SZS Blatt 3

Christian Baumann 3164561, st142624@stud.uni-stuttgart.de
Ellen Hafner 3253401, st151037@stud.uni-stuttgart.de
Marvin Knodel 3229587, st149003@stud.uni-stuttgart.de
Lion Wagner 3231355, st148345@stud.uni-stuttgart.de

28. November 2018

Christian Baumann 3164561
Ellen Hafner 3253401
Marvin Knodel 3229587
Lion Wagner 3231355

Aufgabe 1

a)

Normal: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Schlüssel: O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

Geheimer Text: ELE Eqogdufk Gqngzs
↓↓↓ ↓↓↓↓↓↓↓ ↓↓↓↓↓↓
Normaler Text: SZS Security Uebung

b)

Symmetrisch:
Es gibt nur einen Schlüssel zum ver- und entschlüsseln.

Asymmetrisch:
Es gibt zwei Schlüssel, einen öffentlichen der zum entschlüsseln und einen privaten der zum verschlüsseln verwendet wird.

c)

Bei HTTPS wird der symmetrische Schlüssel asymmetrisch verschlüsselt.
Der verschlüsselte Schlüssel und der öffentliche Schlüssel werden dann an den User gesendet und mit dem symmetrischen Schlüssel werden die Nutzdaten verschlüsselt.
Es ist sinnvoll um erhöhte Sicherheit zu garantieren.

Christian Baumann	3164561
Ellen Hafner	3253401
Marvin Knodel	3229587
Lion Wagner	3231355

Aufgabe 2

a)

b)

c)

Christian Baumann	3164561
Ellen Hafner	3253401
Marvin Knodel	3229587
Lion Wagner	3231355

Aufgabe 3

a)

b)

c)