Aufgabe 3.8

Beschreibung

Alice und Bob sind Brieffreunde und wollen neuerdings Porto sparen und sich deshalb nun Emails schicken. Da Bob und Alice aber ihrem Emailprovider nicht trauen, da er die Texte verändern könnte, haben sie sich überlegt, dass sie ihre Texte kryptografisch signieren wollen. Zum Signieren möchten sie das RSA Verfahren nutzen, um die Texte mittels Schlüsselpaaren aus öffentlichen und geheimen Schlüsseln zu signieren. Dazu müssen sie als erstes Schlüsselpaare generieren und die öffentlichen Schlüssel in einem letzten Briefwechsel austauschen. Danach wollen sie ihre Emails mit den generierten Schlüsseln signieren und die Signatur an den Text anhängen.

Aufgabenstellung

Schreiben Sie für Alice und Bob ein Programm zum Generieren der Schlüssel und zum Signieren/ Überprüfen ihrer Korrespondenz. Der Schlüsselgenerator soll aus zwei unterschiedlichen Primzahlen p und q ein Schlüsselpaar generieren und ausgeben. Das Signier- / Prüfmodul soll auf Basis eines eingelesenen Textes und dem eingegebenen Schlüssel die Signatur des Schlüssels berechnen und ausgeben. Bei der Signatur soll der private Schlüssel des Senders verwendet werden und bei der Überprüfung der Signatur der öffentliche Schlüssel des Absenders.

Testprogramm

Eingabe Schlüsselgenerator
Zwei unterschiedliche Primzahlen p und q (1 ist keine Primzahl!)

Ausgabe Schlüsselgenerator
Ein Schlüsselpaar besteht aus:

- Öffentlicher Schlüssel bestehend aus der Zahl e und der Generatorzahl g
- Privater Schlüssel bestehend aus der Zahl d und der Generatorzahl g

Eingabe Signatur-/Prüfmodul
Dateipfad zum Text, welcher signiert werden soll und abhängig, ob die Signatur generiert oder überprüft werden soll der jeweilige Schlüssel.

Ausgabe Signatur-/Prüfmodul
Text mit Signatur oder Text mit Prüfergebnis.

Hinweise zum Programm

Überlegen Sie zuerst, wie man für Texte eindeutig eine Prüfsumme berechnen kann. Transformieren Sie dann diese Prüfsumme mit dem RSA Verfahren und fügen Sie diese dem Text hinzu. Implementieren Sie das RSA Verfahren wie folgt:

Schlüsselgenerierung:

$p, q \in prim$	$11, 17 \in prim$
$g = p \cdot q$	$187 = 11 \cdot 17$
$\varphi(g) = (p-1) \cdot (q-1)$	$160 = (11-1) \cdot (17-1)$
Finde Zahl e, wobei gilt $ggt(e, \varphi(g)) = 1$	$ggt(7, 160) = 1$
Finde Zahl d, wobei gilt $(d \cdot e)\ mod(\varphi(g)) = 1$	$(23 \cdot 7)\ mod(160) = 1$
$\{e, g\}$ = Öffentlicher Schlüssel	$\{7, 187\}$ = Öffentlicher Schlüssel
$\{d, g\}$ = Privater Schlüssel	$\{23, 187\}$ = Privater Schlüssel

Signieren/Prüfen der Signatur

Signieren der Nachricht:	Prüfen der Signatur s:
Bilde Prüfsumme k für den Text 'Hallo Alice'	Bilde Prüfsumme k für den Text 'Hallo Alice'
'Hallo Alice' $\rightarrow 123$	'Hallo Alice' $\rightarrow 123$
Signiere die Prüfsumme	Überprüfe die Signatur
$k^d \ mod(g) = s$	$s^e \ mod(g) = k$
$123^{23} mod(187) = 30$	$30^7 mod(187) = 123$

Wie groß muss muss die Zahl g ìm Hinblick auf die Prüfsummen mindestens sein, damit die Signatur eindeutig ist?