Name _____ Matrikelnummer _____

Aufgabe	1	2	3	4	5	Σ	Note
Punkte	/25	/20	/15	/20	/10	/90	

Klausur Rechnersicherheit

Sommersemester 2015

21.07.2015

Marian Margraf

Bearbeitungshinweise

- Schreiben Sie *jetzt* Ihren Namen auf das Deckblatt.
- Die Klausur besteht aus fünf Aufgaben und insgesamt 90 Punkten.
- Sie haben 90 Minuten Bearbeitungszeit.
- 45 Punkte sind hinreichend, um die Klausur zu bestehen.
- Als Hilfsmittel ist ausschließlich ein beliebig beschriftetes Blatt A4-Papier zulässig.
- Beantworten Sie alle Aufgaben direkt auf der Angabe. Verwenden Sie ggf. die Rückseiten.
- Diese Klausur besteht aus 7 Seiten. Überprüfen Sie zu Beginn der Klausur, ob Ihr Geheft vollständig ist.

Aufgabe 1: Grundlagen [25 Punkte]

1. Geben Sie an, unter welchen Bedingungen ein Benutzer im einfachen Bell-LaPadula Sicherheitsmodell auf ein Objekt sowohl lesen als auch schreiben darf. [3 Punkte]

2. Erklären Sie, warum Kollisionen in Hashfunktionen unvermeidbar sind. [3 Punkte]

3. Erklären Sie den Unterschied zwischen schwacher und starker Kollisionresistenz. [5 Punkte]

4. Beschrieben Sie ein Instanzauthentisierungsverfahren, dass nicht anfällig für Phishing, Man-in-the-Middle- und Replay-Angriffe ist. [3 Punkte]

5. Erläutern Sie kurz, worauf die Sicherheit Elliptischer Kurven im Diffie-Hellmann-Schlüsselaustausch beruht. [2 Punkte]

6. Worauf basiert im Web of Trust das Vertrauen in die Schlüssel? [3 Punkte]

7. Nach welchen Prinzipien erzeugen moderne Betriebssysteme Zufallszahlen, die für kryptographische Anwendungen geeignet sind? [2 Punkte]

8. Welche Sicherheitsanforderungen stellt man an Zufallszahlengeneratoren? [2 Punkte]

9. Erläutern Sie die Vorteile von Zwei-Faktor-Authentisierung. [2 Punkte]

Aufgabe 2: Block Cipher und Betriebsmodus [20 Punkte]

1. Erklären Sie, wie in der Praxis Klartexte verschlüsselt werden, die über die (häufig konstante) Klartextlänge der Verschlüsselungsmethode hinaus gehen. [5 Punkte]

2. Erläutern Sie den Betriebsmodus Electronic Code Book und seine Schwäche. [5 Punkte]

3. Im Cipher Block Chaining (CBC) Betriebsmodus wird der Klartext vor der Verschlüsselung mit dem Schüsseltext des vorhergehenden Blocks XOR-verknüpft. Der erste Block wird entsprechend mit dem Initialisierungsvektor XOR-verknüpft. Beschreiben Sie die Entschschlüsselung im CBC Betriebsmodus. [5 Punkte]

4. Angenommen, im k-ten Schlüsseltextblock ist ein Übertragungsfehler. Geben Sie alle Blöcke an, die nicht korrekt entschlüsselt werden können. [5 Punkte]

Aufgabe 3: Hashfunktionen nach Merkle-Damgård [15 Punkte]

1. Gegeben sei eine Kompressionsfunktion $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Erläutern Sie das Konstruktionsschema für Hashfunktionen nach Merkle-Damgård. [4 Punkte]

2. Nennen Sie ein Beispiel für eine sichere Kompressionsfunktion. [2 Punkte]

Sei $H : \{0,1\}^* \to \{0,1\}^n$ eine Hashfunktion.

3. Was versteht man unter starker Kollisionsresistenz? [2 Punkte]

4. Friedrich (F, the fool) glaubt, seine Hashfunktion H erreicht ein Sicherheitsneveau von 100 bit bezüglich starker Kollisionsresistenz bei Brute-Force-Angriffen, wenn der Bildraum die Größe 2^{100} hat, denn schließlich ist die Wahrscheinlichkeit, eine Kollision zu finden dann $\frac{1}{2^{100}}$. Erläutern Sie warum n tatsächlich deutlich größer sein muss, um das gewünschte Sicherheitsniveau zu erreichen. [7 Punkte]

Aufgabe 4: Cross Site Request Forgery [20 Punkte]

1. Erläutern Sie Cross Site Request Forgery am Beispiel eines HTTP GET-Requests. [5 Punkte]

2. Friedrich möchte CSRF verhindern, indem sein Webdienst nur POST-Requests annimmt. Erläutern Sie anhand eines Beispiels, warum diese Maßnahme wirkungslos ist. [5 Punkte]

3. Eine gängige Methode, CSRF zu verhindern, besteht darin, dass Requests eine zufällige ID an den Server zurücksenden müssen. Der Zugriff auf diese ID wird vom Browser nach der Same-Origin-Content-Policy verhindert. Konstruieren Sie einen Angriff, der eine Cross-Site-Scripting-Lücke ausnutzt, um diesen Schutz zu umgehen. [10 Punkte]

Aufgabe 5: Informationsfluss [10 Punkte]

1. Erklären Sie den Unterschied zwischen statischer und dynamischer Informationsflusskontrolle. [3 Punkte]

2. Geben Sie ein Beispiel, warum in praktischen Anwendungen statische Informationsflusskontrolle nicht ausreichend ist. [7 Punkte]