Klausur Grundlagen der Systemsicherheit (Teil B)

Es gelten die Bearbeitungshinweise von Teil A. Sie haben zur Beantwortung der folgenden **4 Aufgaben** 40 Minuten Zeit. Es können 40 Punkte erreicht werden. Sie dürfen keine Unterlagen verwenden. Ein (nicht programmierbarer) Taschenrechner ist erlaubt. Bitte antworten Sie kurz, stichpunktartig und präzise. Viel Erfolg!

		Aufgabe	Punkte
Name:	.....	1	
Vorname:	.....	2	
Matr.-Nr:	.....	3	
		4	
			_____

Aufgabe 1 (6) Grundlagen der IT-Sicherheit

a) (4) Grenzen Sie die Begriffe Security und Safety voneinander ab. Nennen Sie jeweils ein konkretes Beispiel.

b) (2) Nennen Sie zwei biometrische Authentifizierungsverfahren.

Aufgabe 2 (10) Kryptosysteme

Ergänzen Sie den Lückentext sinnvoll mit Begriffen aus dem Bereich der IT-Sicherheit. Beachten Sie, dass die zu ergänzenden Begriffe mehrfach auftreten können.

Kryptographische Systeme (Kryptosysteme) lassen sich sowohl zur Erreichung des Schutzziels **(1)** als auch zur Erreichung des Schutzziels **(2)** einsetzen. In den kryptographischen Algorithmus geht neben der zu schützenden Nachricht weiterhin ein **(3)** ein.

Gegenüber den **(4)** haben **(5)** Kryptosysteme den Nachteil, dass die Kommunikationspartner zur Sicherstellung der Vertraulichkeit auf einem absolut sicheren Weg den verwendeten geheimen Schlüssel austauschen müssen.

Bei **(6)** Kryptosystemen wird nicht die ganze Nachricht, sondern lediglich ein **(7)** Schlüssel mit einem **(8)** Kryptoverfahren verschlüsselt. Dadurch wird eine bessere Performanz als bei reinen **(siehe 8)** Verfahren erreicht.

Manche Kryptosysteme können nicht nur als Konzelationssysteme, sondern auch als **(9)** eingesetzt werden. Diese erlauben es einem Empfänger einer Nachricht zu beweisen, dass diese tatsächlich von einem bestimmten Sender stammt. Solche Systeme gewährleisten also das Schutzziel **(10)**.

(1) .....

(2) .....

(3) .....

(4) .....

(5) .....

(6) .....

(7) .....

(8) .....

(9) .....

(10) .....

Aufgabe 3 (16) Sicherheit von Passwörtern: Diceware

Diceware ist eine Methode, um Passwörter mit einem Würfel zu erzeugen. Dazu werden mehrere Wörter aus einer fest definierten Wortliste ausgewählt und durch Leerzeichen verbunden. Die Wörter werden mittels eines Würfels ermittelt. Für jedes Wort werden fünf Würfelwürfe gebraucht, deren Augenzahl als Ziffern einer fünfstelligen Zahl dienen. Anhand dieser Zahl wird das zugehörige Wort aus der Wortliste ausgewählt (Quelle: Wikipedia). Beispiel:

1. Es wird mit einem Würfel fünfmal gewürfelt. Die Zahlen lauten 4, 3, 1, 4 und 2.
2. Das zugehörige Wort wird in der Wortliste nachgeschlagen, z. B. „merken“.
3. Die Schritte 1 und 2 werden noch vier Mal ausgeführt. Dabei erhält man z. B. folgende Wörter: 43142 merken, 15613 boom, 22543 ekd, 66445 zonen, 51615 ragt
4. Das resultierende Passwort lautet somit „merken boom ekd zonen ragt“.

Bearbeiten Sie folgende vier Aufgaben a) bis d):

a) (4) Wie viele verschiedene Passwörter mit fünf Wörtern, die jeweils durch ein Leerzeichen verbunden sind, lassen sich so erzeugen?

b) (4) Wie viele Wörter bräuchte man, um dasselbe Sicherheitsniveau zu erreichen, das ein Schlüssel mit 512 Bit bei einem symmetrischen Konzelationsverfahren bietet?

c) (6) Ihr Freund Fred sagt: „Wenn ein Angreifer weiß, dass ein Passwort mit Diceware generiert worden ist, kann er es schneller ermitteln, weil er sich beim Brute-Force-Angriff viele Versuche spart.“ Ist diese Aussage allgemeingültig? Ermitteln Sie zur Beantwortung, wie viele Versuche ein Angreifer höchstens braucht, um das Passwort „i am old“ zu erraten,
   - für den Fall A, dass der Angreifer weiß, dass der Diceware-Ansatz bei der Erzeugung des Passworts verwendet wurde, aus wie vielen Worten das Passwort besteht und welche Wortliste verwendet wurde;
   - für den Fall B, dass der Angreifer *nicht* weiß, dass der Diceware-Ansatz bei der Erzeugung des Passworts verwendet wurde. Nehmen Sie bei der Berechnung an, dass der Angreifer die Länge des Passworts weiß und die in Frage kommenden Zeichen kennt (nur Kleinbuchstaben, keine Umlaute, keine Ziffern, keine Sonderzeichen).

d) (2) Diceware bietet bestimmte Vorteile gegenüber Passwörtern, die auf herkömmliche Weise erzeugt werden. Nennen Sie je einen Vorteil aus Nutzer- und aus Sicherheitssicht.

Aufgabe 4 (8) Sichere Protokolle (s. B. Schneier: *Applied Cryptography*, 2. Aufl., 1996, S. 86)

Anlageberater Ali versucht Kuno als neuen Kunden zu gewinnen.

Ali: Meine Anlage-Empfehlungen sind äußerst wertvoll: Letzten Monat habe ich meinen Kunden diese fünf Aktien empfohlen. Sie haben ihren Wert seitdem verdoppelt.

Kuno: Aha. Aber woher weiß ich, dass du mir nicht einfach fünf Aktien genannt hast, die im letzten Monat gut gelaufen sind? Sag mir doch einfach, welche Aktien du momentan empfiehlst. In einem Monat überprüfe ich dann die Qualität deiner Empfehlung – und wenn ich zufrieden bin, dann beauftrage ich dich.

Ali: Das kann ich leider nicht machen. Schließlich könntest du dein Geld mit meiner Empfehlung einfach selbst anlegen – ohne mich zu bezahlen.

Kuno: Das mache ich nicht, vertrau mir!

Ali: Das ist mir zu riskant. Aber ich kann dir versichern, dass ich meine Empfehlung nicht nachträglich verändert habe. Vertrau mir!

So kommen Ali und Kuno nicht weiter. Entwerfen Sie ein geeignetes Protokoll, bei dem keiner der beiden betrügen kann. Verzichten sie dabei – falls möglich – auf eine dritte Partei.