Kryptosysteme, Keymanagment (KSK3) für CMS
10. Übungsblatt für den 19. Dezember 2006

36. Alice signiert einen Kaufvertrag m, der den Hashwert $h(m) = 54985$ hat, mit ihrem öffentlichen ElGamal-Schlüssel

$$(p, g, A) = (1052813, 2, 708855)$$

und erhält die digitale Signatur

$$(r, s) = (909582, 434075).$$

Verifiziere Alice's Signatur.

37. (*Fortsetzung von Bsp. 36*) Fälsche eine Signatur von Alice für eine Nachricht m' mit Hashwert $h(m') = 13420$, der vertraut wird, wenn man die Bedingung $1 \leq r \leq p-1$ nicht überprüft. (Der öffentliche Schlüssel, die Nachricht und die Signatur von Alice aus Beispiel 36 dürfen verwendet werden, nicht aber der geheime Schlüssel a und der geheime Parameter k.) Überprüfe die gefälschte Signatur.

38. (*Fortsetzung von Bsp. 36*) Alice signiert einen weiteren Kaufvertrag m_2, der den Hashwert $h(m_2) = 824799$ hat, und erhält die Signatur

$$(r_2, s_2) = (909582, 547161).$$

Sie hat den gleichen Parameter k verwendet, wie im Beispiel 36. Berechne zuerst k und anschließend Alice's geheimen Schlüssel a.

39. Warum verwenden digitale Signaturschemata mit Message Recovery (wie zB RSA mit Message Recovery) eine Redundanzfunktion? Welche Attacken können dadurch verhindert werden?