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 (8) Grundlagen der IT-Sicherheit

a) (3) Welche der drei klassischen Schutzziele lassen sich unmittelbar mit kryptographischen Techniken erreichen, welche nicht?

b) (5) Was drückt ein Angreifermodell aus und welche vier Aspekte werden dabei üblicherweise berücksichtigt?

Beachten Sie die Rückseite!

Aufgabe 2 (10) Kryptographie

a) (8) Bob möchte Alice über das Internet das Ergebnis eines Würfelwurfs senden. Bob verschlüsselt das Ergebnis vor der Übertragung mit dem deterministischen RSA-Verfahren. Alice hat bereits ein RSA-Schlüsselpaar erzeugt und dabei die folgenden Parameter verwendet: $p_A = 5$, $q_A = 11$, $e_A = 3$, $d_A = 27$. Bob hat ebenfalls ein RSA-Schlüsselpaar erzeugt und dabei folgende Parameter verwendet: $p_B = 17$, $q_B = 5$, $e_B = 3$, $d_B = 43$. Die öffentlichen Schlüssel haben die beiden bereits über einen sicheren Kanal ausgetauscht. Bob hat gewürfelt und möchte das Ergebnis nun an Alice senden. Er überträgt dazu $c_B = 9$. Zeigen Sie, dass eine passive Angreiferin (Eve), die lediglich die öffentlichen Schlüssel und c_B kennt, mittels einer Chosen-Plaintext-Attack Bobs Wurfergebnis m_B ermitteln kann. Welche Zahl hat Bob gewürfelt?

b) (2) Wie kann sich Bob vor diesem Angriff schützen?

Aufgabe 3 (6) Schadsoftware

Ergänzen Sie den Lückentext sinnvoll mit Begriffen aus dem Bereich der IT-Sicherheit.

Ein **(1)** ist ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine sogenannte Schadensfunktion ausführt. Er ist zur **(2)** fähig. Ein **(3)** ist ein Computerprogramm, das neben einer **(4)** eine **(5)** ausführt. Ein **(6)** verfügt wie ein **(siehe 1)** über die Fähigkeit zur **(siehe 2)**, ist aber im Gegensatz zu diesem ein selbstständig lauffähiges Programm.

(1) .....

(2) .....

(3) .....

(4) .....

(5) .....

(6) .....

Beachten Sie die Rückseite!

Aufgabe 4 (16) Timing-Angriff

Ein digitaler Safe lässt sich nur mit einer Chipkarte und einem Passwort öffnen. Der Safe übermittelt das eingegebene Passwort an die Chipkarte. Dort ist das korrekte Passwort abgelegt. Die Chipkarte überprüft die Eingabe und signalisiert dem Safe das Ergebnis. Dabei kommt folgende Funktion zum Einsatz:

```
1 boolean check(char[] input) {
2     char[] pwd = this.getStoredPassword();
3     if(input.length == pwd.length) {
4         for(int i=0; i < input.length; i++) {
5             if(input[i] != pwd[i]) return false;
6         }
7     } else return false;
8     return true;
9 }
```

a) (4) Identifizieren Sie die zwei Fehler in *check*, die einen Timing-Angriff ermöglichen.

Fortsetzung von Aufgabe 4

Angreifer Mallory weiß, dass das Passwort aus Kleinbuchstaben (inkl. ä, ö, ü und ß) und Ziffern bestehen kann. Ein Brute-Force-Angriff ist allerdings aussichtslos, da die Chipkarte nach 100 Fehlversuchen einen Selbstzerstörungsmechanismus aktiviert. Mallory hat bereits eine Reihe von häufig verwendeten Passwörtern ausprobiert – bislang jedoch ohne Erfolg. Die Antwortzeiten der Chipkarte sind in der folgenden Tabelle dargestellt (Werte in Nanosekunden).

1	123456	15328	11	sauber	15344	21	sicher	15349
2	banane	15326	12	scares	15367	22	sind	15317
3	benno	15311	13	schaden	15315	23	sinn	15311
4	bernhardiner	15319	14	schimpanse	15318	24	sommer	15351
5	datenträger	15312	15	schimpfen	15318	25	super	15319
6	edwin	15316	16	schirm	15385	26	tag	15315
7	hallo	15318	17	schlange	15312	27	übung	15320
8	ich	15319	18	schutz	15384	28	urlaub	15331
9	katzen	15332	19	scopes	15361	29	vorlesung	15315
10	klausur	15314	20	scrape	15364	30	würste	15336

b) (8) Was verraten die Zeiten über das Passwort? Womit fährt Mallory fort?

c) (4) Kann Mallory das Passwort noch vor der Selbstzerstörung ermitteln? (Begründung!)