Betriebssysteme und Sicherheit, WS 2019/20

7. Aufgabenblatt – Kryptographie

Geplante Bearbeitungszeit: eine Woche

Aufgabe 7.1

(a) Welches sind die drei Haupt-Schutzziele in der Datensicherheit?

(b) Welche Aufgaben haben kryptographische Systeme?

(c) Nach welchem Grundprinzip arbeiten solche Systeme? Was versteht man unter symmetrischen, asymmetrischen und hybriden kryptographischen Systemen?

Aufgabe 7.2 Der RSA-Algorithmus (Algorithmus von Rivest/Shamir/Adleman, 1977) hat folgende Struktur:

(I) Wähle zufällig zwei Primzahlen $p \neq q$ mit annähernd gleicher Stellenzahl.

(II) Bilde $n = p \cdot q$. In diesem Fall gilt für die Eulersche Funktion φ: $\varphi(n) = (p-1) \cdot (q-1)$.

(III) Wähle c mit $2 < c < \varphi(n)$, so dass $\mathrm{ggT}\,(c,\varphi(n)) = 1$.

(IV) Berechne d mit $c \cdot d \equiv 1 \bmod \varphi(n)$ und $1 < d < \varphi(n)$.

(V) Verteile (n,c) als öffentlichen Schlüssel und nutze (n,d) als privaten Schlüssel.

Eine Nachricht x wird durch $x^c \equiv y \bmod n$ verschlüsselt und entschlüsselt durch $y^d \equiv x \bmod n$, wobei $0 \leq x,y < n$.

(a) Auf welcher Annahme basiert die Sicherheit dieses Algorithmus?

(b) Begründen Sie die einzelnen Restriktionen in (I) und (III). Welche Aussage trifft die Eulersche Funktion? Welche Bedeutung hat Schritt (IV) für das Vorgehen?

(c) Demonstrieren Sie den RSA-Algorithmus an folgendem Beispiel:

Der Modul sei $n = 55$, der öffentliche Schlüssel sei $c = 7$. Verschlüsseln Sie damit die Nachricht $x = 2$. Berechnen Sie den privaten Schlüssel d, entschlüsseln Sie die verschlüsselte Nachricht und zeigen Sie deren Übereinstimmung mit x.

Hinweise:

- Benutzen Sie zur Berechnung des ggT zweier Zahlen a und b mit (o.B.d.A.) $a > b$ sowie der Summendarstellung nach dem Erweiterten Euklidischen Algorithmus eine Tabelle folgender Form:

	a	b	
a	1	0	
b	0	1	
x_i	s_i	t_i	y_i

mit

$$y_i = -\left(x_{i-1} \operatorname{div} x_i\right)$$
$$x_{i+1} = x_{i-1} \bmod x_i$$
$$s_{i+1} = s_i \cdot y_i + s_{i-1}$$
$$t_{i+1} = t_i \cdot y_i + t_{i-1}$$

div bezeichnet die ganzzahlige Division, mod den dabei auftretenden Rest.

In obiger Tabelle beginnt i mit 0, die Formeln gelten ab $i = 1$ (zuerst ist also y_1 in der „b-Zeile“ zu berechnen). Der Algorithmus bricht ab bei $x_i = 0$, und dann gilt: $x_{i-1} = \mathrm{ggT}(a,b) = s_{i-1} \cdot a + t_{i-1} \cdot b$.

Die letzte Gleichung gilt auch in jeder Zeile, was zur Rechenkontrolle genutzt werden sollte.

- Benutzen Sie zur Entschlüsselung der Nachricht binäre Exponentiation, auch bekannt als „Square and Multiply“. Zur einfachen Notation bietet sich dabei das folgende Schema für die Berechnung von a^b an:

b	a
x_i	y_i

mit

$$x_{i+1} = \lfloor x_i \div 2 \rfloor \quad x_0 = b$$
$$y_{i+1} = y_i^2 \quad y_0 = a$$

Der Algorithmus bricht ab bei $x_i = 1$. Abschließend werden alle diejenigen y_i zum Endergebnis multipliziert, deren zugehöriges x_i ungerade ist.

Aufgabe 7.3 Um die Faktoren p,q eines RSA-Schlüsselpaars zu generieren werden in der Praxis Zufallszahlen benutzt.

