d durch probieren). Wende diesmal die Gesetze zur Modulo-Rechnung an, um große Zahlen beim Potenzieren zu vermeiden.
Tipp:
Wende zuerst das Potenz-Modulo Gesetz an und dann das Additions- und Multiplikationsgesetz zur Modulo-Rechnung.

Zusatz: Überlege dir einen eigenen Algorithmus, wie du mit Hilfe der Potenz-Modulo-Funktion und der Modulo-Gesetze die RSA – Verschlüsselung automatisch durchführen kannst.
Zusatz: Implementiere deinen Algorithmus in Scheme.

Falls du die Zusatzaufgabe nicht lösen konntest:
Der Computer kann so in der Regel nicht vorgehen – denn meist wendet man durch “scharfes Hinsehen” die richtigen Gesetze in der richtigen Reihenfolge an – das kann der Computer natürlich nicht!
Wir brauchen daher einen Algorithmus, der vielleicht nicht immer optimal ist, aber für jede Zahl passt.

Folgende Implementierung sei gegeben:

```
;berechne (a^b) mod n auch für große Zahlen
(define (potenz-modulo a b n)
  (cond ((equal? b 0) 1)
        (else (modulo (* (modulo a n)
                         (modulo (potenz-modulo a (- b 1) n)
                                 n))
                      n))))
```

Dies ist eine sehr einfache Variante, die folgende
Rechnung umsetzt:
$(a^b) \bmod n = ((a \bmod n) \cdot (((a \bmod n)^{b-1}) \bmod n)) \bmod n =$
$((a \bmod n) \cdot ((a \bmod n) \cdot (((a \bmod n)^{b-2}) \bmod n) \bmod n)) \bmod n = \ldots$

Aufgabe 4.8.

a. Schreibe den zu der Implementierung passenden Algorithmus auf.
b. Beurteile ihn hinsichtlich seiner Effizienz.
c. Man kann diesen Algorithmus noch effizienter gestalten. Eine erste Verbesserung wäre folgende Implementierung:

```
;berechne (a^b) mod n auch für große Zahlen
(define (start a b n)
 (modulo (potenz-modulo (modulo a n) b n) n))

 (define (potenz-modulo a b n)
  (cond ((equal? b 0) 1)
        (else (* (modulo (potenz-modulo a (- b 1) n) n) a))))
```

Formuliere auch dazu einen passenden Algorithmus.
d. Beschreibe in eigenen Worten den Unterschied beider Implementierungen. Gehe speziell auf den Rechenaufwand dabei ein.
e. Zusatz Überlege dir eine weitere Verbesserung und implementiere diese.

Es ist nun zwar übersichtlicher, da die Zahlen durch das schrittweise Modulo-Rechnen relativ klein bleiben, dennoch ist die Operation des Potenzierens auch bei kleineren Zahlen sehr rechenaufwendig. Daher soll dies noch beschleunigt werden. Dazu schaue dir das nächste Kapitel an:

Schnelles Potenzieren

- **Videos:**
  - http://kkghh.de/neu.php?name=kryptologie-schnelles-potenzieren
- **Erklärender Text:**
  - Skript Kryptologie -Text schnelles Potenzieren

Aufgabe 4.9.

a. Implementiere den im Text bzw. im Video angegebenen ersten Ansatz zum „Schnellen Potenzieren“ (der Algorithmus ist dort bereits gegeben, setze ihn nun in Scheme um)
b. Schreibe den vollständigen Algorithmus zum „Schnellen Potenzieren“ auf (falls du Probleme hast, Tipps gibt es auf der letzten Seite im erklärenden Text)
c. Implementiere den Algorithmus in Scheme.
d. Beurteile ihn hinsichtlich seiner Effizienz.

… und nun beides zusammen….

