Solution of Exercisesheet 1

Exercise 1-1

NO ONE SHALL BE SUBJECTED TO ARBITRARY INTERFERENCE WITH HIS PRIVACY FAMILY HOME OR CORRESPONDENCE NOR TO ATTACKS UPON HIS HONOUR AND REPUTATION EVERYONE HAS THE RIGHT TO THE PROTECTION OF THE LAW AGAINST SUCH INTERFERENCE OR ATTACKS

Exercise 1-2

Key: KVUMDLQXTZGEYBIFWRAPHSONCJ

FEW FALSE IDEAS HAVE MORE FIRMLY GRIPPED THE MINDS OF SO MANY INTELLIGENT MEN THAN THE ONE THAT IF THEY JUST TRIED THEY COULD INVENT A CIPHER THAT NO UEKONE COULD BREAK

Exercise 1-3

THE BANANA IS AN EDIBLE FRUIT BOTANICALLY A BERRY PRODUCED BY SEVERAL KINDS OF LARGE HERBACEOUS FLOWER IN GPLANTSINTHEGENUSMUSA IN SOME COUNTRIES BANANAS USED FOR COOKING MAY BE CALLED PLANTAINS THE FRUIT IS VARIABLE IN SIZE COLOR AND FIRMNESS BUT IS USUALLY ELONGATED AND CURVED WITH SOFT FLESH RICH IN STARCH COVERED WITH ARIND WHICH MAY BE GREEN YELLOW RED PURPLE OR BROWN WHEN RIPE THE FRUITS GROW IN CLUSTERS HANGING FROM THE TOP OF THE PLANT WORLDWIDE THERE IS NO SHARP DISTINCTION BETWEEN BANANAS AND PLANTAINS ESPECIALLY IN THE AMERICAS AND EUROPE BANANA USUALLY REFERS TO SOFT SWEET DESSERT BANANAS PARTICULARLY THOSE OF THE CAVENDISH GROUP WHICH ARE THE MAIN EXPORTS FROM BANANA GROWING COUNTRIES BY CONTRAST MUSACULTIVARS WITH FIRMERST ARCHIER FRUIT ARE CALLED PLANTAINS IN OTHER REGIONS SUCH AS SOUTH EAST ASIA MANY MORE KINDS OF BANANA ARE GROWN AND EATEN SO THE SIMPLE TWO FOLD DISTINCTION IS NOT USEFUL AND IS NOT MADE IN LOCAL LANGUAGES

key: crypto

Exercise 1-4

To estimate the period we use the Kasiski test. The distance between the two occurrences given is 241 - 10 = 231 = $3 \cdot 7 \cdot 11$ positions.

Possible periods are thus 3, 7 and 11. If the guess is correct, we can immediately find the corresponding shifts: at position 10 the shift is T - c = 19 - 2 = 17 = r

Similar computations for the other positions gives the shift keys rrectcorrect

We now see that this is not periodic with periods 3 or 11, while period 7 is possible. The keyword of length 7 starts at position 15; hence the keyword is correct.

Solution of Exercisesheet 1

Exercise 1-5

(a) Pr [D is even] = 0.5
(b) Pr [H] = 0.5
(c) Pr [D is prime] = 0.5
(d) Pr [D is prime|H] = 0.5
(e) Pr [D is prime|D is even] = $\frac{1}{3}$
(f) Pr [D is prime $\wedge$ D is even] = $\frac{1}{6}$
(g) Pr [D is prime $\vee$ D is even] = $\frac{5}{6}$
(h) Pr [D is prime] + Pr [D is even] = 1
Why are ((d)) and ((e)) different, even though Pr [H] = Pr [D is even]?
In ((d)) are the events independent from each other, in ((e)) not.
Why are ((g)) and ((h)) different?
In ((g)) counts $D = 2$ one time, in ((h)) is it in both events contained.

Exercise 1-6

$\pi(x) < \frac{x}{ln(x)-4}$ mit $x = 2^{\frac{n}{2}}$ und $n = 2048$

$$\begin{aligned}
Pr[Coll] &= Pr[(p = p') \vee (p = q') \vee (q = p') \vee (q = q')] \\
&\leq Pr[p = p'] + Pr[p = q'] + Pr[q = p'] + Pr[q = q'] \\
&= \frac{4}{\pi(x)} \\
&< \frac{4 \cdot (\ln x - 4)}{x} \\
&= \frac{4 \cdot (\ln x - 4)}{x} \\
&= \frac{4 \cdot (\ln 2^{\frac{n}{2}} - 4)}{2^{\frac{n}{2}}} \\
&= \frac{4 \cdot (\frac{n}{2} \cdot \ln 2 - 4)}{2^{\frac{n}{2}}}
\end{aligned}$$

Solution of Exercisesheet 1

$$
\begin{aligned}
Pr[\bigcup_{1\le i<j\le n} Coll_{i,j}] &\le \sum_{1\le i<j\le n} Pr[Coll_{i,j}] \\
&= \sum_{1\le i<j\le n} \left[\frac{4\cdot(\frac{n}{2}\cdot\ln 2-4)}{2^{\frac{n}{2}}}\right] \\
&= \sum_{j=1}^{n}\sum_{i=1}^{j-1} \left[\frac{4\cdot(\frac{n}{2}\cdot\ln 2-4)}{2^{\frac{n}{2}}}\right] \\
&= \sum_{j=1}^{n}(j-1)\cdot\left[\frac{4\cdot(\frac{n}{2}\cdot\ln 2-4)}{2^{\frac{n}{2}}}\right] \\
&= \frac{(n-1)\cdot n}{2}\cdot\left[\frac{4\cdot(\frac{n}{2}\cdot\ln 2-4)}{2^{\frac{n}{2}}}\right] \\
&\le \frac{n^2}{2}\cdot\left[\frac{4\cdot(\frac{n}{2}\cdot\ln 2-4)}{2^{\frac{n}{2}}}\right] \\
&= \ldots
\end{aligned}
$$

Exercise 1-7