Programmierpraktikum Informatik - Thema Kryptographie

Gruppe Kryptographie

Affin lineare Blockchiffren

Verschlüsselungsfunktionen affin linearer Blockchiffren der Länge n sind folgendermaßen definiert:

$$E : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, \quad v \mapsto Av + b \bmod m,$$

mit $A \in \mathbb{Z}_m^{(n,n)}$ und $v, b \in \mathbb{Z}_m^n$. Dabei muß $\det A$ teilerfremd zu m sein, damit E bijektiv ist. Der Schlüssel besteht also aus dem Paar (A, b). Die zugehörige Entschlüsselungsfunktion ist

$$D : \mathbb{Z}_m^n \to \mathbb{Z}_m^n, \quad v \mapsto A'(v - b) \bmod m,$$

mit $A' = (a' \text{ adj } A) \bmod m$. Dabei ist a' das Inverse von $\det A \bmod m$, und adj A die *Adjunkte* von A. Sie ist definiert als

$$\text{adj } A = ((-1)^{i+j} \det A_{j,i}).$$

Beispiele

1. **Caesar- oder Verschiebungschiffre**
   $n = 1$, $A = (1)$, Schlüssel ist $b \in \mathbb{Z}_m$.

   $$E(v) = v + b \bmod m, \quad v, b \in \mathbb{Z}_m.$$

2. **Vigenère-Chiffre**
   A ist die Einheitsmatrix, Schlüssel ist $b \in \mathbb{Z}_m^n$.

   $$E(v) = v + b \bmod m, \quad v, b \in \mathbb{Z}_m^n.$$

3. **Hill-Chiffre**
   b ist der Nullvektor, Schlüssel ist $A \in \mathbb{Z}_m^{(n,n)}$.

   $$E(v) = Av \bmod m, \quad v \in \mathbb{Z}_m^n, A \in \mathbb{Z}_m^{(n,n)}.$$

4. **Permutationschiffre (Spezialfall Hill-Chiffre)**
   Analog zur Hill-Chiffre ist

   $$E(v) = Av \bmod m, \quad v \in \mathbb{Z}_m^n, A \in \mathbb{Z}_m^{(n,n)}.$$

   Dabei sind nur Matrizen A zugelassen, die aus der Einheitsmatrix $E \in \mathbb{Z}^{(n,n)}$ entstehen, indem man eine beliebige Anzahl von Spalten vertauscht. D.h. für jede Permutation $\pi \in \mathcal{S}_n$ definiere eine Matrix $A = E_\pi$, bei der in der j-ten Spalte der Einheitsvektor $e_{\pi(j)}$ steht.

Aufgaben:

1. Wieviele verschiedene Schlüssel gibt es zu den vier vorgestellten affin linearen Verschlüsselungsverfahren?

2. Implementiere die vier affin linearen Verfahren in jeweils einer Klasse, die von der Klasse "Kryptosystem" abgeleitet ist.
   Hinweis: Um das Entschlüsselungspaar (A', b) zu erhalten, muß man zwei mathematische Methoden implementieren. Die erste Methode rechnet Determinanten zu gegebenen Matrizen aus, die zweite soll Inverse für beliebige Zahlen über Restklassenringen bestimmen.

3. Man überlege sich, wie man das bisher festgelegte Modell für die Darstellung der kryptographischen Protokolle verbessern könnte.

4. Jemand aus der Gruppe sollte sich in das DES-Verfahren (Kapitel 6 im Buchmann) einarbeiten. Im nächsten oder übernächsten Treffen sollte der- oder diejenige den Algorithmus kompakt für die anderen präsentieren.
   Was muß man eventuell an der Basisklasse "Kryptosystem" ändern, um die DES-Verschlüsselung zu implementieren?

Die Aufgaben werden am 20. November um 9.30 Uhr im Rechnerraum 25.12-02.37 besprochen.