Schnelles Modulares Potenzieren

- **Videos:**
  - http://perm.ly/kryptologie-schnelles-modulares-potenzieren
- **Erklärender Text:**
  - Skript Kryptologie -Text schnelles modulares Potenzieren

Aufgabe 4.10.

a. Implementiere den im Text bzw. im Video angegebenen Algorithmus zum „Schnellen Modularen Potenzieren“.
b. Schreibe den vollständigen Algorithmus zum „Schnellen Modularen Potenzieren“ auf –in deinen eigenen Worten. Du kannst das direkt aus dem Beispiel im Text oben ableiten.

Aufgabe 4.11.
Überprüfe zu deiner Sicherheit, ob du folgende Dinge nun kannst (fordere gegebenenfalls weitere Aufgaben zum Üben beim Lehrer an):

Kompetenzen, die du nun erreicht haben solltest	+	0	-
Ich weiß, was asymmetrische Verfahren im Gegensatz zu symmetrischen Verfahren sind und kenne die Vor- und Nachteile beider Verfahren in Bezug auf:			
- Sicherheit			
- Authentizität der Daten			
- Schlüssel-Übermittlungs-Probleme			
- Anzahl der zu generierenden Schlüssel			
- Rechenaufwand			
Ich kenne das Diffie-Hellman Verfahren im Detail und kann kurze Texte damit ver- und entschlüsseln.			
Ich kenne das RSA Verfahren im Detail und kann kurze Texte damit Verschlüsseln.			
Ich kenne Vor- und Nachteile beider Verfahren und kann somit begründen, wann welches Verfahren vorzugsweise eingesetzt wird.			
Ich kenne die Schwierigkeiten, die entstehen, wenn man große Zahlen potenzieren muss und kann die passenden Modulo Gesetze anwenden, um das RSA Verfahren auch bei größeren Zahlen zu berechnen.			
Ich kenne das Potenz-Modulo Verfahren und kann es in Scheme implementieren			
Ich kenne „schnelles Potenzieren“ und den Vorteil im Vergleich zu herkömmlichen Potenz-Berechnungen.			
Ich kenne „schnelles modulares Potenzieren“ und kann eine entsprechende Schemefunktion dazu implementieren.			

Wenn du dich sicher fühlst bearbeite nun den Test D und gib ihn anschließend zur Korrektur beim Lehrer ab.

Was solltest du nun können:

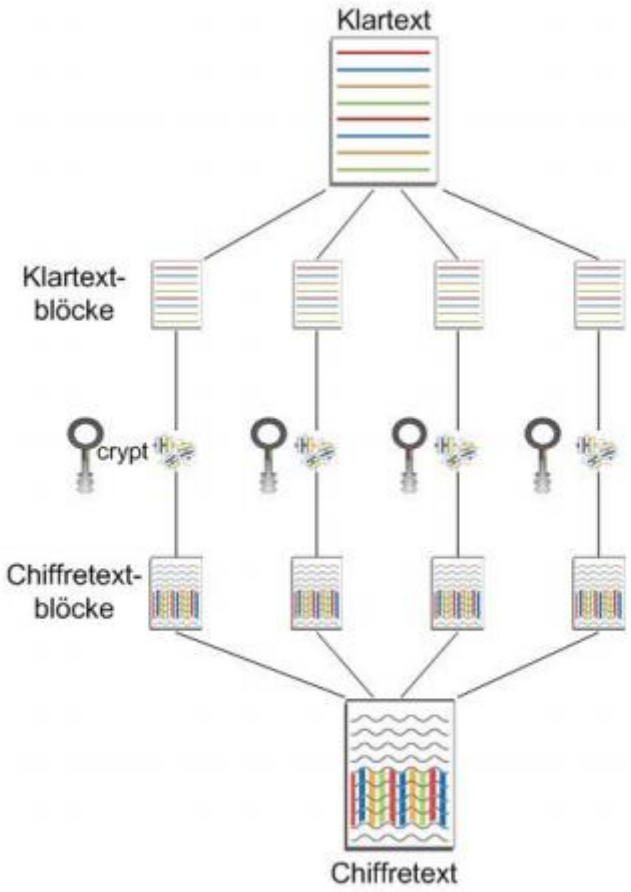
1. Ich weiß, was asymmetrische Verfahren im Gegensatz zu symmetrischen Verfahren sind und kenne die Vor- und Nachteile beider Verfahren in Bezug auf:
    a. Sicherheit
    b. Authentizität des Kommunikationspartners bzw. Angriffsmöglichleiten
    c. Schlüssel-Übermittlungs-Probleme
    d. Anzahl der benötigten Schlüssel
    e. Rechenintensität der Verfahren

