

Orsum occulendi

AES in Java | PKN

Lukas Bischof, Philipp Fehr

Inhaltsverzeichnis

[Einleitung 2](#_Toc481613811)

[Das Problem 2](#_Toc481613812)

[Planung 2](#_Toc481613813)

[Verwendete Lösung 3](#_Toc481613814)

[Einleitung 3](#_Toc481613815)

[Funktionsweise AES 4](#_Toc481613816)

[Reflexion 6](#_Toc481613817)

# Einleitung

Philipp Fehr und Lukas Bischof haben in dem Projekt „Orsum Occulendi“ versucht,  
den AES-Algorithmus in Java umzusetzen. Damit die Kommunikation in unserem bereits vorhandenen Java Vier-Gewinnt verschlüsselt werden kann.  
Während der Entwicklung wurde das Projekt zusätzlich von Herrn Tromsdorff  
und Herrn Veselcic betreut.

# Das Problem

Das zentrale Problem des Projekt ist, dass die Verschlüsselung unseres Java Vier-Gewinnt Spieles nicht verschlüsselt übertragen wird und somit eine erhebliche Sicherheitslücke aufweist, da man mit einer Man-In-The-Middle Attacke die Spiele verändern sowie die Spieler getäuscht werden können.

# Planung

Zuerst haben wir uns einen groben Überblick über die Funktionsweise von AES verschafft. Dabei hat uns eine Aufnahme von einer Präsentation von Christof Paar sehr geholfen. Während der Umsetzung untersuchten wir dann jeder einzelne Schritt und setzten diesen dann um, sobald wir die Mechanik verstanden hatten.

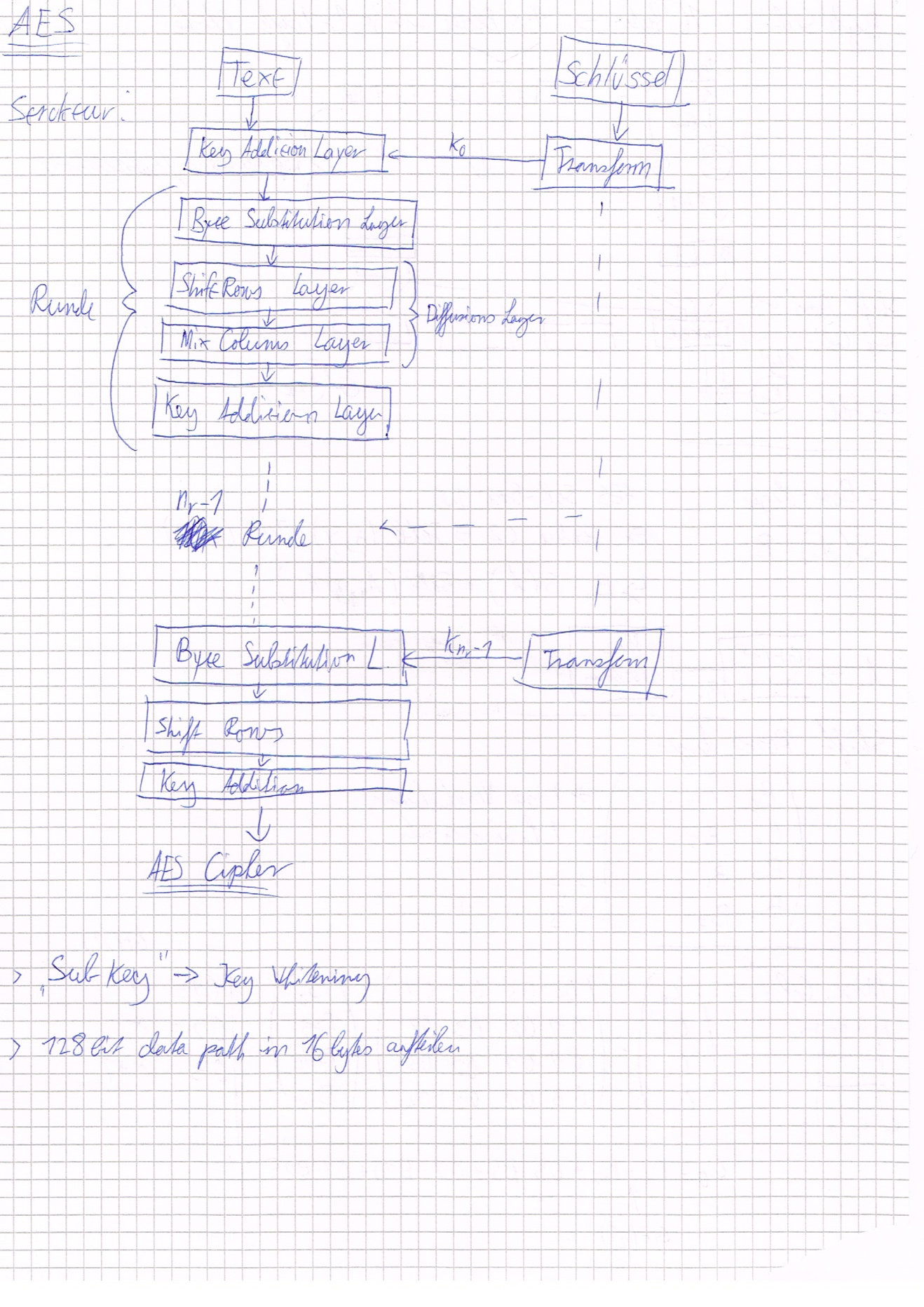
Als wir dann mit dem Algorithmus fertig waren, implementierten wir diesen in unser Server/Client Modell des Spiels.

