Walther-Rathenau-Gewerbeschule Freiburg	**Public Key Verschlüsselung** RSA digitale Signatur Zertifikate	Fach: ITS	Gruppe:
		2022-02-03	Seite **1**
		Name:	
		Klasse: E2FI1T	
		Punkte: /20	Note:

1 E-Portfolio

Unter `https://mahara.wara.de` läuft ein sog. *E-Portfolio-Server*. Er holt sich Benutzer-Anmeldeinformationen aus dem Samba/LDAP-Verzeichnis der Schule, d.h. man kann sich dort einfach mit seinem Schulbenutzernamen und -Passwort anmelden.
Nachfolgende Aufgaben und Fragen sollen bearbeitet und die Ergebnisse in einem Portfolio auf `mahara.wara.de` abgelegt werden. Für erste Schritte mit mahara gibt es eine Menge Infos/Lehrvideos im Netz.
Falls irgend ein Satz einer Antwort mit irgendeinem Inhalt aus dem Netz übereinstimmt, gibt es 0 Punkte für die Aufgabe. D.h. es muss alles selbst formuliert werden.
Bitte alle Seiten für die Mitglieder der Gruppe *e2fi1t* und den Benutzer *dt* sichtbar machen.

2 Public Key Infrastruktur

1. Bei Verschlüsselung hat man immer das Problem des geheimen Schlüsseltauschs. Wie löst ein *Public Key Verfahren* dieses Problem?

2. Public-Key-Verschlüsselung wird auch *Asymmetrische Verschlüsselung* genannt. Demgegenüber stehen die *Symmetrischen Verschlüsselungsverfahren*. In der Praxis werden beide Verfahren nebeneinander verwendet. Stelle Vor- und Nachteile von symmetrischer und asymmetrischer Verschlüsselung gegenüber.

3. zu welchen Verfahren gehört SSL/TLS ? Beschreibe den Ablauf einer SSL-Sitzung.

3 Asymmetrische Verschlüsselung

1. Stelle einen Merksatz zur Ver- und Entschlüsselung bei asymmetrischen Verfahren auf. Verwende dabei die Begriffe "*öffentlicher Schlüssel*" und "*privater Schlüssel*"

4 RSA

Das bekannteste asymmetrische Verfahren ist der RSA-Algorithmus.
Er arbeitet mit 3 Zahlen:

Hauptmodul N

Verschlüsselungsexponent e

Entschlüsselungsexponent d

In den folgenden Beispielen sollen N, d und e folgende Werte haben:

$$\begin{aligned} N &= 681 \\ e &= 3 \\ d &= 151 \end{aligned}$$

Verschlüsselt werden können nur Zahlen. D.h. soll ein Text verschlüsselt werden, muss man den Zeichen Zahlen zuweisen. Damit alles möglichst einfach bleibt, verwenden wir hier im Beispiel ASCII-Codes:

```
'0'=48, '1'=49, '2'=50, ...
'A'=65, 'B'=66, 'C'=67, ...
'a'=97, 'b'=98, 'c'=99, ...
```

Der RSA-Algorithmus verschlüsselt dann nach folgender Formel:

$$chiffre = (code^e) \bmod N$$

Beispiel:

$$65^3 \bmod 681 = 182$$

Entschlüsselt wird mit der gleichen Formel, aber dem Entschlüsselungsexponenten d und N:

$$182^{151} \bmod 681 = 65$$

1. Welche Bedeutung hat das Wörtchen **mod** in den Formeln? Gib ein Beispiel.
2. Was ist der Modulooperator in C und in Java?
3. Beschreibe die Funktion des Modulooperators in Worten
4. Wie wird entschlüsselt?
5. Verschlüssle Deinen wara-Usernamen mit N=681, e=3. Dokumentiere jeden Einzelschritt.
6. Entschlüssle die Chiffre-Zahlen wieder mit N=681, d=151. Dokumentiere jeden Einzelschritt
7. Aus welchen Zahlen bestehen hier im Beispiel jeweils der öffentliche und der private Schlüssel?

Hinweis: durch die Potenzen ergeben sich riesige Zwischenwerte, die ein gewöhlicher Taschenrechner nicht darstellen kann. Lösen kann man die Berechnung mit dem shell-kommando **bc** (das verwendet beliebig viele Stellen) oder auf `https://www.wolframalpha.com` (Achtung, andere Syntax wie bc).

4.1 Programmieraufgabe

1. Potenzieren ist mehrfaches Multiplizieren. Das kann man einfach in einer Schleife programmieren. Beim RSA-Algorithmus wird erst potenziert und dann wird das Ergebnis mod N gerechnet. Dabei stört das riesige Zwischenergebnis der Potenz. Schreibe eine Funktion `potMod(int code, int N, int e)`, die ohne grosses Zwischenergebnis auskommt.

5 Hash-Algorithmen

1. Beschreibe in eigenen Worten, was ein Hash-Algorithmus macht.
2. Welches sind die wichtigsten Hash-Algorithmen?
3. welchen SHA256-Wert hat folgende Zeichenkette:

   ```
   netzwerkTechnikMachtSpass
   ```

   Achte darauf, dass nur die Zeichenkette in einen Hash-Wert umgerechnet wird und keine Newline-Zeichen ungewollt hinzugefügt werden.
4. Beschreibe die Begriffe *Diffusion, Konfusion und Unumkehrbakeit* von Hash-Algorithmen.
5. Demonstriere die Diffusion von SHA256 an einem Beispiel

6 Digitale Signatur

Man kann eine Zeichenkette auch mit seinem eigenen, privaten Schlüssel verschlüsseln.

1. Wer kann diese Chiffre entschlüsseln?
2. Beschreibe an einem Beispiel den genauen Ablauf der Erstellung einer digitalen Signatur. Welche Rolle spielt dabei der Hashwert der unverschlüsselten Zeichenkette?
3. Beschreibe, wie die digitale Signatur geprüft wird.

7 Zertifikate

Wenn man einen öffentlichen Schlüssel aus dem Netz anfordert, kann man sich nicht sicher sein, dass man nicht von einem Angreifer einen falschen, öffentlichen Schlüssel untergeschoben bekommt. Aus diesem Grund werden öffentliche Schlüssel signiert.

1. Welche Daten enthält ein Certificate Signing Request (CSR)
2. An wen wird ein CSR geschickt, wie nennt man diese Institutionen allgemein?
3. Beschreibe im Detail, wie diese Institution aus dem CSR ein sog. Zertifikat erstellen.
4. Welche Bestandteile enthält ein Zertifikat? Bitte so detailliert beschreiben wie möglich. Warum ist der Name Zertifikat nicht ganz exakt?