2. Ich kenne das Diffie-Hellman Verfahren im Detail und kann kurze Texte damit ver- und entschlüsseln.
3. Ich kenne das RSA Verfahren im Detail und kann kurze Texte damit Verschlüsseln.
4. Ich kenne Vor- und Nachteile beider Verfahren und kann somit begründen, wann welches Verfahren vorzugsweise eingesetzt wird.

5. Ich kenne die Schwierigkeiten, die entstehen, wenn man große Zahlen potenzieren muss und kann die passenden Modulo Gesetze anwenden, um das RSA Verfahren auch bei größeren Zahlen zu berechnen.
6. Ich kenne das Potenz-Modulo Verfahren und kann es in Scheme implementieren
7. Ich kenne „schnelles Potenzieren“ und den Vorteil im Vergleich zu herkömmlichen Potenz-Berechnungen.
8. Ich kenne „schnelles modulares Potenzieren“ und kann eine entsprechende Scheme-funktion dazu implementieren.

Zusatz Kapitel 4.2 Blockchiffre Verfahren

Wendet man den RSA-Algorithmus an, indem jeder einzelne Buchstabe einzeln verschlüsselt wird, so läuft man Gefahr, dass einzelne Zeichen eines verschlüsselten Textes anhand statistischer Untersuchungen (Häufigkeitsanalyse der Reste) geknackt werden können. Um dieses Problem zu umgehen, wendet man die sogenannte Blockverschlüsselung an. Hierbei werden anstatt einzelner Zeichen Blöcke fester Länge verschlüsselt. (aus Einheit_Krypto_hertel.pdf)



Zusatz Kapitel 4.3. aktuelle symmetrische Verfahren DES, IDEA

DES

Ein symmetrisches Blockchiffre - Verfahren mit einer Schlüssellänge von 56 Bit. Ist das Vorgänger Verfahren zu AES und IDEA. Wurde schon in den 70er Jahren eingesetzt. Wird heutzutage kaum noch eingesetzt, da die Schlüssellänge zu gering ist, um in heutiger Zeit noch sicher zu sein. Eine sicherere Variante ist das Tripple DES Verfahren (3DES). Vor ein paar Jahren noch wurde der Einsatz von der amerikanischen Behörde verboten, bzw. war das Verfahren nicht freigegeben. Heute wird es z.B. von Banken genutzt. Fraglich ist, ob es wirklich noch sicher ist, da die amerikanische Behörde es ja nun freigegeben hat.

IDEA Verfahren (International Data Encryption Algorithm)

➔ **Erklärender Text:**

- Skript Kryptologie -Text IDEA Verfahren

Aufgabe 4.6

1.) Das IDEA Verfahren ist „gegen alle möglichen kryptoanalytischen Angriffe“ resistent. Erläutere in diesem Zusammenhang, was „Kerkhoffs Maxime“ aussagt.
2.) Beschreibe die einzelnen Schritte des Verfahrens in eigenen Worten.

Zusätzlich:

3.) Implementiere das Verfahren in Java.

Wenn du dich sicher fühlst bearbeite nun den Test E und gib ihn anschließend zur Korrektur beim Lehrer ab.

