PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *19.05.2025*
***Abgabe**: bis SO 18.05. 17:00 an uhl@cs.sbg.ac.at*

27.) Zur Known-Plaintext Attacke gegen 2 Key EDE TripleDES (Slide 138f): Erklären/beweisen sie die angegebene Angriffskomplexität / Laufzeit der Oorschot, Wiener Attacke und die Anzahl der im Mittel notwendigen Versuche für a. Hinweis: sehen sie sich die Originalarbeit dazu an.

28.) Erklären sie warum die Berechnung von Diskrete Logarithmen und Quadratwurzeln in Modulararithmetik "computationally infeasible" ist, während in klassischer Arithmetik die entsprechenden Berechnungen nicht besonders aufwändig sind.

29.) Erklären sie (und rechnen sie ein konkretes Beispiel durch), wie modulare Inversion mit dem erweiterten Euklidischen Algorithmus realisiert werden kann.

30.) Beweisen sie: Ist $n = p \cdot g$ mit p und g Primzahlen: $\phi(n) = (p-1)(g-1)$.

VIEL ERFOLG !!