**SMS1 für MC, FHS Hagenberg**
**12. Übungsblatt für den 13. Jänner 2005**

**Schlüsselaustausch nach Diffie-Hellman**

1. Alice und Bob wollen sich mit dem Verfahren von Diffie-Hellman auf einen gemeinsamen Schlüssel einigen. Es gelingt Ihnen, den Datenaustausch zwischen den beiden zu kontrollieren. So erfahren Sie die Primzahl $p = 1728439$ und den Generator $\alpha = 27318$ von $\mathbb{Z}_p^*$, die verwendet werden.

   Sie fangen weiters den von Alice für Bob bestimmten Schlüssel $a = 1709421$, sowie den von Bob für Alice bestimmten Schlüssel $b = 1109585$ ab. Was sollen Sie an Alice bzw. Bob schicken, um deren Nachrichten in Zukunft entschlüsseln zu können?

2. Erklären Sie die wesentlichen Elemente des DES-Algorithmus zur symmetrischen Verschlüsselung [1, 7.4.2].

3. Verschlüsseln Sie die Nachricht "Heute ist der 13.1.2005." mit DES (ECB) und dem Schlüssel $k$ = 0123456789ABCDEF (in Hexadezimaldarstellung). Entschlüsseln Sie das Ergebnis dann wieder.

   Sie können dazu etwa das freie Paket "CrypTool" (`www.cryptool.de`) verwenden. Dort finden Sie DES unter dem Menüpunkt "Ver-/Entschlüsseln (Symmetrisch)". Schreiben Sie die Nachricht in eine Datei, die Sie verschlüsseln, und speichern Sie die verschlüsselte Datei.

4. Sie wollen mit Bob einen 64-Bit DES-Schlüssel $k$ mit Hilfe des STS-Protokolls austauschen. Sie einigen sich auf eine Primzahl
   $p = 15678100593495627901$ und einen Generator $\alpha = 827469137953256477$.

   (a) Im ersten Schritt schicken Sie $a := \alpha^x \mod p$ für $x = 123456789$ an Bob.

   (b) Als Antwort erhalten Sie $b = 13607259366636426793$ und die verschlüsselte Unterschrift $s$ in der Datei `Cry-DES-des124.hex` (Diese Datei wurde mit CrypTool erstellt).
   Hier soll $s = E_k(S_B(a||b)$ sein, wobei $E_k$ die DES (ECB) -Verschlüsselungsfunktion mit Schlüssel $k$ ist und $S_B$ Bob's RSA-Unterschriftenfunktion mit öffentlichem Schlüssel
   $(n, e) = (191844739581225802488175399033906186045 63, 65)$ ist.
   Unter $a||b$ verstehen wir die Konkatenation von $a$ und $b$.

   (c) Bestimmen Sie $k$ und überprüfen Sie, ob die Nachricht von Bob stammt.

5. Fortsetzung von Bsp. 4: Bestimmen Sie $E_k(S_A(a||b))$ mit Ihrer eigenen RSA-Unterschriftenfunktion $S_A$ mit
   $n = 127968138520478321223959438672931493911 61$ und $d = 257$.

# Literatur


[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.