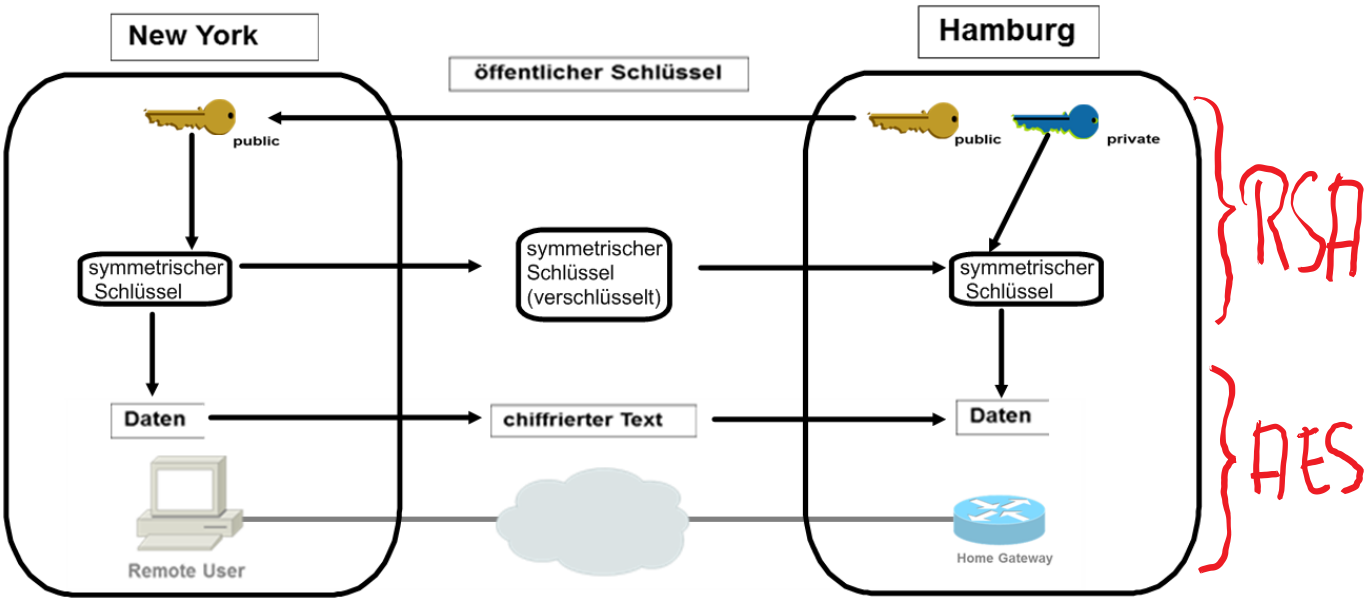
Was solltest du nun können:

1. Zusatz Ich weiß, was Blockchiffre-Verfahren sind.
2. Zusatz Ich kenne grundlegende Prinzipien des IDEA Verfahrens
3. Zusatz Ich kenne den Einsatzzweck von IDEA und DES Verfahren

Modul 5 Hybridverfahren

PGP

PGP (Pretty Good Privacy) ist ein Hybridverfahren. Es nutzt die Vorteile sowohl der symmetrischen als auch der asymmetrischen Verschlüsselung aus.
Der wesentliche Vorteil der asymmetrischen Verschlüsselung ist, dass kein Schlüssel auf geheimen Wegen überbracht werden muss. Der Vorteil der symmetrischen Verschlüsselung gegenüber der asymmetrischen Verschlüsselung ist die Geschwindigkeit, denn sie ist wesentlich schneller als die asymmetrische Verschlüsselung mit ihren extrem langen Schlüsseln.
Daher verwendet PGP zunächst ein asymmetrisches Verfahren (RSA oder neuerdings auch DH), um einen symmetrischen Schlüssel zu verschlüsseln und ihn so zum Empfänger zu befördern. Haben beide Seiten auf diesem Wege einen symmetrischen Schlüssel erhalten, so wird die darauf folgende Nachricht symmetrisch mit Hilfe des symmetrischen Schlüssels und einem passenden symmetrischen Verfahren (IDEA, DES) verschlüsselt.
Das Ganze sieht dann folgendermaßen aus:



Aufgabe 5.1

1.) Erläutere welche Vorteile PGP vereint und welche Nachteile dadurch aus dem Weg geräumt werden.

