2. Rotationschiffre (Caesar-Verschlüsselung)
Entschlüsselter Text (Verschiebung um 3 Stellen):
Code kopieren
DER ANGRIFF ERFOLGT AUF SEECHEIT DIE WEISHEIT SIND GEFAHREN ICH
KAM SAH UND SIEGTE TEILE UND HERRSCHE
3. Vigenère-Verschlüsselung
Verschlüsseln von "BEEF" mit "AFFE":

Verschlüsselter Text: BJJJ
Entschlüsseln von "WRKXQT" mit "SECRET":

Entschlüsselter Text: ENIGMA
4. Vigenère-Codeanalyse
Die entschlüsselte Nachricht der Vigenère-Chiffre ist nicht angegeben, benötigt CrypTool1 für vollständige Analyse.
5. XOR-Stromchiffre
Verschlüsseln der Dezimalzahl 4711 (mit Schlüssel 1000'1101):

Chiffre: 1001 1111 1111 1010
Entschlüsseln:

Entschlüsselter Text: 4711 (nach Rückumwandlung)

KRYPTOGRAFIE AUFGABEN

SYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN

1. **Cryptool-Applikation installieren:** Mit CrypTool1, einem Open-Source-Projekt und somit freier Lern-Software erhalten wir ein Tool in die Hand, dass die Konzepte der Kryptographie und der Kryptoanalyse erfahrbar machen lässt. Installieren Sie nun CrypTool1 auf ihrem Notebook, bei Sicherheitsbedenken als virtuelle Applikation. CRYPTOOL1 kann man hier herunterladen: https://www.cryptool.org/de/ct1/

2. **Rotationschiffre**: Schon der römische Feldherr und spätere Kaiser Julius Cäsar kannte den folgenden Verschlüsselungstrick und nutzte ihn bei seinen geheimen Botschaften: Ersetze jeden Buchstaben durch den, der eine bestimmte Anzahl Stellen später im Alphabet folgt! Somit konnte Cäsar effektiv geheime Botschaften übermitteln, wie z.B. diese Zitate:
   GHU DQJULII HUIROJW CXU WHHCHLW GLH ZXHUIHO VLQG JHIDOOHQ LFK NDP VDK XQG VLHJWH WHLOH XQG KHUUVFKH
   Benutzen Sie nun Ihr CrypTool1 und finden Sie heraus, um welche Zitate es sich handelt! Die Rotationschiffre ist übrigens ein klassisches, symmetrisches Verfahren. Nun aber nicht einfach drauflos probieren. Machen Sie etwas Kryptoanalyse mit einem ASCII-Histogramm. (Tipp: Häufigkeitsanalyse der im Text enthaltenen Buchstaben)

3. **Vigenèreverschlüsselung**: Um etwas warm zu laufen, verschlüsseln wir, diesmal ohne Cryptool, das Wort **BEEF** mit dem Schlüsselwort **AFFE**.
   Wer will, kann sich hier noch an einer Entschlüsselung des Geheimtexts **WRKXQT** mit dem Schlüsselwort **SECRET** versuchen.

4. **Vigenèrecodeanalyse:** Nun wirds spannender: Wir versuchen den Vigenère-Code zu knacken und bedienen uns einem Analysewerkzeug im Cryptool1. Abgefangen haben wir die folgende Vigenère-Chiffre:
   USP JHYRH ZZB GTV CJ WQK OCLGQVFQK GAYKGVFGX NS ISBVB MYBC MWCC NS JOEVB GTV KRQFV AGK XCUSP VFLVBLLBE ESSEILUBCLBXZU SENSWFGVRCES SER CZBCE ILUOLBPYISL CCSZG VZJ

   Neugierig wie wir sind, möchten wir gerne wissen, welcher Text hinter dieser Chiffre steckt. Da uns aber das Schlüsselwort fehlt, müssen wir tief in unsere Trickkiste greifen. (Tipp: Im CrypTool1/Hilfe/Index/Vigenère-Verschlüsselungsverfahren findet man weitere Informationen zum Vigenère-Analyseverfahren.)

