Übungsaufgaben Kryptographie und Kryptoanalyse

25. April 2024

1 Grundlagen kryptographischer Systeme

1-1 **Kryptographische Schlüssel**
Könnten kryptographische Verfahren auch ohne Schlüssel auskommen? Falls ja, wie? Was wären Nachteile – und damit Vorteile der Benutzung von Schlüsseln?

1-2 **Anzahl der Schlüssel**
In einer Gruppe von 10 Teilnehmern möchte jeder mit jedem vertraulich kommunizieren. Wie viele Schlüssel werden insgesamt benötigt bei Verwendung

a) symmetrischer Konzelationssysteme,

b) asymmetrischer Konzelationssysteme?

1-3 **Schlüsselzertifikate**
Schlüsselzertifikate bestätigen die Zugehörigkeit des öffentlichen Schlüssels zum Inhaber des Zertifikats, bestätigt durch die Signatur der ausstellenden Zertifizierungsinstanz (CA). In der Praxis gibt es natürlich nicht nur eine CA, die allen Teilnehmern Zertifikate ausstellt. Beschreiben Sie für die im Zusatzmaterial (Schluesselzertifikate.pdf) beschriebenen Möglichkeiten den Ablauf für den Fall, dass Teilnehmer A das Zertifikat des Testschlüssels von Teilnehmer D überprüfen will!

1-4 **Konzelation und Authentikation**
Vertraulichkeit und Integrität sollen mit symmetrischen Systemen geschützt werden. Welche Möglichkeiten gibt es bzgl. der Reihenfolge der Anwendung der entsprechenden Funktionen, und wie sind diese Möglichkeiten bzgl. Sicherheit und Effizienz (mögliche Parallelisierbarkeit der Ausführung bei Sender und Empfänger) zu bewerten?

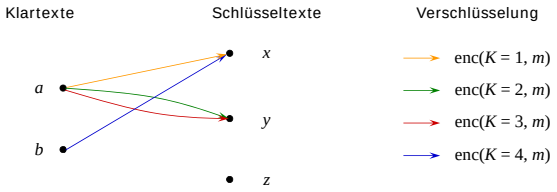
1-5 **Digitale Signatursysteme**
Kann eine informationstheoretisch sichere Signatur erzeugt werden? Begründen Sie Ihre Antwort!

1-6 **Informationstheoretische Sicherheit**

Vervollständigen Sie die folgenden Kryptosysteme mit $|K| \geq |C| \geq |M|$ so, dass sie informationstheoretisch (perfekt) sicher sind! Für alle Systeme gilt $M = \{a, b\}; C = \{x, y, z\}$.

a) $K = \{1, 2, 3, 4\}$

Ergänzen Sie die folgende Tabelle so, dass die entstehenden Schlüsseltexte gleichwahrscheinlich sind!



k_i	$\text{enc}(k_i, a)$	$\text{enc}(k_i, b)$
1	x	
2	y	
3	y	
4		x

b) $K = \{1, 2, 3, 4, 5, 6\}; p(k_i) = p(k) = \frac{1}{|K|}$

Ergänzen Sie die folgende Tabelle und geben Sie die Wahrscheinlichkeiten der Schlüsseltexte $p(c_j)$ an! (Hinweis: Mehrere Lösungen sind möglich.)

k_i	$\text{enc}(k_i, a)$	$\text{enc}(k_i, b)$
1	x	y
2		y
3		y
4		
5		
6		

c) $K = \{1, 2, 3, 4, 5\}; p(1) = 0,4; p(2) = p(5) = 0,1; p(3) = p(4)$

Ergänzen Sie die folgende Tabelle und geben Sie die Wahrscheinlichkeiten der Schlüsseltexte $p(c_j)$ an!

k_i	$\text{enc}(k_i, a)$	$\text{enc}(k_i, b)$
1	x	y
2	x	
3		
4		
5		