PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *17.06.2024*

43.) Rechnen sie ein konkretes Zahlen-Bsp. für das vereinfachte Feige-Fiat-Schamir Protokoll durch (alle Fälle für b) und betrachten sie in diesem Beispiel auch wie der Fall b=1 korrekt gelöst werden kann, obwohl der private Key nicht bekannt ist (durch den beschriebenen Betrug im Setup des Verfahrens).

44.) Implementieren sie OTP Verschlüsselung mit dem Blum-Blum-Shub Generator (wie beschrieben) und vergleichen sie die Ausführungsgeschwindigkeit mit einer OTP Verschlüssleung durch AES-CFB und einer OTP Verschlüssleung durch einen nativen Stream-cipher aus dem eStream Portfolio.

45.) Was muss ein Angreifer tun um den Blum-Blum-Shub Generator zu "brechen" und was ist überhaupt das Ziel eines solchen Angriffs ? Was macht diesen Angriff schwierig ?

46.) Warum muss beim Diffie-Hellman Key-Exchange neben n auch $\frac{n-1}{2}$ eine Primzahl sein (und beweisen sie ihre Erklärung) ?

VIEL ERFOLG !!