Zu guter Letzt versuchen wir, ob das Analysetool auch Resultate liefert, wenn das Passwort wesentlich länger ist. Nehmen sie den entschlüsselten Text von vorhin und verschlüsseln sie ihn erneut, diesmal aber mit diesem Schlüssel:

LoremipsumdolorsitametconsectetueradipiscingelitAeneancommodoligulaegetdolorAeneanmassaCumsociisnatoquepenatibusetmagnisdisparturientmontesnasceturridiculusmusDonecquamfelisultriciesnecpellentesqueeupretiumquissemNullaconsequatmassaquisenimDonecpedejustofringillavelaliquetnecvulputateegetarcuInenimjustorhoncusutimperdietavenenatisvitaejustoNullamdictumfeliseupedemollispretiumIntegertinciduntCrasdapibusVivamuselementumsempernisiAeneanvulputateeleifendtellusAeneanleoligulaporttitoreuconsequatvitaeeleifendacenimAliquamloremantedapibusinviverraquisfeugiatatellusPhasellusviverranullautmetusvariuslaoreetQuisquerutrumAeneanimperdietEtiamultriciesnisivelaugueCurabiturullamcorperultriciesnisiNamegetduiEtiamrhoncusMaecenastempustellusegetcondimentumrhoncussemquamsemperliberositametadipiscingsemnequesedipsumNamquamnuncblanditvelluctuspulvinarhendreritidloremMaecenasnecodioetantetincidunttempusDonecvitaesapienutliberovenenatisfaucibusNullamquisanteEtiamsitametorciegeterosfaucibustinciduntDuisleoSedfringillamaurissitametnibhDonecsodalessagittismagnaSedconsequatleoegetbibendumsodalesaugueveliturcusnunc

Funktionieren nun die Vigenère-Analysetools immer noch?

5. **XOR-Stromchiffre**: Verschlüsseln sie die Dezimalzahl **`4711`** von Hand als XOR-Stromchiffre. Der binäre Schlüssel lautet: **`1000'1101`**. Zur Kontrolle entschlüsseln sie die erhaltene Chiffre wieder.
   (Hinweis: Sie müssen die Dezimalzahl zuerst in eine 16-Bit Binärzahl umwandeln. Führende Nullen dabei nicht weglassen. Sollte der Schlüssel für die Verschlüsselung zu kurz sein, wird dieser mehrmals wiederholt. Der Datenstrom soll in dieser Aufgabe mit der Übertragung des MSB's, also von links nach rechts beginnen.)

6. **AES (Advanced Encryption Standard)**: Öffnen sie nun in der Cryptool-Onlineversion die folgende Visualisierung AES-Rijndael-Animation und studieren sie diese: https://www.cryptool.org/de/cto/aes-animation

7. **Wie sicher ist mein Passwort?** Da Cryptool ja bereits geöffnet ist, kann es auch nicht schaden, mal sein Lieblingspasswort auf seine Sicherheit zu überprüfen. Crypttol bietet dazu einen Passwort-Qualitätsmesser an: Einzelverfahren/Tools/Passwort-Qualitätsmesser

ASYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN

1. Spielen sie in Cryptool1 einen **Schlüsseltausch** gemäss **Diffie-Hellman** durch. Experimentieren sie mit verschiedenen, auch eigenen Parametern. (Sie finden das Tool unter Einzelverfahren→Protokolle→Diffie-Hellman-Demo...)

2. **RSA-Verschlüsselung**: Erzeugen sie zwei asymmetrische Schlüsselpaare: Eines für «Muster Felix» und eines für «Hasler Harry» (Sie finden das Tool unter Digitale Signaturen/PKI→PKI→Schlüssel erzeugen/importieren...)
   Verschlüsseln Sie nun eine Nachricht für Muster Felix und versuchen sie danach, den Text als Hasler Harry, danach als Muster Felix zu entschlüsseln. Was stellen sie fest? (Sie finden die Tools unter Ver-/Entschlüsseln→Asymmetrisch→RSA-Ver/Entschlüsselung...)

3. Im Gegensatz zum Diffie-Hellman-Verfahren (für Schlüsseltausch) kann **RSA** einen kompletten Text verschlüsseln. Sehen sie sich dazu die RSA-Demo an. (Sie finden das Tool unter Ver-/Entschlüsseln→Asymmetrisch→RSA-Demo...)

4. Moderne Verschlüsselungsverfahren arbeiten **hybrid**. Schauen sie sich dazu die beiden Demos zu **RSA-AES** an. (Sie finden die Tools unter Ver-/Entschlüsseln→Hybrid→RSA-AES-Ver/Entschlüsselung...)

