Projekt B Konzeptbericht

Formales

Professor: Prof. Nils Martini

Studenten:

* Matthias Pawlitzek, Matrikelummer *2315565*, 5. Fachsemester
* Simon Hoyos, Matrikelummer *2319104*, 5. Fachsemester
* Max Bauer, Matrikelummer *2323129*, 5. Fachsemester

Projektidee

Entwickeln eines Desktop - Chatprogramms im Stil von WhatsAppWeb, das die kryptographischen Prozesse im Hintergrund visualisieren soll. Ziel ist es, angehenden Informatikern die komplexen Algorithmen interaktiv näher aufzeigen zu können.

Das Projekt soll einen Lerneffekt beim Benutzer hervorrufen, damit dieser mithilfe dieses Programms die einzelnen kryptografischen Prozesse besser verstehen und üben kann.

Dabei soll der Benutzer in Echtzeit anhand eines Logfensters beobachten können, wie digitale Kommunikation auf verschiedene Wege verschlüsselt wird. Die Kommunikation wird immer hybrid-verschlüsselt ablaufen. Der Benutzer kann für jede abzusendende Nachricht das asymmetrische sowie das symmetrische Verschlüsselungsverfahren anpassen, mit diesen Auswahlmöglichkeiten:

Asymmetrisch: RSA, ElGamal

Symmetrisch: Affine Chiffre, Block-Permutations Chiffre, Vigenère Chiffre, Hill Chiffre

Operationsmodi: ECB, CBC, CFB

Ablauf

Beim Login wird der Benutzer sich mit seinem Namen einloggen und seine Schlüsselpaare der zwei vorhandenen asymmetrischen Verfahren zufällig berechnen und die beiden public keys an den Server senden. Falls der Name schon vergeben ist, wird der Benutzer aufgefordert, einen neuen Namen einzugeben. Außerdem wird er sich die vorhandenen public keys bereits eingeloggten User herunterladen.

Daraufhin wird die Main View angezeigt, die aus drei Elementen bestehen wird:

Liste der Online User, Chatfenster, Logfenster.

Der Benutzer kann nun als einzige Interaktion einen anderen Online User (hier User A und User B) auswählen, woraufhin das Modus - Dialogfenster angezeigt wird, das den User A auswählen lässt, welches asymmetrische Verfahren, welches symmetrische Verfahren, welches symmetrische Geheimnis ***S*** sowie welchen Operationsmodus er für die initiale Nachricht an User B verwenden möchte. Nachdem er alle Infos angegeben hat, wird das Chatfenster aktiviert, was den User A eine Nachricht an User B verfassen lässt.

Außerdem wird neben dem Eingabefeld die gewünschte Verschlüsselungskombination angezeigt, die sich mit einem Klick darauf wieder im Modus – Dialogfenster individuell anpassen lässt. So kann für jede Nachricht die Art der Verschlüsselung verändert werden – der Chat ist nicht an eine spezielle Verschlüsselungsart gebunden.

Eine Nachricht lässt sich mit der Return Taste versenden. User A verschlüsselt das individuell eingegebene symmetrische Geheimnis ***S*** mit dem öffentlichen asymmetrischen Schlüssel von User B automatisch und verschlüsselt die eingegebene Textnachricht mit dem Geheimnis ***S.*** Beides wird in einem JSON Objekt verpackt, das zusätzlich folgende Infos beinhaltet:

* ID des Absenders
* ID des Empfängers
* Welches asymmetrische Verfahren benutzt wird
* Welches symmetrische Verfahren benutzt wird

User B bekommt die Nachrichten vom Server, und entschlüsselt zuerst das Geheimnis ***S*** mit seinem privaten Schlüssel und anschließend die chiffrierte Textnachricht mithilfe des Geheimnisses ***S.***

*Nice to have:* Versand und Empfang von ver- bzw. entschlüsselten Bildern.

*Nice to have:* Außerdem soll ein Lernmodus vorhanden sein, mit welchem gezielt kryptografische Algorithmen geübt werden können.