Zusatz Modul 6 Abschließende Wettbewerbsaufgabe (aus BW Inf)

Verschlüsselung

Zara Zackig muss sich leider viele geheime Sätze für telefonische Identitätsfeststellungen auf ihren Geschäftsreisen merken. Auf Grund negativer Erfahrungen in der Vergangenheit ist sie sehr vorsichtig geworden und schreibt die Sätze niemals im Klartext, sondern nur verschlüsselt auf.

Dazu verwendet sie folgendes, selbst erfundenes Verfahren: Sie möchte zum Beispiel den kurzen Satz „Ohne Liebe keine Wahrheit“ verschlüsseln. In alter kryptographischer Tradition ignoriert sie Leer- und Satzzeichen. Nun sucht sie sich eine beliebige Stelle aus ihrem Lieblingsbuch aus, das sie stets mit sich führt. Nehmen wir an, sie wählt folgendermaßen: „Ganz einfach. So geweckt und temperamentvoll und beinahe leidenschaftlich sie ist, oder vielleicht auch, weil sie es ist, sie gehört nicht zu denen, die so recht eigentlich auf Liebe gestellt sind, wenigstens nicht auf das, was den Namen ehrlich verdient. …“

Sie findet nun die Buchstaben ihres Satzes (als eine mögliche Untersequenz) im gewählten Text, markiert sie, zählt die Abstände und erhält so diese Zahlenfolge, welche sie sich notiert:

13 34 7 13 11 3 9 58 1 93 4 1 1 1 4 21 7 3 23 5 5 15

Welche Zeile im Buch als Startpunkt dient, will sie sich aber auswendig merken!

Aufgabe 6.1

Eines Tages will Zara einen ihrer Sätze entschlüsseln und erkennt mit Grauen, dass sie die richtige Zeile im Buch vergessen hat. Die notierte Zahlenfolge lautet:

13 34 7 13 11 3 9 58 1 93 4 1 1 1 4 21 7 3 23 5 5 15

Ermittle für diese und alle weiteren Zahlenfolgen, die zusammen mit dem Text von Zaras Lieblingsbuch auf www.bundeswettbewerb-informatik.de abgelegt sind, welcher Satz bzw. deutsche Klartext dahinter steckt.

Den Text findest du hierEffiBriestK

Weitere Zahlenfolgen:

1 30 21 8 5 19 46 3 22 20 74 9 1 86 1 12 12 8 1 13 295 4 25 96 2 2 327 37 1 1 9 34 11 3 3 9 1 5 2 13 20 79 1 1 1 1 4 55 1 17 1 1 1 4 2 104 12 235 37

71 2 3 15 17 1 10 7 64 1 16 1 2 13 1 27 2 346 4 4 16 89 5 4 4 35 7 2 1 12 3 17 21 5 1 10 27 23 328 11 26 7 14 5 2 26 1 12 14 4 52 48 6 106 11 9 22 1 26 1 29 11 1

