Verschlüsselung

DEZSYS06

Pitirut Stefan, Willinger Andreas

28.01.2015

Inhaltsverzeichniss

[Aufgabenstellung 3](#_Toc410332371)

[Designüberlegung: 4](#_Toc410332372)

[Arbeitsaufteilung 6](#_Toc410332373)

[Aufwandsschätzung 6](#_Toc410332374)

[Arbeitsdurchführung 6](#_Toc410332375)

[Erfolge: 6](#_Toc410332376)

[Niederlagen: 6](#_Toc410332377)

[Verwendete Technologien 7](#_Toc410332378)

[AES 7](#_Toc410332379)

[RSA 7](#_Toc410332380)

[Testen des Programmes 8](#_Toc410332381)

[Quellen 9](#_Toc410332382)

# Aufgabenstellung

**Kommunikation [12Pkt]**  
Programmieren Sie eine Kommunikationsschnittstelle zwischen zwei Programmen (Sockets; Übertragung von Strings). Implementieren Sie dabei eine unsichere (plainText) und eine sichere (secure-connection) Übertragung.

Bei der secure-connection sollen Sie eine hybride Übertragung nachbilden. D.h. generieren Sie auf einer Seite einen privaten sowie einen öffentlichen Schlüssel, die zur Sessionkey Generierung verwendet werden. Übertragen Sie den öffentlichen Schlüssel auf die andere Seite, wo ein gemeinsamer Schlüssel für eine synchrone Verschlüsselung erzeugt wird. Der gemeinsame Schlüssel wird mit dem öffentlichen Schlüssel verschlüsselt und übertragen. Die andere Seite kann mit Hilfe des privaten Schlüssels die Nachricht entschlüsseln und erhält den gemeinsamen Schlüssel.  
  
**Sniffer [4Pkt]**  
Schreiben Sie ein Sniffer-Programm (Bsp. mithilfe der jpcap-Library [http://jpcap.sourceforge.net](http://jpcap.sourceforge.net/) oder jNetPcap-Library <http://jnetpcap.com/>), welches die plainText-Übertragung abfangen und in einer Datei speichern kann. Versuchen Sie mit diesem Sniffer ebenfalls die secure-connection anzuzeigen.  
  
**Info**  
Gruppengröße: 2 Mitglieder  
Punkte: 16

* Erzeugen von Schlüsseln: 4 Punkte
* Verschlüsselte Übertragung: 4 Punkte
* Entschlüsseln der Nachricht: 4 Punkte
* Sniffer: 4 Punkte

