

Aufgabe 22: (8 Punkte)

In der Vorlesung wurde das *Needham-Schroeder-Protokoll* zur Authentifizierung vorgestellt. Es besitzt jedoch eine Schwachstelle, falls ein Angreifer in den Besitz eines gültigen Sitzungsschlüssels gelangen kann. Beschreiben Sie das Vorgehen bei dieser Attacke und erläutern Sie anschließend das sogenannte *Otway-Rees-Protokoll*, das diese Schwachstelle vermeiden soll. Diskutieren Sie auch kurz die Sicherheit des letzteren Verfahrens.

Aufgabe 23: (4 Punkte)

Ein Protokoll zur Senderanonymität ist das sog. Protokoll der dinierenden Kryptographen, das sich durch folgendes Beispiel illustrieren lässt:

Drei Kryptographen A , B und C gehen in einem Restaurant essen. Nach dem Essen teilt ihnen der Restaurantbesitzer mit, dass das Essen anonym bezahlt wird, und zwar entweder von einem der drei Kryptographen oder von ihrem Arbeitgeber. Falls einer der drei bezahlt, soll dessen Anonymität gewahrt bleiben; zahlt jedoch ihr Arbeitgeber, so möchten die Kryptographen dies gerne wissen.

Wie können die drei ihr Problem lösen? (mit Begründung)

Aufgabe 24: (2 Punkte)

Schicken Sie 4 Links zu interessanten kryptographischen Webseiten.