D_KRYPTOGRAFIE_PGP_ANNEX

Aufgaben

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)?

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

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

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

7. 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?

   ---

8. 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?

9. 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?

10. 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

11. 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?

12. 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?

13. 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?

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

15. Was bedeutet S/MIME?

16. 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?

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

---

18. **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/

19. **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.)*

26. **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?

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

28. **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?

29. **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.

30. **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.

20. **Mit Gpg4win/Kleopatra eine Nachricht verschlüsseln <u>und</u> 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.

---

34. **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.

35. **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)

36. **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.?)

37. **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.
    a. In der oberen Menüzeile rechts aussen (Drei waagrechte Striche übereinander) → Anwendungsmenü von Thunderbird anzeigen
    b. 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.
    c. 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.
    d. 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!
    e. In diesem Menü lässt sich auch einstellen, ob standardmässig EMails verschlüsselt und/oder signiert werden sollen. Darauf verzichten wir vorerst einmal.

38. PublicKeys von Klassenkameraden importieren
Suchen sie sich in ihrer Klasse eine EMail-Zielperson aus und importieren sie den Public-Key dieser Person.

39. **EMails in Thunderbird verschlüsseln und/oder Signieren**
Falls man bereits PublicKeys von Lernenden importiert hat, kann man nun mit dem Verschlüsseln und Signieren beginnen:
    a. Unter Verfassen die EMail-Adresse des Empfängers eingeben.
    b. Prüfen sie unter Sicherheit/Verschlüsselungstechnologie ob auch OpenPGP aktiv ist.
    c. 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.
    d. Erstellen und verschlüsseln sie nun eine EMail für ihre Zielperson.
    e. Erstellen und signieren sie eine EMail für ihre Zielperson.
    f. Erstellen, verschlüsseln und signieren sie eine EMail für ihre Zielperson.
    g. Prüfen sie die verschlüsselten und/oder signierten EMails die sie selber erhalten haben.