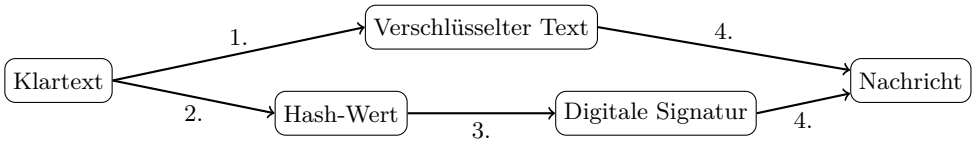
(a) Wie kann man auf einem Computer Zufall (Entropie) erzeugen?

(b) Einige Endgeräte verwenden schlechte Entropiequellen. Was kann passieren, wenn eine große Anzahl solcher Systeme RSA-Schlüssel generiert?

(c) Die öffentlichen Schlüssel von Alice und Bob haben folgende Moduln: $n_a = 73.684.837$ und $n_b = 63.546.229$. Überprüfen Sie, ob beide Moduln sich einen Faktor teilen! Faktorisieren Sie n_a und n_b!

Klausuraufgabe I

Ein Chat-System zum Austausch von kurzen Nachrichten soll die Vertraulichkeit und Integrität der übertragenen Daten sicherstellen. Jeder Teilnehmer besitzt ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel. Für jede Kommunikationsbeziehung wird außerdem ein sicher ausgehandelter symmetrischer Schlüssel vorausgesetzt.
Das Chat-System verwendet das folgende Design:



1. Der Klartext der Nachricht wird mit dem symmetrischen Kommunikationsschlüssel verschlüsselt.
2. Parallel dazu wird die Nachricht von einer kryptografischen Hash-Funktion zusammengefasst.
3. Dieser Hash-Wert wird mit dem privaten Schlüssel des Senders in eine digitale Signatur umgewandelt.
4. Beide Nachrichtenteile werden zusammengefügt und über ein unsicheres Netz zum Empfänger gesendet.

a) Nennen Sie konkrete kryptografische Algorithmen, mit denen die Schritte 1, 2 und 3 jeweils umgesetzt werden können.

b) Diskutieren Sie die Sicherheit des gegebenen Verfahrens unter den genannten Schutzzielen. Wie ließe sich die Sicherheit des Verfahrens verbessern?

c) Wir nehmen an, dass durch Fortschritte bei Quantencomputern alle kryptografischen Algorithmen unsicher werden, die auf Faktorisierung oder diskreten Logarithmen beruhen. Nennen Sie einen kryptografische Algorithmus, der von dieser Entwicklung betroffen wäre und einen, der nicht betroffen wäre.

Klausuraufgabe II

Alice und Bob kommunizieren über ein verschlüsselndes Chatsystem. Dafür haben beide vor Beginn der Kommunikation asymmetrische Schlüsselpaare erstellt und die geeigneten Teilschlüssel sicher miteinander ausgetauscht. Im laufenden Chat wird jede Nachricht sowohl verschlüsselt als auch signiert.

a) Sind die folgenden Aussagen korrekt? *Falls ja, genügt eine einfache Angabe ohne Begründung.* Falsche Aussagen sind zu inhaltlich entsprechenden, sinnvollen Aussagen zu berichtigen.
HINWEIS: Bei Korrekturen von falschen Aussagen genügt es Teile der vorgegebenen Sätze zu streichen bzw. zu ergänzen. Eine einfache Negation der Aussage ist jedoch nicht zulässig.

1. Alice und Bob verwenden jeweils das Verfahren AES für die Erstellung der Schlüsselpaare.
2. Alice hat vor Beginn der Kommunikation Bob ihren privaten Schlüssel zur Verfügung gestellt.
3. Beim Schlüsselaustausch musste auf mögliche Man-in-the-Middle-Angriffe geachtet werden.
4. Ein passiver Angreifer kann den Klartext-Inhalt der verschlüsselten Chat-Nachrichten nicht lesen.
5. Ein passiver Angreifer erhält keinerlei Informationen über den Chatverlauf.
6. Durch Prüfen der Signatur kann Alice sicher erkennen, dass eine Chatnachricht von Bob stammt.
7. Gelangt ein Angreifer an den geheimen Schlüssel von Alice, so kann er damit alle zukünftigen und vergangenen Nachrichten entschlüsseln, die an Alice gerichtet sind.
8. Besitzt ein Angreifer lediglich die öffentlichen Schlüssel, so kann er unter keinen Umständen die Vertraulichkeit des Chatsystems brechen.

b) Alice und Bob möchten über das Chatsystem auch Dateien austauschen, die potenziell mehrere Gigabyte groß sind. Schlagen Sie eine geeignete Erweiterung des Chatsystems vor, die dies effizient ermöglicht und begründen Sie ihren Vorschlag!