5. **Optionale** Aufgabe für Mathe-Fans: Wir verwenden hier nochmals die RSA-Demo. Sie finden das Tool unter Ver-/Entschlüsseln→Asymmetrisch→RSA-Demo...
   Wir möchten nun der **Sicherheit** etwas auf den Zahn fühlen:
   Um den geheimen und öffentlichen Schlüssel zu erstellen, müssen zuerst zwei Primzahlen gewählt werden. Unter Primzahlen generieren kann bei Primzahl p bzw. q eine Primzahlunter- und Obergrenze bestimmt werden, in dessen Bereich Primzahlen generiert werden. Öffentlich ist dann das RSA-Modul N und der öffentliche Schlüssel e. Wir möchten nun prüfen, wie gross die beiden Primzahlen p und q gewählt werden müssen, damit die Faktorisierung des RSA-Moduls N und damit das Knacken des geheimen Schlüssels d nicht so mühelos gelingen kann. Das RSA-Modul N kann mit folgendem Tool faktorisiert werden: Analyse→Asymmetrische Verfahren→Faktorisieren einer Zahl...
   Erstellen sie nun mit RSA-Demo bei kleinen, max. 2-stelligen Primzahlen das RSA-Modul N und lassen sie danach die Zahl im anderen Tool faktorisieren. Sie werden feststellen, dass die Faktorisierung in wenigen Augenblicken erledigt ist und somit der Geheimtext entschlüsselt werden könnte. Wiederholen sie nun den Versuch mit grossen Primzahlen. Sie können dazu im Menü «Primzahlen generieren» die Primzahlobergrenze p und q auf zum Beispiel 128 Bit (2^{128}) erhöhen. Versuchen sie nun das erhaltene RSA-Modul N mit dem Analyse-Tool zu faktorisieren. Sie werden sehen, dass dies nun nicht mehr so ohne weiteres (Zeitaufwand) gelingen wird.

6. **Hashwert**: Führen Sie nun im Cryptool die Hash-Demo aus. Sie finden diese unter Einzelverfahren → Hashverfahren → Hash-Demo...

7. **Dokument signieren:** Erstellen sie ein kurzes Dokument und signieren sie dieses. Siehe Digitale Signaturen/PKI → Dokument signieren bzw. Dokument überprüfen. Nehmen sie am signierten Dokument eine kleine Änderung vor und überprüfen sie die Signatur erneut. Was stellen sie fest?

8. **Hashwert-Manipulation bei der digitalen Signatur:** Der Nachricht muss ein eindeutiger Hashwert entsprechen. Mit unsicheren oder veralteten Hashverfahren ist dies aber nicht immer der Fall. Wie Sie in der folgenden Analyse der Hashverfahren erfahren dürfen, kann je nach gewähltem Hashverfahren eine zumindest teilweise Hashwert-Übereinstimmung von verschiedenen Nachrichten erreicht werden. Probieren Sie es doch einfach einmal mit Cryptool selber aus. Siehe Analyse → Hashverfahren → Angriff auf den Hashwert der digitalen Signatur...
   Die einzelnen Schritte:

   a. Erstellen sie eine Datei original.txt mit dem Textinhalt: «Verkaufe mein Notebook zu CHF 1500.-»
   b. Erstellen sie von der soeben erstellten Datei original.txt eine Kopie mit dem Dateinamen backup.txt.
   c. Erstellen sie eine Plagiats-Datei fake.txt mit dem Textinhalt: «Verkaufe mein Notebook zu CHF 150.-» (Es fehlt absichtlich die letzte Null!)
   d. Erstellen sie zu Kontrollzwecken je einen MD2-Hashwert von allen drei Dateien.
      Einzelverfahren → Hashverfahren → MD2
      Sie stellen fest: original.txt und backup.txt haben denselben Hashwert, fake.txt einen anderen.
      backup.txt kann nun gelöscht werden. Diese Datei brauchen wir nicht mehr.
   e. Wählen sie nun Analyse → Hashverfahren → Angriff auf den Hashwert der digitalen Signatur...
   f. Als harmlose Datei wählen sie original.txt
   g. Als gefährliche Datei wählen sie fake.txt
      Wählen sie bei den Optionen den schwächsten Hashalgorithmus MD2 und eine signifikante Bitlänge von 16 (Bit).
      Nach der Ausführung erhalten sie zwei Varianten von ihren Ausgangsdateien:
      «original.txt» ergibt «Harmlose Nachricht: MD2, <92 14>»
      «fake.txt» ergibt «Gefährliche Nachricht: MD2, <92 14>»
      Das bedeutet: Cryptool hat von beiden Ausgangsdateien Varianten mit kleinen Ergänzungen/Änderungen gefunden bzw. erstellt, die sich in den ersten 16 Bit des Hashwerts nicht unterscheiden: <92 14>
   h. Sie können nun diesen Vorgang mit einer längeren signifikanten Bitlänge wie z.B. 24,32, etc. wiederholen.
      Sie werden feststellen, dass der Suchvorgang in Cryptool immer länger dauert. Bei einer signifikanten Bitlänge von 128 wäre der Hashwert bei der Textdatei original.txt und fake.txt komplett berechnet. Das heisst, es liegen nun zwei Dokumente vor, die denselben Hashwert besitzen.