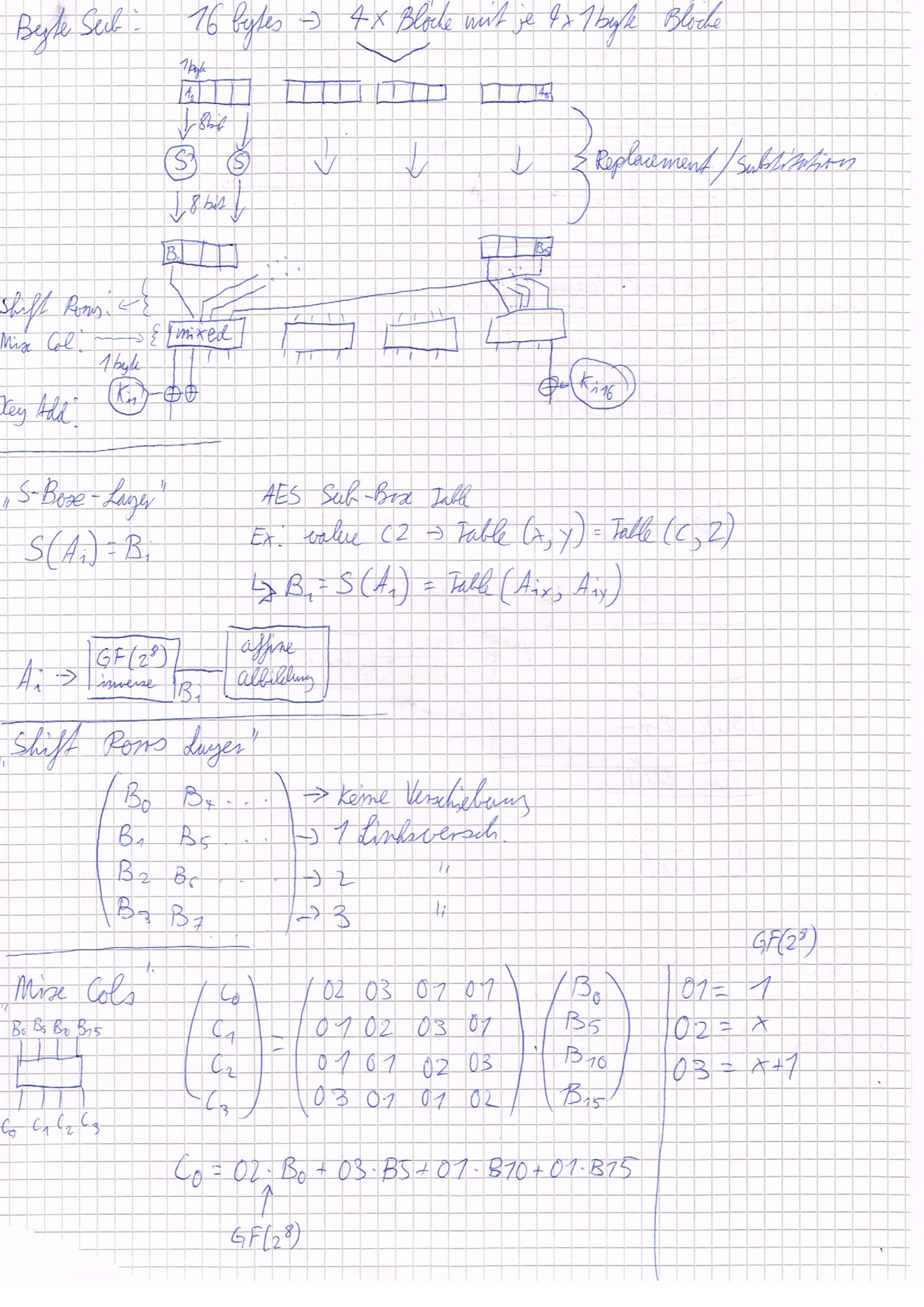
# Verwendete Lösung

## Einleitung

Da eine fertige AES-Library zu verwenden langweilig wäre und keine Herausforderung bieten würden, haben wir uns dazu entschieden AES selber zu umzusetzen. Um zudem vollumfänglich eine sichere Kommunikation zu ermöglichen haben wir unser Krypto System mit den eingebauten Java-Libraries mit einem RSA Schlüsselaustausch erweitert.

## Funktionsweise AES





# Reflexion

Nachwort Philipp

Ich

Nachwort Lukas

In dem Projekt haben wir den Algorithmus sehr gut und koordiniert umgesetzt. Jedoch schlichen sich manchmal dumme Fehler ein, welche wir teilweise über eine Woche lang suchten und uns nach dem Finden dann dementsprechend über die Banalität aufregten.

Ich finde trotzdem, dass dies ein gelungenes Projekt ist, welches restlos nach unseren Wünschen funktioniert.