TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Betriebssysteme

Betriebssysteme und Sicherheit, WS 2021/22

13. Aufgabenblatt – Sicherheit II

Geplante Bearbeitungszeit: 24.01.2022 – 28.01.2022

Kryptographische Systeme: Grundsätzlich unterscheidet man in zwei Arten von Kryptographischen Systemen: *Konzelationssysteme* und *Authentikationssysteme*. Ersteres wird verwendet um Vertraulichkeit zu erreichen, während Zweiteres verwendet wird um Integrität zu gewährleisten.

Grundprinzip kryptographischer Systeme: Kryptographische Systeme basieren immer darauf, dass es einen Schlüssel gibt, mit Hilfe dessen Vertraulichkeit oder Integrität erreicht werden kann. Dabei unterscheidet man drei unterschiedliche Arten:

Symmetrische Systeme: Beide Partner verwenden den selben Schlüssel. Dieser muss geheim ausgetauscht werden. Die Verfahren sind in der Regel aber sehr schnell (z.B. AES).

Asymmetrische Systeme: Die Systeme benutzen zwei Schlüssel. Eine öffentlicher und ein geheimer Schlüssel. Dadurch, dass einer der Schlüssel öffentlich ist, ist der Schlüsselaustausch einfacher und muss nicht im Geheimen statt finden. Die Verfahren sind in der Regel jedoch langsam (z.B. RSA).

Hybride Systeme: Das sind Verfahren, die versuchen die Vorteile von symmetrischen und asymmetrischen Systemen zu verbinden. Typischerweise nutzen solche Verfahren asymmetrische Systeme zum Austausch eines geheimen Schlüssels (*Sessionkey*), der dann für die effiziente symmetrische Verschlüsselung der eigentlichen Daten verwendet wird. So kombiniert man den Vorteil des einfachen Schlüsselaustauschs von asymmetrischen Verfahren mit dem hohen Geschwindigkeit von symmetrischen Verfahren.

Aufgabe 13.1 Erklären Sie die Bedeutung der Schlüssel in kryptographischen Systemen.

Aufgabe 13.2 RSA wird in der einfachen, unsicheren Variante als Konzelationssystem mit dem Modul $n = 69$ verwendet.

(a) Welche(r) der Werte 7, 8, 11, 13 könnte(n) als öffentlicher Schlüssel k_e verwendet werden?

(b) Als öffentlicher Schlüssel wurde $k_e = 5$ festgelegt. Der Angreifer beobachtet den Schlüsseltext $c = 20$ und hat bereits in Erfahrung gebracht, dass für den Klartext $m < 10$ gilt. Wie kann der Angreifer vorgehen, um den Klartext zu bestimmen, und wie lautet der Klartext? (Auch wenn es bei diesen einfachen Zahlen leicht möglich wäre – ohne den privaten Schlüssel zu ermitteln!)

Aufgabe 13.3 RSA wird in der einfachen, unsicheren Variante als Signatursystem mit dem Modul $n = 51$ und dem Testschlüssel $k_t = 3$ verwendet. Sie erhalten zwei Nachrichten mit zugehöriger Signatur $(m_1,s_1) = (15,9)$ und $(m_2,s_2) = (3,12)$. Überprüfen Sie die Signaturen und interpretieren Sie das Ergebnis!

Aufgabe 13.4 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?

Aufgabe 13.5 Das folgende Coverbild sei gegeben (Grauwerte, 8 Bit/Pixel):

0	3	2	3	8
1	1	7	6	8
5	2	4	5	5
3	4	6	6	7
1	3	5	5	6

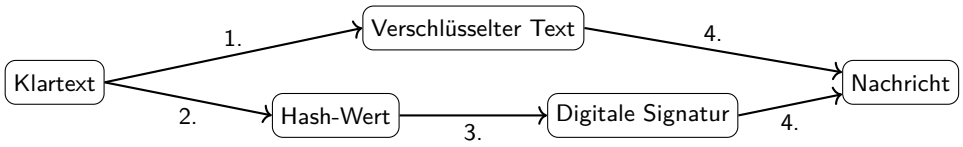
Die folgende Nachricht ist sequentiell (zeilenweise von links nach rechts, von oben nach unten, keine Abstände) einzubetten: emb = 11001001010. Geben Sie das resultierende Stegobild an bei Verwendung von

(a) LSB-Ersetzung, (b) Inkrementieren, (c) Dekrementieren.

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!