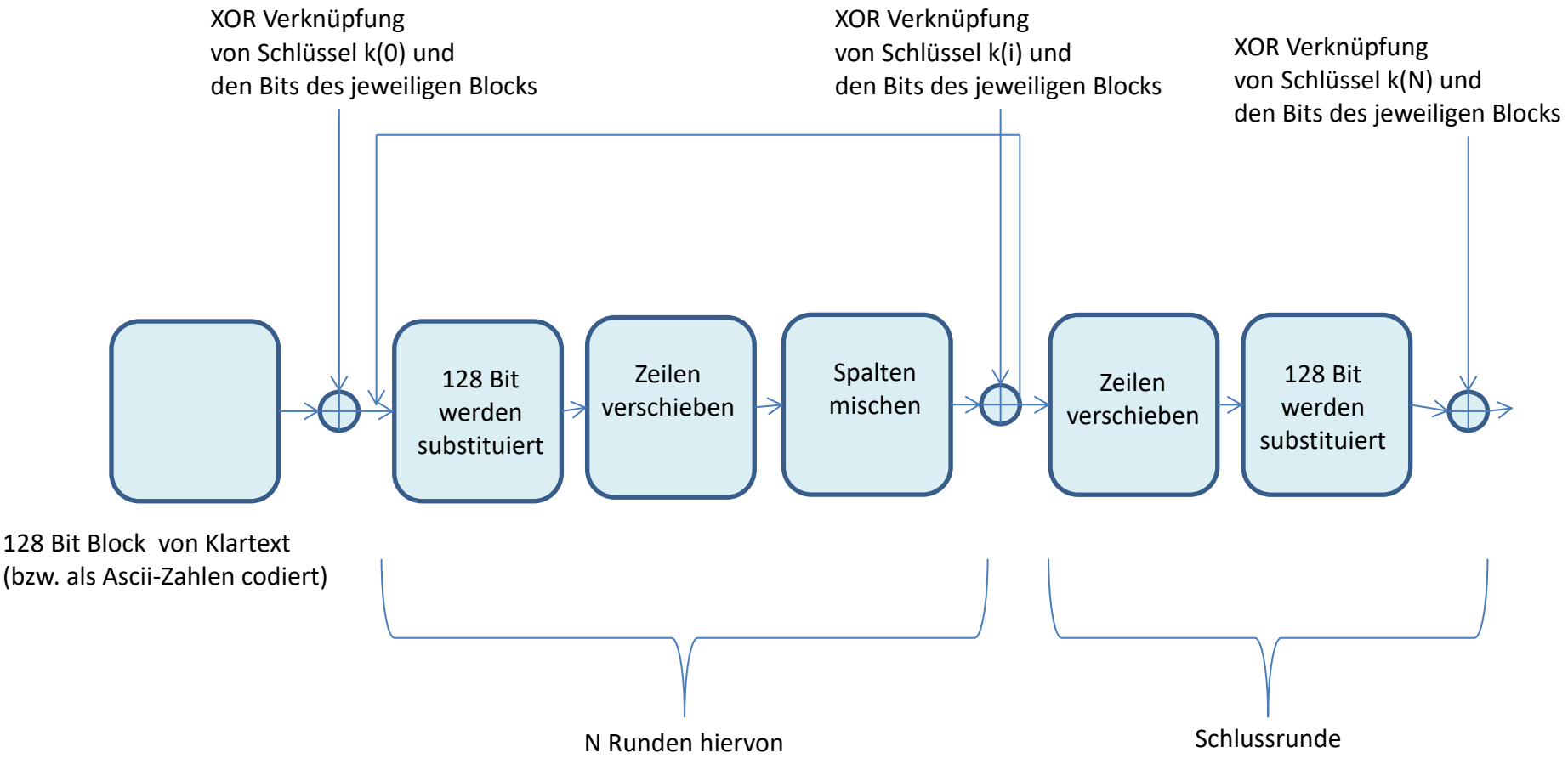
3 5 13 1 8 20 3 4 3 91 107 1 4 2 2 5 21 4 8 53 4 6 1 1 1 3 39 1 45 1 9 7 62 52 1 26 12 4 11 32 1 1 3 5 1 1 5 3 2 52 35 30 1 7 1 1 4 34 8 26 1 6 408 1 1

u.s.w. hier zahlenfolgen

Vorführung: Aufgabe BWINf

Anhang

AES Verfahren als Übersicht



Ascii Tabelle

Dezimal	Zeichen		Dezimal	Zeichen		Dezimal	Zeichen		Dezimal	Zeichen
64	@		80	P		96	`		112	p
65	A		81	Q		97	a		113	q
66	B		82	R		98	b		114	r
67	C		83	S		99	c		115	s
68	D		84	T		100	d		116	t
69	E		85	U		101	e		117	u
70	F		86	V		102	f		118	v
71	G		87	W		103	g		119	w
72	H		88	X		104	h		120	x
73	I		89	Y		105	i		121	y
74	J		90	Z		106	j		122	z
75	K		91	[		107	k		123	{
76	L		92	\		108	l		124	|
77	M		93	]		109	m		125	}
78	N		94	^		110	n		126	~
79	O		95	_		111	o		127	DEL