technische universität dortmund

Prof. Dr. Jan Jürjens, Thomas Ruhroth
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
SFL – Abgabe: 3.12.2014

Sicherheit: Fragen und Lösungsansätze – Übung 4

AUFGABE 1(One Way Hash) (2BP+4LP):

1. Implementieren Sie die Funktionen als einfache Javaoperationen **public String hashX(String in)**. Die Funktionen sollen dabei möglichst laufzeitoptimal implementiert werden. (4BP)
2. Sind die gegeben Funktionen One-Way-Hash-Funktionen? Wenn Ja, begründen Sie ihre Antwort (Max. 50 Worte je Funktion). Wenn Nein, implementieren Sie die Umkehrfunktion.
3. Sind die Funktionen kollisionsresistent bzw. schwach kollisionsresistent? Betrachten Sie als Domäne alle möglichen Strings, alle deutschen Texte und die Menge aller Shakespeare-Sonette (Max. 100 Worte je Sonnet).
4. Berechnen Sie für jede Funktion die Werte für
   - "Sicherheit: Fragen und Loesungsansaetze"
   - hash2"Dies ist ein Beispiel für eine kryptografische Hash-Funktion."
   - "SFL"

Funktionen:

1. Für einen Text wird die Anzahl der einzelnen Buchstaben (Groß/Kleinschreibung wird ignoriert) bestimmt und als Ziffernfolge aller Buchstabenzahlen ohne führende Nullen im Dezimalsystem ausgegeben. Zum Beispiel führt der Text "Implementieren Sie folgende einfache Hash-Funktion" zum Hashwert "20119312501226210122100000".
2. Die Buchstaben des gegebenen Textes werden in Zahlen von 1 bis 26 "übersetzt", das Ergebnis wird in Blöcke zu je zwölf Ziffern getrennt, ein möglicherweise unvollständiger letzter Block wird ignoriert. Für jeden Block wird jetzt folgendes durchgeführt:
   - Bilde die Summe S_u aller Ziffern an ungeraden Stellen.
   - Bilde die Summe S_g aller Ziffern an geraden Stellen.
   - Addiere S_u mit $3S_g$.
   - Ziehe die letzte Ziffer der Summe von 10 ab. (Sollte das Ergebnis 10 sein, verwende 0)

   Die Folge der Ergebnisse wird zur Ausgabe. Zum Beispiel führt der Text "Implementieren Sie folgende einfache Hash-Funktion" zum Hashwert "81222".

3. Jeder Buchstabe wird wie bei der Caesarverschlüsselung durch einen anderen Buchstaben ersetzt. Es wird dabei jeder Buchstabe durch den drei Positionen weiter im Alphabet folgenden ersetzt. Dabei wird nach dem "Z" beim "A" weitergezählt. Die Groß/Kleinschreibung bleibt genauso wie alle anderen Zeichen unverändert.

AUFGABE 2(Schlüsselaustausch) (4LP):

Drei Kommunikationspartner, A, B, C, wollen miteinander kommunizieren. Sie haben sich auf einen Schlüsselaustausch gemäß des Diffie-Hellman-Verfahrens geeignet, woraufhin C die Primzahl $p = 19$ vorgeschlagen hat. B hat dann mit $\alpha = 3$ die primitive Wurzel festgelegt.

1. Der private Schlüssel von A laute 11, der öffentliche Schlüssel von B 14. Berechnen Sie den gemeinsamen Schlüssel der beiden Teilnehmer.
2. C hat mit seinem privaten Schlüssel, 17, schon einen gemeinsamen Schlüssel, 2, hergestellt. Wer ist sein Kommunikationspartner?