Übung 3

Abgabetermin: 10. November 2011 **vor** der Vorlesung

1. *Mehrfache Verschlüsselung*

   Eine beliebte Methode, um die Sicherheit von symmetrischen Algorithmen zu vergrößern, beruht auf der Idee, denselben Algorithmus mehrfach anzuwenden:

   $$y = e_{k2}(e_{k1}(x))$$

   Wir haben in der Übung bereits gesehen, dass die Mehrfachanwendung der Permutationschiffre keinen Sicherheitsgewinn bringt. In dieser Aufgabe werden wir zeigen, dass Doppel-Verschlüsselung von affinen Chiffren ebenfalls nicht sicherer ist als die einfache Verschlüsselung.

   Angenommen wir haben zwei affine Chiffren $e_{k1} = a_1x + b_1$ und $e_{k2} = a_2x + b_2$.

   (a) Zeigen Sie, dass es eine affine Chiffre $e_{k3} = a_3x + b_3$ gibt, die genau dieselbe Verschlüsselung (und Entschlüsselung) wie die Kombination $e_{k2}(e_{k1}(x))$ erzeugt. (10 Pkt.)

   (b) Bestimmen Sie a_3, b_3 mit $a_1 = 7, b_1 = 13$ and $a_2 = 18, b_2 = 9$ mit Modulus 23 (10 Pkt.)

   (c) Beschreiben Sie kurz was passiert, wenn Sie eine Brute-Force Attacke gegen die Zweifach-Verschlüsselung der affinen Chiffre anwenden. Hat sich der effektive Schlüsselraum vergrößert? Kennen Sie einen effektiveren Angriff auf die affine Chiffre, als einen Brute Force Angriff? (10 Pkt.)

   Bemerkung: Die Verwendung von Mehrfach-Verschlüsselung ist von großer praktischer Bedeutung. Bei DES erhöht sich z.B. die Sicherheit, wenn wir dieses mehrfach hintereinander anwenden — wir werden dieses Thema in ein paar Wochen in der Vorlesung behandeln.

2. *Affine Chiffre*

   Dechiffrieren Sie den folgenden Text:

   `fhhp://5v8.qtje/twjo_f9c8ni_whglhneotxegn`

   unter Benutzung der affinen Chiffre mit den Schlüsselwerten $a = 11$, $b = 6$ und dem Modulus 26. Hinweis: Ziffern und Satzzeichen wurde nicht verschlüsselt. (20 Pkt.)

3. *One-Time Pad Sicherheit*

   Auf den ersten Blick scheint es, als ob eine brute-force Attacke (vollständige Schlüsselsuche) gegen das One-time Pad möglich ist. Das ist ein Paradoxon, da wir wissen, dass das OTP uneingeschränkt sicher ist. Beschreiben Sie kurz (maximal **3 Sätze**), warum die brute-force Attacke nicht durchführbar ist.

   Anmerkung: Sie müssen das Paradoxon lösen, d.h. eine Antwort ”Der OTP ist uneingeschränkt sicher und deshalb ist eine brute force Attacke nicht durchführbar” ist nicht ausreichend!

4. *One-Time Pad Rechenaufgabe*

   Das One-Time Pad (OTP) wurde in der Vorlesung zur Verschlüsselung des binären Alphabets ($\Sigma \in \{0,1\}$) eingeführt. Hiermit können Daten von beliebiger Länge bitweise verschlüsselt werden.

   Entschlüsseln Sie den folgenden Ciphertext:
   `18 03 07 1e 04 4c 28 1d 0c 01 54 09 49 27 0a 53 17 06 1b 19 5a`
   welcher mit dem OTP Schlüssel:
   `48 6f 72 73 74 20 47 6f 65 72 74 7a 20 49 6e 73 74 69 74 75 74`
   verschlüsselt worden ist. Die Entschlüsselung ist von Hand durchzuführen (Klausurbedingungen). Verwenden Sie eine ASCII-Zeichensatz-Tabelle, um den Klartext und den Schlüssel wiederzugewinnen (Klausurbedingungen: von Hand). (15 Pkt.)

5. *One-time Pad Angriff bei sich wiederholendem Schlüssel*

   Sie haben bislang einige Verschlüsselungsübungen bereits per Hand erledigt. Im Übungsordner befindet sich eine verschlüsselte JPG Datei `boardingpass.jpg.hex`. Zudem wird das Programm "`CrypTool`"(aktuell 1.4.30) benötigt, welches Sie sich kostenlos herunterladen können. (Leider nur für MS Windows verfügbar. UNIX/Linux Benutzer mögen bitte Emulatoren benutzen, um das Programm zu nutzen. Alternativ stehen Arbeitsplätze in der CIP-Insel der Fakultät zur Verfügung.)

   Joe ist verschwunden. Sein letztes Lebenszeichen ist ein Online-Ticket auf seinem Rechner, welches leider verschlüsselt abgelegt wurde. Anhand des Dateinamens konnten erkennen, dass es sich bei dem Chifrat um eine JPG Datei handelt. In diesem Format übermittelt nur eine Airline ihre Tickets. Von dieser erfahren Sie, dass das Ticket zur Übertragung mit einem sich wiederholenden Schlüsselstring XOR verknüpft wurde. Dieser String ist allerdings bei jeder Übertragung zufällig und nicht mehr bekannt.

   (a) Öffnen sie willkürlich einige Dateien im JPG Format mit dem CrypTool, und schauen sie sich jeweils den Anfang der Datei an. Beschreiben Sie, was alle Dateien gemeinsam haben.

   (b) Der Schlüssel zur Verschlüsselung der o.g. Datei hat eine Länge von sechs Zeichen. Wie lautet er (HEX Darstellung)?

   (c) Nutzen Sie dieses Wissen um mit Hilfe des CrypTools die Datei zu dechiffrieren (entschl..symmetrisch..klassisch..XOR). Wohin ging Joes letzte bekannte Reise ? Wie lautet die Flugnr. ? Mit welcher Fluggesellschaft war er unterwegs?

   (15 Pkt.)

Historische Bemerkung: Es wird berichtet, dass das Ehepaar Rosenberg in den 50er Jahren eine solche Verschlüsselung verwendete, um der UDSSR Wissen über den Bau der Atombombe zukommen zu lassen. Da sie auf dem elektrischen Stuhl endeten, können wir die Mehrfachverwendung eines OTP Schlüssels nicht uneingeschränkt empfehlen.