Übungsaufgaben zur Vorlesung Kryptographie, Prof. Dr. N. Martini

Hinweise zur Klausur: Hier sind einige Rechenaufgaben aufgeführt, die in dieser oder ähnlicher Form in der Klausur gestellt werden könnten. Hinzu kommen Verständnisfragen (z.B. wie funktioniert DES, RC4, Triple-DES, AES, DH, RSA Operationsmodi, Hash-Funktionen usw.).
Hilfsmittel in der Klausur: eine DINA4-Seite, das selbstständig und handgeschrieben erstellt wurde (Sie können alles aufschreiben, was Sie selbst meinen zur Klausur brauchen zu können). Soll heißen: keine Kopien, kein z.B. per Textverarbeitung oder anderweitig am Computer hergestelltes Blatt. Ggf. notwendige Hilfen, wie z.B. Vigenere-Quadrat, Häufigkeitsverteilungen o.ä. werden bei der Klausur verteilt.
Ein einfacher Taschenrechner wird zur Klausur gestellt.

1. Einfache Substitution

Der folgende Chiffretext ist mit einer einfachen Substitutions-Chiffre erzeugt worden (Umlaute sind als Einzelbuchstaben geschrieben z.B. ä = ae):

ckd iblscdci hgckdci nckiakcg xzco tcoiblgciicgzdy

Wandeln Sie diesen Chiffretext in den Klartext zurück, wobei alle Schritte zu begründen sind (nur die bloße Angabe einer Lösung reicht nicht!)

2. Block-Permutation

Das folgende Chiffretext-Wort ist mit einer Block-Permutation erzeugt worden:

acsternhcnhercseahchexlt

Wandeln Sie diesen Chiffretext in den Klartext zurück, wobei alle Schritte zu begründen sind (nur die bloße Angabe einer Lösung reicht nicht!)

3. Vigenere-Chiffre

Der folgende Chiffretext ist mit einer Vigenere-Chiffre erzeugt worden (Umlaute sind als Einzelbuchstaben geschrieben z.B. ä = ae):

its wnmvlzfpswnmpfjwdjp pnkyjx dngs smnmx kzq lgwnmptjwdjr pnrpw xfjv

Lösungshinweise:

- Das häufigste Trigramm entspricht SCH
- im ersten Textblock ist das E nicht der häufigste Buchstabe, in den weiteren ist das E der häufigste Buchstabe
- Leerzeichen sind nicht mitverschlüsselt (d.h. zählen bzgl. der Blockgröße bzw. Schlüssellänge nicht mit) und sind nur der einfacheren Les- und Lösbarkeit eingefügt.
- allgemeine Hinweise: verwenden Sie nicht unnötig viel Zeit auf die Lösung dieser Aufgaben (die Beschreibung der geplanten Vorgehensweise ergibt bereits einen nicht unerheblichen Teil der Punkte)

4 Affine Chiffre (Tausch-Chiffre)

a) Warum muss bei einer affinen Chiffre ($c = (m \cdot t + k) \bmod n$) die Bedingung $ggt(t, n) = 1$ erfüllt sein?

b) Berechnen Sie den Chiffretext zum Klartext „KLAUSUR“, mit $n = 26$, $t = 9$, $k = 4$, und A=0, B=1,..., Z=25

c) Berechnen Sie die Dechiffrier-Funktion ($m = ((c - k) \cdot b) \bmod n$), wobei das Modulo-Inverse b zu $t = 9$ mittels des erweiterten euklidischen Algorithmus zu bestimmen ist (raten gilt nicht!)

5. RSA-Verfahren

a) Erklären Sie am Beispiel von RSA das Prinzip eines asymmetrischen Verschlüsselungs- bzw. Signaturverfahrens

b) Für das RSA-Verfahren seien die Primzahlen $p = 5$ und $q = 7$ sowie der öffentliche Schlüssel $e = 5$ gegeben; begründen Sie die Richtigkeit der Wahl von $e = 5$.

c) Berechnen Sie mit diesen Werten den privaten Schlüssel (raten gilt nicht und gibt auch keine Punkte!!) und erläutern Sie, warum der private Schlüssel nicht aus dem öffentlichen Schlüssel abgeleitet werden kann

d) Chiffrieren Sie die Klartextnachricht $m = 4$

e) Dechiffrieren Sie den sich daraus ergebenden Chiffretext

6. Primzahl-Faktorisierung
Zerlegen Sie die in den folgenden Aufgaben angegebenen Zahlen in ihre Primfaktoren

- Primzahl-Faktorisierung mit Probedivision
  a) 85
  b) 1760
  c) 5967
  d) 1000
- Fermat-Methode
  a) $n = 161$
  b) $n = 133$
  c) $n = 451$

7. Primzahl-Test
Testen Sie mithilfe des Miller-Rabin-Tests, ob die folgenden Zahlen mit 75% Wahrscheinlichkeit Primzahlen sind oder nicht:

a) 61

b) 101

8. ElGamal-Verschüsselung

a) Beschreiben Sie den Ablauf von ElGamal in der Variante als Verschlüsselungsverfahren

b) berechnen Sie ein Zahlenbeispiel mit Primzahl $p = 17$; wählen Sie beliebige – aber geeignete – Werte für den privaten Schlüssel, die Nachricht usw.