Name _____ Matrikelnummer _____

Einführung in die Informationssicherheit

Bitte lesen Sie die Fragen sorgfältig durch und überprüfen Sie am Ende ob Sie die Fragen vollständig beantwortet haben.

1. Was bedeutet „exhaustive key search“? (1P)
2. Richtig oder Falsch?: Das Faktorisieren von bestimmten großen (zusammengesetzten) Zahlen ist ein schwieriges mathematisches Problem. Begründen sie ihre Antwort. (1P)
3. Was ist eine digitale Signatur? (1P)
4. Welche Sicherheitsaspekte sind bei elektronischem Geld besonders zu beachten? (2P)
5. Was ist „OS fingerprinting“? (1P)
6. Erklären sie das Prinzip einer Replay Attacke. (1P)
7. Erklären sie die Begriffe GID und UID. (1P)
8. Wofür benutzt man ein „Key Distribution Center“? (1P)
9. Welcher Typ elektronischer Signaturen ist gleichgestellt mit handschriftlichen Unterschriften? (1P)

Punkte _____

Antworten

1. Das vollständige Durchsuchen des Schlüsselraumes wird so bezeichnet. Alle möglichen Schlüssel werden ausprobiert solange bis der korrekte Schlüssel gefunden wird.

2. Richtig, die besten bekannten Algorithmen zum Faktorisieren von sehr grossen zusammengesetzten Zahlen brauchen (sub)exponentielle Laufzeit.

3. Datenstring der eine Nachricht mit einem Unterzeichner verbindet.

4. Anonymität (es sollte nicht einfach möglich sein die Handlungen eines Benutzers mittels seines Geldes mitverfolgen zu können), Kopieren (bzw. das mehrfache Ausgeben einer Münze, das Problem von Kopien muss hinreichend gelöst sein).

5. Ist eine Technik mit der ein Angreifer die Art (Version) des Betriebssystems herausfinden kann.

6. Ein Angreifer fängt ein Passwort während einer Authentisierung ab und benutzt es später um sich selbst zu authentisieren.

7. Group ID (gibt an zu welcher Benutzergruppe der Benutzer gehört), User ID (erlaubt es den Benutzer eindeutig zu identifizieren)

8. Zum Verteilen von Schlüsseln in Systemen die auf symmetrischer Verschlüsselung basieren.

9. Eine qualifizierte (sichere) elektronische Signatur, die auf einem qualifizierten Zertifikat beruht.

Gesamtpunkte: 10

„Gute Ratschläge“

- In dieser Klausur wird „Wissen“ geprüft, also erwarte ich mir das sie den Stoff, der im Skriptum steht, auch gelernt haben.
- Es werden keine Algorithmen genau geprüft (Ausnahme RSA). Also, ich frage nicht wie DSA oder ECDSA genau funktionieren. Ich frage aber sehr wohl, wie ein Algorithmus prinzipiell funktioniert. Zum Beispiel kann durchaus eine Frage kommen wo ich sie bitte das Prinzip einer Signaturerstellung (für Signaturschemen mit Appendix) funktioniert. Oder, wie das Verschlüsseln mit RSA prinzipiell geht.
- Sie sollen die Fragen typischerweise kurz beantworten. Das heißt, das sie die korrekte Antwort in zwei oder drei Sätzen formulieren müssen. Typischerweise bedeutet das, dass sie nicht um den heissen Brei herumreden sollen, schwafeln ist nicht erwünscht!