Verschlüsselung

DEZSYS06

Pitirut Stefan, Willinger Andreas

28.01.2015

Inhaltsverzeichniss

[Aufgabenstellung 3](#_Toc410208067)

[Designüberlegung: 4](#_Toc410208068)

[Arbeitsaufteilung 7](#_Toc410208069)

[Aufwandsschätzung 7](#_Toc410208070)

# 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

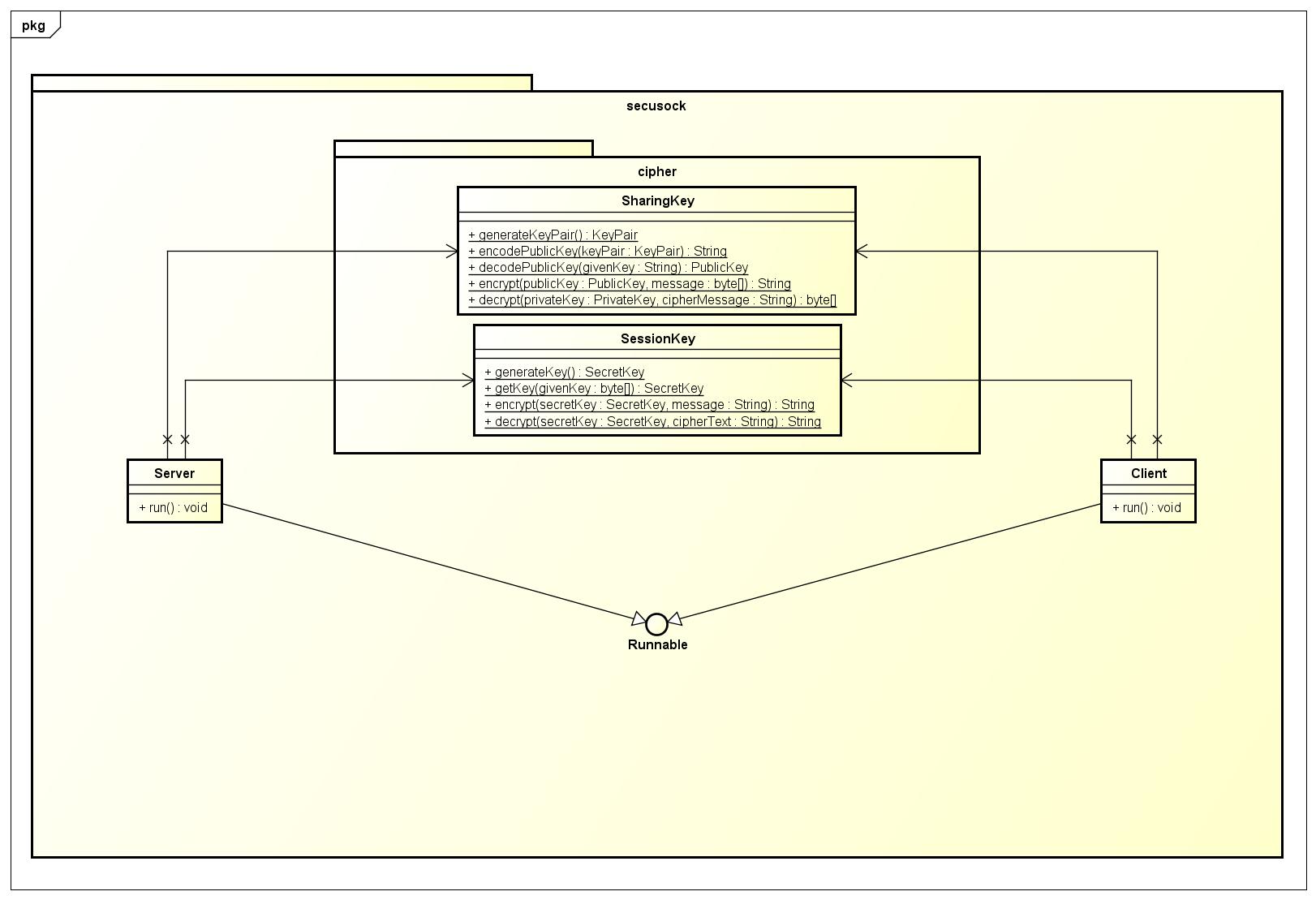
# Designüberlegung:

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:
  + erstellt den SharingKey basierend auf RSA
  + sendet den PublicKey via Sockets an den Server
    - 🡪 Pkey | „ eine Nachricht “
  + Server erhält den Verschlüsselten PublicKey
  + sss
  + sss

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 |  |
| Designüberlegung | 2 h |  |
| Client | 1 h 30 m | 1 h |
| Server | 1 h 30 m | 1 h |
| Sniffer | 2 h |  |
| **Gesamt:** | **9 h** | **h** |

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

# Arbeitsdurchführung

## Erfolge:

## Niederlagen:

# Verwendete Technologien

# Testen des Programmes

# Quellen