



JAVA STARS 2005 - Sun Microsystems Award

Projekttitlel:

***Moderne Verschlüsselungstechniken
am Beispiel RSA***

Übersicht

Teamnummer	180
------------	-----

Schulnummer	169092
-------------	--------

Schulname	Evangelisch Stiftisches Gymnasium Gütersloh
-----------	---

Schulform	Gymnasium
-----------	-----------

Name des Teams	Schlüsselbund
----------------	---------------

Projektname	Moderne Verschlüsselungstechniken am Beispiel RSA
-------------	---

Projektkurzbeschreibung (max. 4 Zeilen)	
--	--

Unterrichtsfach	Informatik
-----------------	------------

Gruppengröße	4
--------------	---

Altersgruppe	18
--------------	----

Inhaltsverzeichnis

1	PROJEKTBECHREIBUNG	4
1.1	PROJEKTBECHREIBUNG.....	4
1.2	PROJEKTIDEE	4
1.3	THEMA.....	4
1.4	UNTERRICHTSFACH.....	4
1.5	NUTZEN FÜR DEN UNTERRICHT	4
1.6	PROBELÄUFE	4
1.7	INSTALLATION / START DES PROGRAMMS.....	5

1 *Projektbeschreibung*

1.1 *Projektbeschreibung*

Das Programm soll eine Einführung in die Public-Key beziehungsweise in die RSA-Verschlüsselung bieten. Mit dem Programm ist es möglich sich die Grundlagen zu erarbeiten.

Das Programm kann Schlüssel generieren und auch Texte mithilfe dieser codieren und decodieren. Veranschaulicht wird dies mithilfe mehrerer Oberflächen die zwei Benutzer, Alice und Bob, simulieren. Mit Hilfe dieser ist es möglich einen Nachrichtenaustausch zu simulieren. Inbegriffen ist hier das Codieren und Decodieren von Nachrichten.

Auf weiteren Oberflächen werden einerseits Hintergrundinformationen geboten und mithilfe einer grafischen Umsetzung des „Kartentricks“ die Funktionsweise des Public-Key Verfahrens näher gebracht.

Andererseits werden auf einer Oberfläche die einzelnen Schritte einer Codierung vorgestellt.

1.2 *Projektidee*

Wir waren daran interessiert uns näher mit modernen Verschlüsselungsmethoden zu beschäftigen. So sind wir auf die RSA-Verschlüsselung gestoßen.

1.3 *Thema*

Moderne Verschlüsselungsmethoden → RSA- Verschlüsselung

1.4 *Unterrichtsfach*

Informatik

1.5 *Nutzen für den Unterricht*

Das Programm stellt die sehr komplexe RSA-Verschlüsselung auf eine anschauliche Weise dar. Wird dieses Thema im Informatik Unterricht behandelt so kann dieses Programm einerseits unterstützend eingesetzt werden, aber auch als Grundlage dienen.

1.6 *Probeläufe*

Buttons in folgender Reihenfolge

Start (um das Programm nach dem Ladevorgang zu starten),

Einführung, Texte, vor, vor...., Kartentrick, vor, neue schlüssel und buttons folgen

Hauptprogramm:

Variante 1. links, oben auf bearbeiten, „Schlüssel schnell erzeugen“

Variante 2. links, oben auf bearbeiten, in das textfeld z Bsp. 6, primzahlen, zwischenwerte, schlüssel, übernehmen

→

Rechts unten bearbeiten, Text in das Textfeld eingeben, public key von alice auswählen, anwenden, senden, links unten auf bearbeiten, empfangen, private key von alice, anwenden,

Erweitert, neue schlüssel, Text in das Textfeld links oben, und den Pfeilen folgen

1.7 *Installation / Start des Programms*

(Ggf. RSA.zip in einen Ordner nach Wahl entpacken und anschließend in diesen Ordner wechseln)

Den Ordner RSA – Projekt öffnen und von dort die RSA.bat Datei ausführen.