Cryptography, winter term 16/17: Assignment 1

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due November 9, 2016

Exercise 1.1 (Shift Cipher) The following is an encryption of English text using a shift-cipher. Find the key and decrypt the ciphertext.

O QFMDHCGMGHSA GVCIZR PS GSQIFS SJSB WT SJSFMHVWBU OPCIH HVS GMGHSA SLQSDH HVS YSM WG DIPZWQ YBCKZSRUS

Exercise 1.2 (Bonus: Vigenère Cipher) For some reasons, the TAs of the Cryptography lecture have to communicate over an unsafe channel while they create Problem 1.5. Lurking around in front of their office, you overheard them talking about it. Apparently, they decided to use the Vigenère cipher to encrypt their messages. The next day, you were able to eavesdrop a part of their communication and to obtain an encrypted chat protocol. Can you decrypt it? Which principle did they violate? Maybe there is some information hidden that can help you to solve Problem 1.5. You can find the encrypted protocol here:

http://www-cc.cs.uni-saarland.de/crypto1617/encrypted_protocol/

Exercise 1.3 (False positives) In the sprit of interdisciplinary education, picture yourself as a student of criminal law, presented with the following case:

A murder has happened, and witnesses are nowhere to be found. Luckily, the culprit blundered and left some of his DNA at the crime scene. The police then conduct a massive screening of 10 Million people, and perform DNA tests on each of them. The test they use, on average, identifies *wrongly* one out of every million people as having the same DNA, i.e. the test reports a match with the sample DNA although they are actually distinct one millionth of the time. At the same time, if the samples actually *are* identical, the test *always* correctly reports this. You, in your future role of a judge, are now to decide the fate of a person whose DNA produces a positive test result. Would you count this as evidence against this person? Why? (In other words, calculate the probability that this person actually is the sought murderer, given that the murderer is among the sampled people.)

Exercise 1.4 (Coin tossing) In this exercise, you will show how to simulate fair coins with biased coins and vice versa.

(a) You are given a biased coin, i.e. $\Pr[H] = p$ for some $0 < p < 1$, and $\Pr[T] = 1 - p$. Demonstrate an algorithm that, using only this biased coin, produces the outputs H and T with equal probability and prove that it is correct and halts with probability 1.

Hint / Bonus: Consider the experiment where the biased coin is flipped two times and let C_1 and C_2 denote the outcomes of the flips. Compute the probability $\Pr[C_1 = H | C_1 \neq C_2]$. For bonus points, calculate the expected runtime (i.e., number of iterations) of your procedure.

(b) You are given a fair coin, i.e. $\Pr[H] = \Pr[T] = 1/2$, and some $0 < t < 1$.[1] Let $(a_i)_i$ be the binary expansion of t, i.e. $t = \sum_{i=1}^{\infty} \frac{a_i}{2^i}$. Consider the following strategy, where initially, $n = 1$.

(i) Throw the coin. Let the result be r.

(ii) If $r = H$, compute the a_n. If $a_n = 1$, output H, otherwise, output T.

(iii) If $r \neq H$, start over and increase n by one.

Prove that this strategy terminates after two iterations in expectation, and that it in fact produces H with probability t.

Bonus: Take a moment and ogle in awe at the mindboggling simplicity of this procedure and the supreme power it entails: You can now imitate any (computably) biased coin with—in expectation—just two coin tosses.

Exercise 1.5 (The Haunty Mall Problem) It is the evening of the 31st of October, and after a long day's studies, you decide to make a recreational trip to the local mall. But — who could have seen it coming! — your visit turns into a living nightmare when you are captured by dreadful creatures (demons, ghosts and suchlike) and dragged down into the eternal fires of hell. You then find yourself trapped in a gruesome game: The soulless dwellers of hell thrive on seeing students suffer, and hence they confront you with a riddle.

There are 666 closed gates in front of you. Of these gates, 665 harbour only everlasting, hellish pain and sorrow, but one of them, so you are promised, will lead you back to your earthly home. You have to decide for one of these 666 gates, and after you do so, one of the demons will open, 664 of the remaining 665 portals you did not choose, such that behind *all* of them there is, you know, everlasting, hellish pain and sorrow. You can now decide: Will you stick with your original choice, or will you change your mind and pick the only remaining closed gate?

Prove to the demons that your years at university have made you immune against soulless creatures thriving on seeing students suffer, by showing how to maximize your chance of returning home. Good luck!

[1] For those acquainted with the term: t needs to be computable.