TU Ilmenau
Institut für Mathematik, Diskrete Mathematik
Prof. Michael Stiebitz/Dr. Axel Wolf

Sommersemester 2019

Aufgaben zur Prüfung Kryptographie

Aufgabe 1

bggbf zbcf gebgmg bggb: sbeg zbcf sbeg bggbf zbcf ubcfg sbeg bggb: fbfb bggb ubyg xbxf bggb ubyg bofg bggb ubepug bggb: zbcf zbcf bggb ubssg bggbf zbcf xybcsg bggb: xbzz zbcf xbzz bggbf zbcf xbzzg bggbf zbcf xbgmg bggb: btbggbtbgg

Entschlüsseln Sie den Text. Er wurde mit Caesar verschlsselt. Bestimmen Sie die Entropie.

Aufgabe 2

rla pbsfnsf mzwluh cca zdwansu ycwt rlf vbh wu ozssb sismhsu voszh lg kps ulgqofsp rojvrlqylf gaisynsu op bbr nsvu sbanklw iur ou rsu yilghlb zpsga aou ghlwua rwl tzbh. rlf gaift wga ro, kws dwzksb tssys vbdtlb ou zour, it rwjys kostas gi nlfryisjysu rwl aspghlb albgjvsu voisb lwblb gjvbbdtlb rps spgsupoobsu toszsu jcu rsu pfbsqrsb.

Entschlüsseln Sie den Text. Er wurde mit Vigenere verschlüsselt. Bestimmen Sie die Entropie.

Aufgabe 3

Wir betrachten folgendes Chiffriersystem $(\mathcal{K}, \mathcal{G}, \mathcal{S}, k, d)$ mit $\mathcal{K} = \{0, 1\}$, $\mathcal{G} = \{a, b\}$, $\mathcal{S} = \{s, t\}$, sowie

$$k_s(0) = a, k_s(1) = b. k_t(0) = b, k_t(1) = a.$$

Die Wahrscheinlichkeiten für das Auftreten von $T \in \mathcal{K}$ seien $p_{\mathcal{K}}(0) = 1/4$ und $p_{\mathcal{K}}(1) = 3/4$. Die Schlüssel treten mit folgenden Wahrscheinlichkeiten auf $p_{\mathcal{S}}(s) = 1/4$ und $p_{\mathcal{S}}(t) = 3/4$. Untersuchen Sie die Sicherheit des Systems. Ist das Chiffriersystem perfekt sicher?

Aufgabe 4 Miller–Rabin Test

Mit Hilfe des Fermat-Tests kann nicht festgestellt werden, dass $n = 561$ zusammengesetzt ist. Zeigen Sie mit Hilfe des Miller-Rabin Testes, dass $a = 2$ eine Zeuge gegen die Primalitt von n ist.

Aufgabe 5 RSA Verfahren

Betrachten RSA(n, p, q, k, g) für Alice, wobei $n = 35237$ ist und k minimal ist.

(a) Geben Sie k an und den zugehörigen geheimen Schlüssel g. Erläutern Sie, wie man mit Hilfe des erweiterten Euklidischen Algorithmus den Wert g bestimmen kann.

(b) Alice hat den Geheimtext $T = 11111$ erhalten. Wielautet der zugehörige Klartext T?

(b) Bob hat von Alice die Signatur (ohne Hashfunktion) $s = 12345$ erhalten. Geben Sie das zugehörige Dokument m an.

Aufgabe 6 Common Modulus Attack

Alice benutzt RSA(n, p, q, k, g) und Bob benutzt RSA(n, p, q, ℓ, f). An beiden soll der Klartext m versendet werden. Somit erhält Alice den Geheimtext $c_A = m^k$ Mod n und Bob erhält den Geheimtext $c_B = m^\ell$ Mod n. Ist nun ggT(k, ℓ)=1, so kann man aus den Geheimtexten c_A und c_B den Klartext m bestimmen, ohne die geheimen Schlüssel zu kennen. Wie geht das.

Anmerkung Wenn Sie Rechnungen mit Maple oder ähnlichen Programmen durchführen, so bringen Sie die Maple sheets mit.

Aufgabe 7 EIGamal Verfahren

Der öffentliche EIGamal Schlüssel von Alice ist $p = 53$, $g = 2$ und $A = 30$. Bob erzeugt damit den Schlüsseltext $(24, 37)$. Wie lautet der Klartext.