   Was ist nun das Gefährliche dabei:
   Würden sie als Bösewicht nun eine Variante mit dem modifizierten aber sonst korrekten Text «Verkaufe mein Notebook zu CHF 1500.-» ihrem Opfer Felix Muster zur digitalen Signierung vorlegen und dieser auch tatsächlich unterschreiben, wäre ihre Schelmerei schon zur Hälfte gelungen: Sie besässen ein modifiziertes korrektes Dokument mit gültiger Signatur, würden dieses aber durch ihre gefährliche Datei mit dem modifizierten Fake-Text «Verkaufe mein Notebook zu CHF 150 .-» ersetzen. Der von Felix Muster signierte Hashwert gilt ja für beide modifizierten Dokumente. Würde nun Susi Sorglos das gefälschte Dokument inklusive Signatur erhalten, dessen Echtheit überprüfen und dann auch noch lesen, wäre der Schaden schon angerichtet:

Die ahnungslose Frau würde annehmen, das Dokument stammt tatsächlich und unverfälscht von Felix Muster, was ja infolge ihrer Manipulation (Modifikationen) nicht zutrifft und würde vielleicht sogar auf den Kauf des für CHF 150.- angebotenen Notebooks bestehen.
Geht es nur um belanglose Dinge, stellt das kein grosses Problem dar. Handelt es sich aber um Votings, rechtlich verbindliche Offerten oder sogar Software-Updates, droht nachhaltiger Ärger.

Schlussfolgerung:
Niemals fremde Dokumente unbekannten Inhalts signieren!
(Um jetzt aber dieser Erfahrung etwas Brisanz zu nehmen, soll gesagt sein, dass während der Berechnung aller Hash-Bits (in unserem Fall 128) doch etwas Zeit vergeht (Die ersten 64 Bit am PC zu berechnen dauert ca. 1 bis 4 Tage - HW/SW-abhängig/Stand 2020) und das der MD2 ja auch schon etwas in die Jahre gekommen und bei aktuellen Signier-Tools schon längst durch leistungsfähigere und kaum manipulierbare Algorithmen ersetzt worden ist.)

DIE SCHLÜSSELVERWALTUNG

1. Wie kann ich einen Public-Key verifizieren?

2. Was versteht man unter Public Key Infrastruktur (PKI)?

3. Was bedeutet Certification-Authority (CA) und was Trust-Center (TC)?

SICHERES INTERNET UND ZERTIFIKATE

1. Wer hat das Zertifikat für die Bankwebseite www.ubs.com ausgestellt und wie lange ist es gültig?

2. Wer hat das Zertifikat für die für die Schulwebseite www.tbz.ch ausgestellt und wie lange ist es gültig?

3. Wer hat das Zertifikat für die für die Webseite www.example.ch ausgestellt und wie lange ist es gültig?

4. Wählen sie irgendeine Applikation aus, die auf ihrem PC installiert ist. Stellen sie sich nun vor, sie müssten diese von Hand aktualisieren oder aus Kompatibilitätsgründen auf eine frühere Version zurückstufen. Wo finden sie aktuelle und frühere Versionen ihrer Software und wie wird sichergestellt, dass die dort angebotene SW-Version auch wirklich echt ist bzw. vom SW-Entwickler stammt?

