

Kryptographie Probeklausur WS 2006_07

Aufgabe 1:

- 1) Ist die Gleichung $46x \equiv 77 \pmod{122}$ lösbar? Wenn ja, geben Sie eine Lösung an.
- 2) Ist die Gleichung $46x \equiv 2 \pmod{122}$ lösbar? Wenn ja, geben Sie eine Lösung an.

Aufgabe 2:

Beweisen Sie folgende Aussagen:

- 1) Für alle $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt:
$$a \cdot b \pmod{n} = (a \pmod{n})(b \pmod{n}) \pmod{n}$$
- 2) Zu jeder multiplikativen Chiffre gibt es eine multiplikative Dechiffrierfunktion.

Aufgabe 3:

- 1) KLAUSUR wird per Tauschchiffre auf RIDFXFG abgebildet. Bestimmen Sie die Abbildungsvorschrift für die Tauschchiffre.
- 2) Verschiebechiffre: Entschlüsseln sie folgenden Satz:
SNRPUYR VUE QRA XBCS ONG QVR JRVFFR XBRAVTVA NRATFGYVPU
FVR QRAXG MHIVRY QNIBA XEVRTG ZNA SVRORE

Aufgabe 4:

Vigenère Chiffre: Chiffretext C

- 1) a) Welche Informationen ermitteln Sie aus C mit dem Kasiskitest?
b) Geben Sie die Definition des Koinzidenzindex für den Text C an.
c) Berechnen Sie den Koinzidenzindex für C, der aus gleichen Buchstaben besteht.
d) Koinzidenzindex berechnen für zufälligen Text C, in dem die Häufigkeit aller Buchstaben in etwa gleich ist.
- 2) Definition einer linearen Funktion angeben, die als Ein- und Ausgabe Folgen von Bits hat.
Ist f mit $f(x_1 x_2 \dots x_{n-1} x_n) = x_n x_2 \dots x_{n-1} x_1$ eine lineare Funktion?

Aufgabe 5:

- 1) Der öffentliche El-Gamal Schlüssel von Bob ist $p=29$, $g=2$, $A=7$. Sie haben herausgefunden, dass sein privater Schlüssel $a=12$ ist. Bob erhält die Nachricht (2,2). Wie lautet der Klartext?
- 2) Der private Rabin-Schlüssel von Klara sind die Primzahlen $p=11$ und $q=19$. Geben Sie alle möglichen Klartexte für die Nachricht $c=4$ an. Überprüfen Sie die Richtigkeit der Lösungen, indem Sie die erhaltenen Lösungen wieder chiffrieren.

Aufgabe 6:

- 1) Der öffentliche RSA-Schlüssel von Alice ist $n=55$, $e=3$.
 - a) Warum ist $e=3$ ein zulässiger Exponent?
 - b) Alice erhält die Nachricht 2. Wie lautet der Klartext?
 - c) Wie lautet die digitale Signatur von Alice unter einem Dokument mit dem Hashwert $h=11$?

- 2) Bob hat im ElGamal Signaturverfahren den öffentlichen Schlüssel $(p_B=53, g_B=3, A_B=7)$ und Alice $(p_A=29, g_A=2, A_A=7)$. Vor Ihnen liegt der Vertrag $(\text{text}, 21, 28)$. Wer von beiden hat ihn unterschrieben, wenn $h(\text{text})=13$ gilt?