# Designüberlegung:

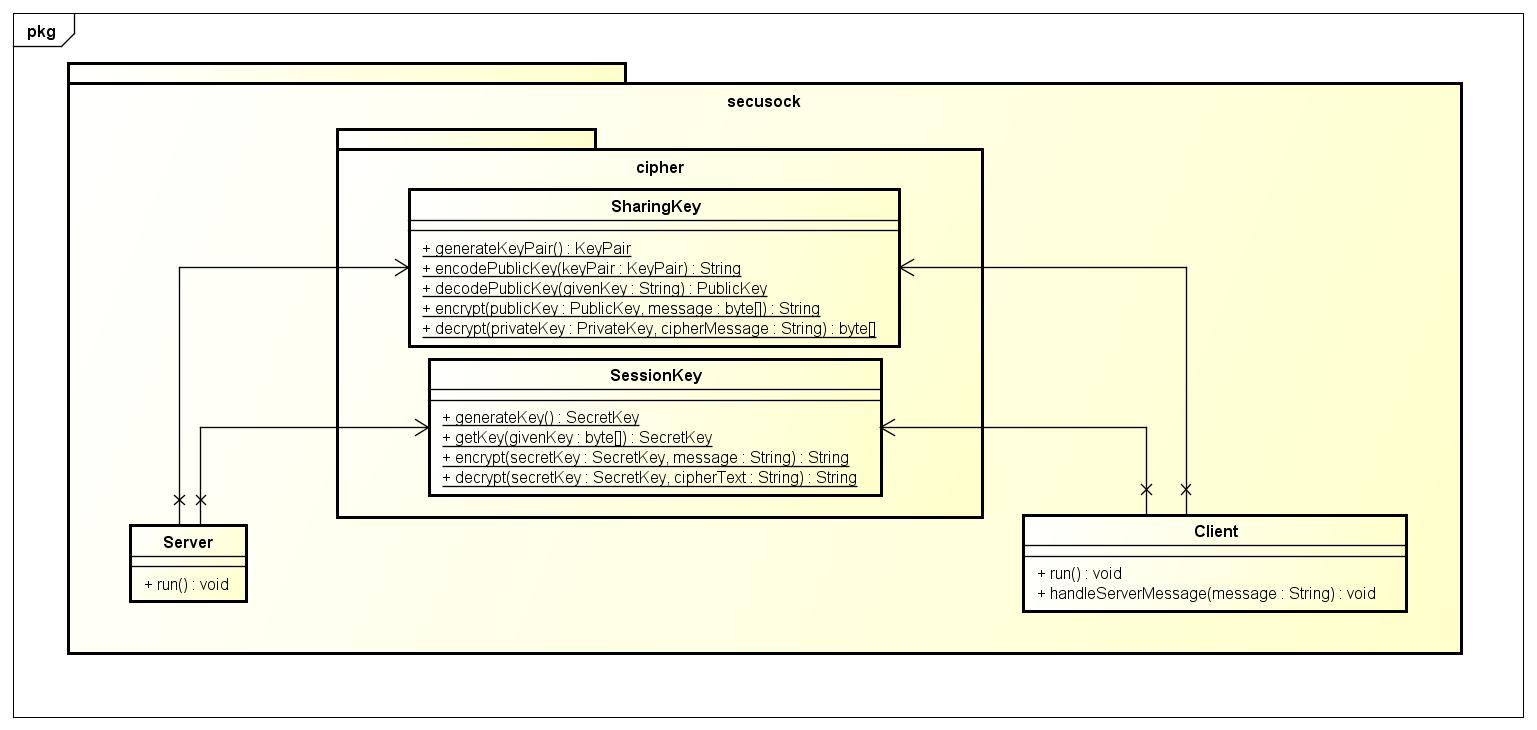
Als erstes hatten wir die Idee, die jeweiligen Verschlüsselungsalgorithmen auszuprobieren, somit habne wir diese als Erstes versucht zu implementieren. Nachdem wir dies realisiert hatten, haben wir uns überlegt, die jeweiligen Schritte mittels einer „Start-Klasse“ darzustellen.

Unser nächster Gedankengang war, wie wir die Übertragung der jeweiligen Schlüssel/Nachrichten realisieren sollten.

Den Entschluss, den wir gefasst haben war folgender:

* Client hat keinen sessionKey:
  + Der Befehl !keys muss eingegeben werden um die folgenden Schritte zu ermöglichen
    - erstellt den SharingKey basierend auf RSA
    - sendet den PublicKey via Sockets an den Server
      * 🡪 GENKEY | publicKey
    - Server erhält den verschlüsselten PublicKey
    - Server erstellt den AES secretKey und verschlüsselt ihn mithilfe des publicKeys
    - Server schickt diesen mithilfe von Sockets an den Client
      * 🡪 SETKEY | secretKey
    - Client erhält den secretKey und entschlüsselt ihn mithilfe des privateKeys und setzt ihn auch (local)
  + Wenn der !keys Befehl nicht verwendet wird, sendet der Client die Nachricht unverschlüsselt
    - 🡪 PLAINMSG | message
* Client hat sessionKey:
  + Client verschlüsselt Nachricht und sendet diese an den Server mittels Sockets
    - 🡪 ENCMSG | message
  + Server entschlüsselt mithilfe des sessionKeys und zeigt die Nachricht an
* In beiden Fällen sendet der Server GOTMESSAGE | 0 zurück

Unser Konzept schaut wie folgt aus:



# Arbeitsaufteilung

|  |  |  |
| --- | --- | --- |
|  | **Pitirut** | **Willinger** |
| Dokumentation | X | X |
| Designüberlegung | X | X |
| Cipher |  | X |
| Client | X | X |
| Server | X | X |
| Sniffer | X |  |

# Aufwandsschätzung

|  |  |  |
| --- | --- | --- |
| **Pitirut** | Geschätzte Zeit | Tatsächliche Zeit |
| Dokumentation | 2 h | 1 h 30 m |
| Designüberlegung | 2 h | 30 m |
| Client | 1 h 30 m | 1 h |
| Server | 1 h 30 m | 1 h |
| Sniffer | 2 h | 2 h 30 m |
| **Gesamt:** | **9 h** | **6 h 30 m** |

|  |  |  |
| --- | --- | --- |
| **Willinger** | Geschätzte Zeit | Tatsächliche Zeit |
| Dokumentation | 1 h | 1 h |
| Designüberlegung | 1 h | 30 m |
| Cipher | 2 h 30 m | 3 h |
| Client | 1 h 30 m | 1 h |
| Server | 1h 30 m | 1 h |
| **Gesamt:** | **7 h 30 m** | **6 h 30 m** |

# Arbeitsdurchführung

## Erfolge:

* Sniffer war in Python einfacher als erwartet
* Encryption schneller realisiert als gedacht, jedoch Zeitverlust durch die Niederlage

## Niederlagen:

* Beim Ausführen auf einer standard Java installation, ist das Problem aufgetaucht, dass ein „Invalid Key size or Parameters“ Fehler geworfen wird. Dieser entstand daraus, da wir nicht die JAR’s hatten, um die Keysize limitation von AES (die Standardmäßig auf 16Bit limitiert ist) aufzuheben. Diese JAR’s befinden sich in dem REQUIRED Ordner, diese MÜSSEN in das /lib/security Verzeichnis der JRE eingefügt werden.

# Verwendete Technologien

## AES

*“The Advanced Encryption Standard is based on a design principle known as a substitutionpermutation network. Its predecessor DES used a Feistel network(a network of linked Feistel functions). AES’s block size is fixed on 128 bits and a key size of 128, 192, or 256 bits. Based on the Rijndael specification the block and key sizes may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. Different from the last chapter DES, the number of rounds are specified as follows:*

*• 10 cycles of repetition for 128-bit keys*

*• 12 cycles of repetition for 192-bit keys*

*• 14 cycles of repetition for 256-bit keys*

*Each round consists of 4 processing steps, some of them depend on the encryption key itself. To transform the ciphertext back into the original plaintext the same encryption key and a set of reverse rounds are applied.” [1]*

## RSA

*“RSA is by far the simplest public key encryption algorithm to understand, and to implement. It is named after the three inventors - Ron Rivest, Adi Shamir, and Leonard Adleman, and has also withstood years of extensive cryptanalysis (the study of cracking the ciphertexts).” [1]*

# Testen des Programmes

Um das Programm auszuführen, muss Apache Ant installiert sein.  
Wenn das der Fall ist, wechselt man in das Verzeichnis, wo die build.xml liegt und führt folgenden Befehl aus:

|  |
| --- |
| ant jar |

Dieser Befehl erzeugt eine JAR Datei, die im Ordner out/ gefunden werden kann.

Sobald der obige Befehl fertig ist,wechselt man in den Ordner out/ und das Programm kann mithilfe des folgenden Kommandos ausgeführt werden:

|  |
| --- |
| java -jar SecuSock\_<nummer>\_Pitirut-Willinger.jar |

Wobei <nummer> das aktuelle Datum im Format YYYYMMdd ist, z.B. 20150129.

Im Folgenden wählt man dann den Typ der Ausführung aus (Server/Client) und gibt die benötigten Informationen ein (IP/port).

# Quellen

[1] Gary Ye, Christian Janeczek, Cryptography, zuletzt bearbeitet: 19.01.15, zuletzt geöffnet: 29.01.15