I. Bouw
F. Kiraly

20.05.2008
SS 2008

Übungen zur elementaren Zahlentheorie - Blatt 5

Abgabe bis 29.05.2008 um 10:00

Aufgabe 17: Affine Chiffren (2+2+2+2 = 8 P)

In der Vorlesung wurde die Klasse der affinen Chiffren vorgestellt. Dazu wird ein Alphabet mit $n \in \mathbb{N}$ Buchstaben in der kanonischen Reihenfolge mit den kanonischen Restklassen modulo n identifiziert. Buchstabenweise wird dann für festes $a, b \in \mathbb{Z}/n\mathbb{Z}$ die Abbildung

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} : x \mapsto ax + b$$

auf den Klartext angewendet.

(a) Für welche Wahl von a und b existiert die Umkehrabbildung? Betrachten sie als Beispiel den Fall $a = 13$ im lateinischen Alphabet der Großbuchstaben ($n = 26$).

(b) Geben Sie im Falle der Existenz die Umkehrabbildung explizit an (es reicht dazu zu sagen, wie man sie berechnet).

(c) Zeigen Sie, dass die Hintereinanderausführung zweier affiner Chiffren wieder eine affine Chiffre ist.

(d) Nehmen wir an, die zwei häufigsten Buchstaben in unserem Alphabet werden mit den Restklassen x und y identifiziert. Ferner werden diese Buchstaben durch die Verschlüsselungsabbildung auf $\tilde{x}$ und $\tilde{y}$ abgebildet. Berechnen Sie explizit Verschlüsselungs- und Entschlüsselungsabbildung.

Aufgabe 18: Weitere lineare Verschlüsselungsverfahren (LA: 2+2 = 4 P; IST: 0+0=0 P)

Eine monoalphabetische Substitutionschiffre oder kurz monoalphabetische Chiffre ist eine Chiffre, die durch eine buchstabenweise Bijektion auf einem endlichen Alphabet $\aleph$ modelliert werden kann. Eine polygraphische Chiffre (vom Grade k) ist eine Chiffre, die durch eine Bijektion auf $\aleph^k$ modelliert werden kann. Beispielsweise ist die Caesar-Chiffre monolaphabetisch und die RSA-Chiffre polygraphisch.
Eine Verallgemeinerung der affinen Chiffren sind die sogenannten Hill-Chiffren. Ist $\aleph \cong \mathbb{Z}/n\mathbb{Z}$ das Alphabet (d.h. wir fixieren uns eine konkrete Zuordnung von A zu den kanonischen Restklassen), so betrachte die Abbildung

$$\aleph^m \to \aleph^m : x \mapsto Ax + b.$$

Diese Abbildung ist linear, dabei ist $A \in \mathrm{GL}_m(\aleph)$ eine $m \times m$ -Matrix. Die Arithmetik ist vollkommen analog zu $\mathrm{GL}_m(\mathbb{Z})$ mit dem einzigen Unterschied, dass bei der Multiplikation modulo n gerechnet werden muss. Die dadurch definierte Chiffre nennen wir eine Hill-Chiffre vom Grad m , falls sie eine polygraphische Chiffre ist.

(a) Zeigen Sie: Die Hintereinanderausführung von zwei Hill-Chiffren gleichen Grades ist wieder eine Hill-Chiffre vom selben Grad.

(b) Zeigen Sie: Die obige Zuordnung definiert genau dann eine polygraphische Chiffre (d.h. die Umkehrabbildung existiert), wenn $\mathrm{ggT}(\det A, n) = 1$.

Aufgabe 19: Angewandte Kryptographie I: affine Chiffren (LA: 0+0+3=3P; IST: 2+2+3=7P)

Sämtliche Teilaufgaben beziehen sich auf das lateinische Großbuchstabenalphabet (26 Buchstaben).

(a) Verschlüsseln Sie die Nachricht DIESES BLATT IST KINDERLEICHT mit der affinen Chiffre von Signatur (7,20). Die Signatur ist dabei wie im Skript definiert (d.h. (Faktor, Shift)).

(b) Die Nachricht ZQSYSYNVURRQYRCQHZSFVSQGXR wurde mit der Chiffre (19,12) verschlüsselt. Entschlüsseln Sie sie.

(c) Die folgende Nachricht wurde mit einem unbekannten affinen Schlüssel verschlüsselt. Führen Sie einen Buchstabenhäufigkeits-Angriff auf sie durch. D.h., finden Sie an Hand der Häufigkeitsverteilung der Buchstaben in der deutschen Sprache die ursprüngliche Nachricht heraus. Dokumentieren Sie dabei Ihre Schritte auf dem Übungsblatt. Der Klartext ist in deutscher Sprache geschrieben, Umlaute und ß sind durch die entsprechende Großschreibweise (AE, SS etc) ersetzt worden. Sie finden die Nachricht zum Herumspielen auch als ASCII-Datei auf der Homepage der Vorlesung.

Glh Edoodgh yrp duphq Hsvlorq
Kxehuw Fuhphu
Glh Pdwula vdqj lku Vfkoxpphuolhg ghq Chlohq xqg Nrorqqhq, vfkrq kdhow gdv nohlqh Ihkohujolhg hlq vxhvvhu Wudxp xpvsrqqhq, hv vfkqdufkw glh dowh S-Ixqnwlrq, xqg hlqvdp zhlqw hlq eohlfkhv, mxqjhv, yhuodvvqhv Hsvlorq dp Udqg ghv Vwhuqehuhlfkhv. Gx jxwhu Ydwhu Zhlhuvwudß, Gx Vfkrhsihu xqvuhu Zhow gd, lfk iohk Glfk hlqclj dq xp gdv: Kloi ilqghq plu hlq Ghowd! Xqg zhqqv dxfk qrfk vr zlqclj zdhu xqg ehlqdk Qxoo dp Hqgh, gdv noduvwh Vhlq eolhe rhg xqg ohhu, zhqq vlfk nhlq Ghowd idhqgh. Yhujhehqv vfkoxfkcw glh duph Cdko xqg uxiw qdfk lkuhp Uhwwhu, hv udxvfkw vr wurvworv xqg wulyldo gxufk zhonh Ulhpdqq-Eodhwwhu; glh Vwuhqjh kdw qlfkw Khuc qrfk Rku iüu Olhehvohlgjhixhkoh, gdv duph Hsvlorq huiuru lp hlvljhq Ndonxhoh. Prudo: Xqvwhwlj lvw glh Zhowixqnwlrq, lku zhughwv qlh hujuxhqghq, cx pdqfkhp eudyhq Hsvlorq odhvvw vlfk nhlq Ghowd ilqghq
Vlhkh dxfk: Vshnwuxp Ohalnrq ghu Pdwkhpdwln cxp Vwlfkzruw Kxpru lq ghu Pdwkhpdwln

Aufgabe 20: Angewandte Kryptographie II: RSA (1+2+2 = 5 P)

(a) Bestimmen Sie die Primfaktoren von $n = 1799816309274563$ ohne Probieren. Benutzen Sie dazu $\varphi(n) = 1799816224426080$.

(b) Verschlüsseln Sie die Nachricht BEZOAR mit dem Schlüssel (13, 2747) im RSA-System. Ersetzen Sie dazu zunächst die Buchstaben durch Zahlen auf die in der Vorlesung beschriebene Weise.

(c) Die Nachricht BZQCN! wurde mit dem Schlüssel (31,2747) RSA-verschlüsselt. Entschlüsseln Sie sie. Das Zeichen ! hat dabei die Nummer 85.