AI4-ITSP	Praktikum IT-Sicherheit	Wst
WS10/11	Aufgabe 2 – Diffie-Hellman	16.11.2010 - 17.11.2010

2.1 Diffie-Hellman Demo

Machen Sie sich mit der Diffie-Hellman Demo des CrypTools vertraut.
Speichern Sie für fünf ausgewählte Kombinationen von Primzahlen, Generatoren und Geheimnissen von Alice und Bob die entsprechenden Log-Texte.
(Anmerkung: Die Log-Texte werden jeweils in ein Fenster des CrypTool Hauptprogrammes geschrieben.)

2.2 Diffie-Hellman Schlüsselerzeugung

Implementieren Sie den Diffie-Hellman Schlüsselaustausch.

2.3 Beschleunigung des Schlüsselaustausches

Beschleunigen Sie den DH-Schlüsselaustausch indem Sie die schnelle Exponentiation *Square-and-Multiply* für modulare Exponentiation implementieren und einsetzen.

2.4 Test mittels CrypTool

Testen Sie Ihre Implementierung indem Sie die unter 2.1 mit dem CrypTool erzeugten Log-Texte als Eingaben für ihre Implementierung nutzen.

Viel Spass und Erfolg bei der Ausarbeitung!