Universität Mannheim
Fakultät für Mathematik und Informatik
Lehrstuhl für Praktische Informatik IV
Professor Dr. W. Effelsberg

Hauptdiplomklausur Informatik
September 1997: Seminar [Weis] – Digitales Geld im Internet

Name:..... Vorname:.....

Matrikel-Nr.:..... Semester:..... Fach:.....

Hinweise:

1. Bitte füllen Sie sofort den Kopf des Deckblattes aus.
2. Überprüfen Sie bitte Ihr Klausurexemplar auf Vollständigkeit (5 Seiten).
3. Tragen Sie die Lösungen – soweit möglich – direkt in die Klausur ein.
4. Zugelassene Hilfsmittel: nicht programmierbarer Taschenrechner
5. Bearbeitungszeit: 33 Minuten.

Aufgabe	max. Punktzahl	Punkte
1	15	
2	10	
3	8	
Summe	33	

Aufgabe 1 *[15 Punkte]*

Nennen Sie die sechs von Okamoto und Oha formulierten und allgemein als wünschenswert anerkannten Anforderungen für Digitales Geld und geben Sie an in wie weit die im Seminar diskutierten Implementierungen (digicash, Universal Electronic Cash, Brands Cash, Millicent, Payword, Micormint) diese Forderungen erfüllen.

Aufgabe 2 *[10 Punkte]*

Erläutern Sie das “double spending problem” und geben Sie an welche Gegenstrategien die im Seminar diskutierten Implementierungen dagegen anwenden.

Aufgabe 3 *[8 Punkte]*

Folgender Vereinfachungsvorschlag für das Digicash-Protokoll von Chaum sei gegeben:

Alice erzeugt eine beliebige Seriennummer S und sendet sie geblinded mit der Zufallszahl r zur Bank:

$$M = S \cdot (r^e)$$

e ist der öffentliche „5 DM“-Schlüssel der Bank. Die Bank unterschreibt M mit ihrem „5 DM“-Schlüssel.

$$M^d = (S \cdot r^e)^d = S^d \cdot r$$

Alice entfernt r und erhält S^d. Die Bank erkennt mit ihrem geheimen „5 DM“-Schlüssel d die unterschriebene Seriennummern als Fünfmarkstück an.

Diskutieren Sie die Sicherheit dieses Vorschlages.