technische universität dortmund

Prof. Dr. Jan Jürjens, Christian Wessel
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
Modellbasierte Softwaretechniken
für sichere Systeme – 10.04.2012

Modellbasierte Softwaretechniken für sichere Systeme - Übung 2

1 Symmetrische Verschlüsselung (3 Punkte)

Wird die Vertraulichkeit beim Versenden der Nachricht m bei der Verwendung von symmetrischer Verschlüsselung und verschiedenen Schlüsseln K_1 und K_2 gewahrt?

- $\{\{m\}_{K_1}\}_{K_2} :: K_1$
- $\{m\}_{K_1} :: \{m\}_{K_2} :: K_1$
- $\{\{m\}_{K_1}\}_{K_2} :: \{K_1\}_{K_2}$

2 Verschlüssung mit RSA (3 Punkte)

Der RSA-Signaturalgorithmus D hat die Homomorphie-Eigenschaft, sodass $D(M_1 :: M_2) = D(M_1) :: D(M_2)$ für alle Nachrichten M_1, M_2 gilt. Wie könnte ein Angreifer den Geldbetrag in der Signatur D ("Ich schulde dir 10 EUR.") auf 100 EUR erhöhen, falls kein Hash verwendet werden würde? Der Algorithmus soll dabei nicht gebrochen werden. Zeichenketten können als Konkatenation von Zeichen aufgefasst werden.

3 JCryptool

JCryptool ist ein freies Programm zur Anwendung und Analyse kryptographischer Algorithmen, welches speziell für die Lehre konzipiert wurde. Laden Sie die neueste stabile Version Version des Programms unter http://www.cryptool.org/de/download-jct-de herunter und lesen Sie sich die Funktionsweise des Vigenère/Cäsar-Algorithmus im Handbuch des JCrypttools durch. Dieses finden Sie unter Kryptologie ->Algorithmen ->Verschlüsselung ->Klassisch. Auf der Vorlesungswebseite finden Sie zwei Textdateien, die jeweils einen verschlüsselten Text enthalten. Die Texte enthalten keine Leerzeichen und bestehen lediglich aus Grossbuchstaben ohne Umlaute. Benutzen Sie diese um die beiden folgenden Aufgaben mit Hilfe des JCryptools zu lösen.

3.1 Cäsar-Chiffre (1 Punkt)

Entschlüsseln Sie den Text aus der Datei *aufgabe_2_3_1.txt* und geben Sie die Verschiebung an.

3.2 Vigenère-Chiffre

3.2.1 Entschlüsseln Sie den Text aus der Datei aufgabe_2_3_2.txt mit Hilfe des Vigenère-Breakers im JCryptool und geben Sie das Codewort an. (2 Punkte)

Hinweis: Das Codewort besteht aus 4 Zeichen.

3.2.2 Wie wird die Schlüssellänge im Vigenère-Verfahren berechnet? (1 Punkt)