5. Erstellen sie eine virtuelle Linux-Maschine mit z.B. VirtualBox und Ubuntu. Richten sie nun auf ihrem WIN-PC eine Remoteverbindung via **ssh** zu ihrem Linux-PC ein. Überprüfen sie die Verbindung. Wäre auch eine graphische Anbindung möglich?

6. In dieser Übung untersuchen wir eine **http**-Verbindung und eine **https**-Verbindung mit dem Network-Sniffer **Wireshark**:
   https://www.wireshark.org/
   http://www.example.ch
   https://www.zkb.ch
   Untersuchen sie speziell die OSI-Layer 2,3,4 und 7. Was stellen sie fest? Wo liegen die Unterschiede zwischen http und https? Zusatzfrage: Kann man mit Wireshark bei einer https-Verbindung trotzdem herausfinden, welche Webseite besucht wurde?

HTTP: Daten sind im Klartext sichtbar.
HTTPS: Daten sind verschlüsselt, nur die IP-Adresse und der Hostname sind sichtbar.

7. Öffnen sie die beiden folgenden Webseiten und achten sie auf die Unterschiede in der Webadresszeile. Was stellen sie bezüglich **Protokoll** und **Zertifikat** fest?
   https://juergarnold.ch
   https://www.zkb.ch

   Beides HTTPS seiten
   Juer arnold: Lets encrypt
   ZKB: Swiss Sign ag

8. Wenn sie sich mit Zertifikaten befassen, fallen ihnen früher oder später folgende Anbieter bzw. Webseiten auf:
   http://www.cacert.org
   https://letsencrypt.org/de
   Was genau wird hier zu welchen Konditionen angeboten?

   Gratis zertifikate aber dafuer ist es auch keine hohe zertikfikats stufe.

9. Folgende **TLS Zertifikatsarten** werden unterschieden:
   Domain Validated, Organization Validated und Extended Validation.
   Sie möchten einen Webshop betreiben, wo mit Kreditkarte bezahlt werden kann.
   Welcher Zertifikatstyp ist der richtige?

10. Studieren sie den Beitrag auf der Webseite Let's Encrypt "Wie es funktioniert"
    https://letsencrypt.org/de/how-it-works/
    Was ist der Unterschied zwischen OpenPGP und X.509?

11. Erklären sie den Aufruf einer sicheren Webseite. (**HTTPS**)
    Wie ist der Ablauf beim Protokoll TLS? Wo genau kommen die Zertifikate ins Spiel?

12. Was bedeutet S/MIME?

13. Aus gesetzlichen Gründen sind sie verpflichtet, den gesamten geschäftlichen EMail-Verkehr zu archivieren, auch den verschlüsselten. Was ist das Problem dabei und wie könnte man dies lösen?

14. Optional: Versuchen sie mit Wireshark einen Standard-**TLS-Handshake** zu dokumentieren.

Zertifikatstyp für Webshop:

Extended Validation (EV) Zertifikat: Höchstes Maß an Vertrauen und Sicherheit, zeigt Unternehmensnamen in der Adressleiste.
Unterschied OpenPGP vs. X.509:

OpenPGP: E-Mail-Verschlüsselung, Web-of-Trust, Schlüsselpaare.
X.509: SSL/TLS-Zertifikate, hierarchische PKI, Zertifikate von CAs.
Aufruf einer sicheren Webseite (HTTPS):

Client und Server tauschen Nachrichten aus (Client Hello, Server Hello).
Server sendet Zertifikat.
Client überprüft Zertifikat.
Schlüssel werden ausgetauscht und Session-Keys erstellt.
Datenübertragung erfolgt verschlüsselt.
S/MIME:

Standard für E-Mail-Verschlüsselung und Signierung, nutzt X.509-Zertifikate.
Archivierung verschlüsselter E-Mails:

Problem: Verschlüsselte E-Mails sind ohne private Schlüssel nicht lesbar.
Lösungen: Key Escrow, MTA-Archiving, Sicherung der Schlüsselpaare.
TLS-Handshake mit Wireshark (optional):

Erfassen und analysieren Sie TLS-Pakete (Client Hello, Server Hello, Certificate, Key Exchange, Finished).
Dokumentieren Sie den Ablauf des Handshakes.

