Kryptologie: Übungsblatt 2, Besprechung ab dem 30.4.2018, 10:15, H20

23.) In der Vorlesung wurde das Geburtstagsparadoxon untersucht und festgestellt, dass bei $m \approx 0.5 + 1.177 \cdot \sqrt{n}$ die Wahrscheinlichkeit $1/2$ erreicht bzw. gerade überschritten wird für die Existenz einer Dublette, bei zufälliger Auswahl von m Zufallszahlen aus der Menge $\{1, 2, \ldots, n\}$ (mit Zurücklegen). Dies ist der Median der zugrunde liegenden Wahrscheinlichkeitsverteilung.

Man berechne das erste und das dritte Quartil; das heißt, bei welchem Zusammenhang zwischen m und n wird die betreffende Wahrscheinlichkeit $1/4$ bzw. $3/4$?
Was heißt das konkret für $n = 365$ wie beim Geburtstagsproblem?

24.) Ein rückgekoppeltes Schieberegister bestehe aus 4 Speichergliedern (Flip-Flops) b_1, b_2, b_3, b_4, die jeweils ein Bit (0 oder 1) speichern können. Sobald ein elektrischer Impuls auf das Schieberegister gegeben wird, nehmen b_2, b_3, b_4 die vorherigen Werte von b_1, b_2, b_3 an. Durch die Rückkopplung nimmt b_1 den Wert $b_2 \oplus b_4$ an (wobei mit b_2 und b_4 die vorherigen Werte gemeint sind).
Fertige einen Schaltplan an.
Wie groß ist die größtmögliche Periodenlänge bei einem Schieberegister dieser Größe?
Wenn dieses Schieberegister diese Periodenlänge nicht erreicht, welche Perioden(-längen) erreicht es dann in diesem konkreten Fall?

25.) Wir beobachten den Ausgabestrom eines n-Bit-Schieberegisters, dessen Rückkopplungsverschaltung wir allerdings nicht kennen. Wie viele Ausgabe-Bits muss man beobachten, bis man die gesamte Periode und die Verschaltung des Schieberegisters bestimmen kann?

26.) Wenn man Schlüssel mit 80 Bit Länge systematisch (Brute Force) durchprobiert und man auf einem sehr schnellen Rechner 10^{-10} Sekunden pro Schlüssel benötigt, wie lange benötigt man dann, um alle Schlüssel durchzuprobieren?

27.) Ein Mann eilt zu seiner Frau in die Geburtsklinik. Ihn erwarten 3 mögliche Informationen:

- Es ist ein Junge (Wahrscheinlichkeit 0,5)
- Es ist ein Mädchen (Wahrscheinlichkeit 0,48)
- Es sind Zwillinge (Wahrscheinlichkeit 0,02)

Wie groß ist der Informationsgehalt, der den Mann (im Durchschnitt) erwartet ? Wie groß ist der Informationsgehalt des Ereignisses *Zwillinge* ?

28.) Der Klartext

E S G E S C H E H E N N O C H Z E I C H E N U N D W U N D E R

wird Vigenère-verschlüsselt mit einem Schlüsselwort der Länge 3. Der Kryptoanalytiker erhält die entsprechende Chiffre und versucht nach der Friedman-Methode die Schlüssellänge zu bestimmen, indem er den Chiffretext entsprechend gruppiert und in jeder Gruppe den entsprechenden $\widetilde{IC}$-Wert ermittelt.

Welche $\widetilde{IC}$-Werte wird er ermitteln, sofern er die richtige Schlüsselwortlänge 3 verwendet?

29.) Gegeben sei eine Wahrscheinlichkeitsverteilung $P = (p_1, p_2, \ldots, p_n)$. Man kann die Formel $\sum_{i=1}^{n}(p_i - \frac{1}{n})^2$ verwenden, um die Abweichung zwischen P und einer Gleichverteilung zu ermitteln. Welchen Zusammenhang gibt es zur Formel $IC(P)$, also dem Koinzidenzindex ?

30.) Die folgende Chiffre

B L O F D W X W C R P U F L Y B E

wurde mit der Autokey-Variante 1 verschlüsselt. Der Schlüssel (und dessen Länge) ist unbekannt. Bestimmen Sie (bis auf einige Anfangsbuchstaben) den Klartext !

31.) Wenn man den $\widetilde{IC}$-Wert einer Vigenère-verschlüsselten Chiffre ermittelt, so wird sich ein Wert zwischen $\frac{1}{26} \approx 3,85\%$ und $7,6\%$ (wie bei einem deutschen Text, oder einem Cäsar-verschlüsselten deutschen Text) ergeben. Bei einem langen Schlüsselwort wird der Wert eher bei $3,85\%$ liegen, bei einem kurzen Schlüsselwort (im Extremfall nur 1 Buchstabe lang, dies entspricht einer Cäsar-Chiffrierung) wird der Wert eher bei $7,6\%$ liegen.
Entwickeln Sie eine Formel, in die man den $\widetilde{IC}$-Wert einsetzen kann und dann eine plausible Schätzung für die Schlüsselwortlänge erhält.