Prof. Dr. Rüdiger Weis

Sicherheit in Verteilten Systememm

Übungsblatt 5: Schüsselverwaltung

Aufgabe 1 Key Freschness (5 Punkte)

Erläutern Sie Gründe für Forderung nach Key Freschness in Verteilten Systemen.

Aufgabe 2 Key Distribution Center (5 Punkte)

Geben Sie ein einfaches Protokoll an, für die Schüsselvereinbarung zwischen Alice und Bob mit Hife eines symmetrische Algorithmen verwendenden Key Distribution Center.

Aufgabe 3 Schlüsselmanagement (9 Punkte)

Eine Gruppe von 10 Teilnehmern soll verschlüsselt kommunizieren.

- Wie viele Schlüssel müssen ausgetauscht werden, falls Public Key Verfahren verwendet werden?
- Wieviele wären es, wenn keine Public Key Verfahren verwendet werden? Nennen Sie zwei mögliche Szenarien.

Aufgabe 4 KDC versus PKI (12 Punkte)

Diskutieren Sie Vor- und Nachteile eines Key Distribution Center gegeüber einer PKI basierten Lösung

Aufgabe 5: Security Properies Hashfunktionen (9 Punkte)

Was versteht man bei der Betrachtung von Hashfunktionen unter preimage resistance, image resistance und second preimage resistance.