PGP und OpenPGP

1. **GPG4WIN auf dem eigenen Notebook installieren**
   GPG4WIN ist eine Free-Windows-Variante von GnuPG bzw. OpenPGP. (PGP wäre übrigens die kommerzielle Variante.) GPG4WIN beinhaltet den GnuPG-Zertifikatsmanager **Kleopatra**. Mit diesem kann man neue Schlüsselpaare erstellen und bestehende importieren und verwalten. Im Weiteren ist es in Kleopatra möglich, Nachrichten zu verschlüsseln und/oder zu signieren. Bei diesem ersten Schritt muss noch nicht unbedingt ein Schlüsselpaar erzeugt werden, das geht später immer noch. Falls doch, empfiehlt es sich, einen Test-EMail-Account bereit zu halten.
   Hier kann man GPG4WIN herunterladen: https://www.gpg4win.de/

2. **Mit GPG4WIN/Kleopatra ein Schlüsselpaar erstellen**
   a) Starten des gpg4win-Zertifikatsmanagers Kleopatra.
   b) Falls das bei der Installation von gpg4win noch nicht geschehen ist, erzeugen eines persönlichen Schlüsselpaars unter Datei/Neues OpenPGP-Schlüsselpaar...
      ***Tipp**: Beim Ausprobieren wird das Benutzen einer Test-E-Mail-Adresse empfohlen.*
      ***Hinweis**: Alternativ wäre auch ein X.509-Schlüsselpaar denkbar. Dazu müsste man aber eine Beglaubigungsstelle einbeziehen, was den Rahmen dieser Übung sprengen würde.*
   c) Beim Erzeugen eines Schlüsselpaars wird eine sogenannte Passphrase verlangt. Dies ist ein Passwort, dass man später beim Erstellen und Öffnen einer verschlüsselten Nachricht eingeben muss. Diese Passphrase darf man darum keinesfalls vergessen und niemals weitergeben.
   d) Exportieren des eigenen öffentlichen Schlüssels. Achtung: Hier den PublicKey und nicht den PrivateKey exportieren! Im Zweifelsfall mit einem Texteditor der Wahl das ASC-File überprüfen! In der ersten Zeile sollte `BEGIN PGP PUBLIC KEY BLOCK` stehen.
   e) Den PublicKey wie folgt umbenennen: Vorname_Nachname_PublicKey.asc
   f) Kleopatra verwaltet die öffentlichen Schlüssel der Kommunikationspartner. Dazu muss man diese aber erst in Kleopatra einpflegen.
   g) Testen: Um PGP auszuprobieren, soll man PublicKeys gegenseitig austauschen. Dies kann z.B. über das Internet geschehen. Im Schulbetrieb kann man ausnahmsweise vertrauen, dass der Schlüssel auch von der Person stammt, auf die der Dateiname hinweist. Ausserhalb der Schule ist das selbstverständlich ein No-Go. *(Wenn sie in gpg4win/Kleopatra ihre beiden Schlüssel exportieren erhalten sie Dateien mit der Endung .asc Die Endung asc ist ein Hinweis, dass es sich um ASCII-Dateien handelt, die mit einem Texteditor wie z.B. Notepad++ geöffnet werden können. Damit lässt sich zumindest feststellen, ob die untersuchte Datei ein PrivateKey oder PublicKey ist. Welcher Person diese zuzuordnen ist, bleibt hier allerdings verborgen. Darum empfiehlt es sich, dem Dateinamen Sorge zu tragen, weil er der einzige Hinweis auf den Besitzer enthält.)*

20. **Fremden Public-Key verifizieren**: Wie können sie die Authentizität des Ausstellerschlüssels überprüfen? Stammt dieser Public-Key auch wirklich von der Person, von der ich dies annehme?

21. **Frage zum OpenPGP-Schlüssel**: Woraus besteht bzw. woran erkennt man diesen?

22. **X.509-Schlüsselpaar**: Nochmals zur Schlüsselerzeugung in Kleopatra (Datei/Neues Schlüsselpaar...). Ein persönliches OpenPGP Schlüsselpaar haben wir ja bereits erstellt. Da gibt es aber auch noch das persönliche X.509-Schlüsselpaar. Probieren

sie das auch mal aus! Was sind die Unterschiede zwischen den beiden Schlüsselvarianten und was hat das mit S/MIME zu tun?

