Kryptologie: Übungsblatt 4, Besprechung ab dem 14.5.2018, 10:15, H20

40.) [Blum-Blum-Shub-Generator]
Man erzeuge Pseudozufallszahlen mit dem Blum-Blum-Shub-Generator

$$z_{i+1} \; = \; (z_i)^2 \bmod n$$

wobei $n = 23 \cdot 29$ und $z_0 = 2$. Wie lang ist die Periode, die sich ergibt?

41.) [Unabhängigkeit]
Die Zufallsvariable X kann die Werte x_1 und x_2 annehmen. Die Zufallsvariable Y kann die Werte y_1, y_2, y_3 annehmen. Diese Werte(-Kombinationen) treten mit folgenden Wahrscheinlichkeiten auf:

	x_1	x_2
y_1	$1/6$	$1/3$
y_2	$1/8$	$1/4$
y_3	$1/24$	$1/12$

Sind die Zufallsvariablen X und Y unabhängig?

42.) [Entropiewerte]
Gegeben ist folgende Wahrscheinlichkeitsverteilung der Zufallsvariablen X und Y:

	x_1	x_2
y_1	$1/4$	$1/4$
y_2	$1/4$	0
y_3	$1/4$	0

Man bestimme $H(X,Y), H(X), H(Y), H(X|Y), H(Y|X), I(X,Y)$.

43.) [Unsicheres 3-Phasen-Protokoll]
Beim Shamir'schen No Key (oder auch: 3-Phasen) Protokoll ist die intuitive Vorstellung die, dass A seine Nachricht m in eine Box einschließt, die er mit seinem Schlüssel abschließt. Diese Box wird an B gesandt. Dieser hängt ein weiteres Schloss (für das B's Schlüssel passt) hinzu und schickt die Box wieder zurück an A. A entfernt nun sein Schloss und schickt die Box, die immer noch von B verschlossen ist, an B zurück. Dieser öffnet nun die Box mit seinem Schlüssel und erhält die Nachricht.
Ein unberechtigter Zuhörer dieser Korrespondenz sieht eine Box, einmal von A verschlossen, einmal sowohl von A als auch von B, und schließlich von B verschlossen. In keinem dieser Fälle kann er sie öffnen.
Beim tatsächlichen (als sicher erachteten) Shamir-Protokoll wird zum Ver- und Entschlüsseln eine modulare Exponentiationsfunktion (modulo einer großen Primzahl) angewandt.

In dieser Aufgabe betrachten wir nun eine deutliche Vereinfachung: Der Klartext m von A wird als ein Bitstring dargestellt. A wählt eine Zufallsbitfolge z derselben Länge und schickt $m' = m \oplus z$ an B. B wählt ebenfalls eine Zufallsbitfolge z' und schickt $m'' = m' \oplus z'$ zurück an A. Dieser schickt $m''' = m'' \oplus z$ an B. Damit wird A's ursprüngliche Verschlüsselung wieder aufgehoben und B erhält tatsächlich $m''' = m \oplus z'$. Nochmaliges bitweises XOR mit z' ergibt bei B schließlich die Nachricht m.

Ein Abhörer, der m', m'', m''' mitlesen kann, kann die Nachricht m sehr leicht berechnen. Wieso?

44.) [Hybride Systeme]
Bei einem modernen Kryptosystem (z.B. Public key wie RSA) wird die Nachricht in Blöcke zerlegt und verschlüsselt (ein Block = 1000 Bit). Allerdings erfordert die Berechnung pro Block bei Sender und Empfänger jeweils *Blocklänge*^{3} Rechenoperationen. Es soll eine Nachricht von 10^6 Bit übertragen werden.
Man berechne, wieviele Rechenoperationen dafür erforderlich sind. (Diese Art der Übertragung wird abfällig manchmal „moderne Kryptographie nach Lehrbuch“ genannt (z.B. textbook-RSA).

Eine bessere Methode besteht darin, die modernen Krypto-Methoden lediglich dafür zu verwenden, um einen geheimen Schlüssel s der Länge 1000 Bit von A nach B zu übertragen. Nachdem beide Kommunikationspartner diesen Schlüssel nun kennen, wird dieser anschließend in einem klassischen Krypto-System verwendet, um die eigentliche Nachricht zu übertragen. Dann ist der erforderliche Rechenaufwand für die klassische Übertragung bei Sender und Empfänger lediglich *Anzahl Blöcke* $*$ ($|s|$ + *Blocklänge*).
Man berechne erneut, wieviele Rechenoperationen bei dieser so genannten hybriden Methode notwendig sind.

45.) [Anzahl der Primzahlen]
Wieviele 500-Bit-Primzahlen gibt es in etwa? Einen wie großen Anteil an den *ungeraden* 500-Bit-Zahlen macht dies aus?

46.) [Sicherheitsniveau]
Wie groß sollte die Schlüssellänge sein, wenn man für das Brechen eines bestimmten Kryptosystems Algorithmen der Laufzeit $n^{\ln(n)}$ zur Verfügung hat (n = Schlüssellänge) und ein Sicherheitsniveau von 80 Bit erreichen möchte? (Eine solche Funktion bezeichnet man als sub-exponentiell oder auch quasi-polynomial.)

47.) [Modulo-Berechnungen]
Wir wollen Rechnungen modulo 6 durchführen. Das heißt, wir verwenden und rechnen nur mit den Zahlen $0, 1, 2, 3, 4, 5$. Man stelle eine Additionstafel und eine Multiplikationstafel auf. Welche Zahl ist das neutrale Element bei der Addition; welche bei der Multiplikation? Man bestimme für jede Zahl x ihr additives Inverses, also dasjenige y mit $x + y =$ neutrales Element (mod 6). Welche Zahlen x besitzen multiplikativ ein Inverses, also ein y so dass $x * y =$ multiplikativ neutrales Element (mod 6).

48.) [Euklid]
Berechne mit dem Euklid-Algorithmus den ggT von 24 und 129.

49.) Beweise: Wenn $a \in \mathbb{Z}_n$ ein multiplikatives Inverses $b \in \mathbb{Z}_n$ mit $a \cdot b \equiv 1 \pmod{n}$ besitzt, dann sind a und n teilerfremd, also $ggT(a, n) = 1$.