23. **Mit Gpg4win/Kleopatra eine Nachricht verschlüsseln**: Nun soll eine beliebige Datei (Nachricht als Text, Bild etc.) für ihren Kommunikationspartner verschlüsselt werden. Dies kann direkt in Kleopatra erfolgen. Stellen sie das verschlüsselte File ihrem Kommunikationspartner zur Verfügung. (Per E-Mail, USB-Stick etc.) Wenn dieser es entschlüsseln kann, wurde die Aufgabe erfolgreich erledigt.

24. **Mit Gpg4win/Kleopatra eine Nachricht signieren**: Nun soll eine beliebige Datei (Text, Bild etc.) für ihren Kommunikationspartner signiert werden. Dies kann ebenfalls wieder direkt in Kleopatra erfolgen. Stellen sie das File inklusive Signatur ihrem Kommunikationspartner zur Verfügung. (Per E-Mail, USB-Stick etc.) Wenn dieser mit der Signatur die Echtheit ihres Files verifizieren kann, wurde die Aufgabe erfolgreich erledigt.

25. **Mit Gpg4win/Kleopatra eine Nachricht verschlüsseln und signieren**: In dieser Aufgabe soll eine beliebige Datei (Text, Bild etc.) für ihren Kommunikationspartner verschlüsselt und signiert werden. Wiederum in Kleopatra. Stellen sie das File inklusive Signatur ihrem Kommunikationspartner zur Verfügung. (Per E-Mail, USB-Stick etc.) Wenn dieser das File entschlüsseln und dank der Signatur den Absender verifizieren kann, wurde die Aufgabe erfolgreich erledigt.

26. **Vorarbeiten zu E-Mails im Mailclient Thunderbird verschlüsseln**
Mozilla's **Thunderbird** ist OpenSource und neben Microsofts **Outlook** ein sehr häufig eingesetzter Mail-Client zum Lesen und Schreiben von News und E-Mails.
Um bei den folgenden Aufgaben nicht sein eigenes, produktives Email-Postfach zu schädigen wird das **Anlegen eines Test E-Mail-Accounts** bei einem Provider ihrer Wahl empfohlen. Beim Austesten der E-Mail-Verschlüsselung in Thunderbird besteht nämlich die Gefahr, aus Unachtsamkeit sein Postfach zu löschen und damit wichtige Emails zu verlieren. Einige Provider verlangen beim Eröffnen eines neuen E-Mail-Accounts die Überprüfung ihrer Identität über eine Mobilenummer, Festnetznummer oder auf dem Postweg. Bei Swisscom zum Beispiel können sie zurzeit - Stand Feb. 2023 - unter Bluewin E-Mail light ohne Swisscom Internet-Abo mit einem zuvor eingerichteten Swisscom-Login kostenlos einen EMail-Account wie folgt einrichten:
Swisscom-Zugangsdaten
Name: Ihr Vorname und Nachname
E-Mail-Adresse: ihrName@bluewin.ch ***(Was halt noch so frei ist)***
Passwort: ***
(Achtung: Nicht das Swisscom-Portal-Passwort, sondern das Swisscom-Mail-Passwort verwenden!)
SSL/TLS: Jeweils aktiviert.
Posteingangsserver:
IMAP4: imaps.bluewin.ch (Port 993)
POP3: pop3s.bluewin.ch (Port 995)
Postausgangsserver:
SMTP: smtpauths.bluewin.ch (Port 465)
Überprüfen Sie Ihren neuen E-Mail-Account, indem Sie Sich gegenseitig noch unverschlüsselte E-Mails zuschicken. Sie können dazu z.B. Swisscom-Webmail benutzen. Swisscom bietet auf ihrer Webseite übrigens entsprechende Hilfestellung. Z.B. auch beim Einrichten Ihres Kontos in Outlook, Thunderbird, auf Tablets, Smartphones etc.

27. **Thunderbird auf ihrem PC/Notebook installieren**:
    Installieren Sie auf Ihrem Notebook den E-Mail-Client Mozilla Thunderbird und richten sie ihr E-Mail-Konto darin ein.
    Thunderbird können sie hier herunterladen: https://www.thunderbird.net/de/
    Bei der Verschlüsselung fokussieren wir uns auf OpenPGP-Schlüssel.
    (Die Alternative wäre S/MIME-Zertifikate)

28. **Den Mailclient Thunderbird einrichten**
    Die Zugangsdaten zu dem persönlichen E-Mail-Account wie E-Mail-Adresse, Login-Name, Passwort, Mail-Ein-/Ausgangserver liegen bereit? Dann kann es losgehen:
    a. Thunderbird herunterladen. Hier findet man Thunderbird: www.thunderbird.net
    b. Thunderbird-Einrichtung starten und eigenen EMail-Account einrichten.
    c. Nachdem man Name und EMail-Adresse eingegeben hat, kann man mit «Manuell einrichten» die Mailserver-Werte direkt eingeben.
       Dazu wählt man: IMAP (Nachrichten auf dem Server speichern)
    d. Nun die Kontoerfassung abschliessen. Wenn Thunderbird den EMail-Account nicht erfolgreich prüfen kann, wurden falsche Angaben gemacht. (Stimmt der Username, Passwort, Eingangs-/Ausgangsserver, Port-Nr. etc.?)

29. **Schlüssel in Thunderbird einrichten**
    Bevor Thunderbird für die EMail-Verschlüsselung bzw. Signierung eingesetzt werden kann, müssen noch ein paar Konfigurationen erledigt werden. Wie bei PGP4WIN/Kleopatra auch, stehen hier beide Schlüsselvarianten OpenPGP und S/MIME-X.509 zur Verfügung. Wir beschränken uns wiederum auf OpenPGP-Schlüssel.
    e. In der oberen Menüzeile rechts aussen (Drei waagrechte Striche übereinander) → Anwendungsmenü von Thunderbird anzeigen
    f. Extras → OpenPGP Schlüssel verwalten: Hier können sie ihr eigens Schlüsselpaar oder PublicKey ihrer Kommunikationspartner importieren.
       Datei → Öffentliche(n) Schlüssel aus Datei importieren.
       Datei → Geheime(n) Schlüssel aus Datei importieren
       Die Schlüssel können z.B. vorher aus Kleopatra exportiert werden.
       Sie können unter «Erzeugen» aber auch ein neues Schlüsselpaar erstellen.
    g. Nun müssen sie überprüfen, ob ihrem EMail-Account bereits ein Schlüssel zugewiesen wurde: Anwendungsmenü von Thunderbird → Konten-Einstellungen → Ende-zu-Ende-Verschlüsselung: Hier sollte unter OpenPGP angezeigt werden: Thunderbird verfügt über 1 persönlichen OpenPGP-Schlüssel für ...
       Dies funktioniert aber nur, wenn sich ihr persönlicher, in Thunderbird importierter Schlüssel auch auf ihre EMail-Adresse bezieht. Im Zweifelsfall generieren sie ein neues, persönliches Schlüsselpaar in Thunderbird, dass sie nun ihrem EMail-Account zuweisen können.
    h. Achten sie darauf, dass der Schlüssel auch tatsächlich verwendet wird. Es darf nicht die Option «Keiner - OpenPGP für diese Identität nicht verwenden» selektiert sein, sondern der Schlüssel darunter!
    i. In diesem Menü lässt sich auch einstellen, ob standardmässig EMails verschlüsselt und/oder signiert werden sollen. Darauf verzichten wir vorerst einmal.

30. Suchen sie sich in ihrer Klasse eine **EMail-Zielperson** aus und importieren sie den **Public-Key** dieser Person.

31. **EMails in Thunderbird verschlüsseln und/oder Signieren**
    Falls man bereits PublicKeys von Lernenden importiert hat, kann man nun mit dem Verschlüsseln und Signieren beginnen:
    j. Unter Verfassen die EMail-Adresse des Empfängers eingeben.
    k. Prüfen sie unter Sicherheit/Verschlüsselungstechnologie ob auch OpenPGP aktiv ist.
    l. Da sie EMails nicht automatisch verschlüsseln, aktivieren sie nun dies für die aktuelle EMail. Zur Auswahl stehen:
        - Sicherheit/Nur mit Verschlüsselung senden
        - Sicherheit/Nachricht unterschreiben
        - Meinen öffentlichen Schlüssel anhängen
        - Zur Kontrolle: Linksunten erscheint OpenPGP inkl. Icon.
    m. Erstellen und verschlüsseln sie nun eine EMail für ihre Zielperson.
    n. Erstellen und signieren sie eine EMail für ihre Zielperson.
    o. Erstellen, verschlüsseln und signieren sie eine EMail für ihre Zielperson.
    p. Prüfen sie die verschlüsselten und/oder signierten EMails die sie selber erhalten haben.