2. Exercise sheet

Hand in solutions until Saturday, 19 April 2014, 23:59:59

Exercise 2.1 (Brute force). (6 points)
To get a better understanding of the amount of work you need to do when employing brute-force cryptanalysis, estimate for which key-sizes you can exhaustively test all keys within a year using your own computer, all computers of a university with, say, 10000 computers, or all computers in the world (there are roughly 2 billion computers out there). You can assume that testing a single key requires exactly one CPU cycle and that each computer runs with 1GHz on average.

Exercise 2.2 (Birthdays). (5 points)
Neglecting skip years and seasonal birthrate irregularities, compute for sets of ten to thirty individuals the probability of birthday collisions. Hint: You might want to write a little program for this task.

Exercise 2.3 (The CBC mode of operation). (10 points)
Consider the CBC mode of operation.
(i) Show that CBC-MAC without final re-encryption is insecure. Argue that re-encryption fixes this issue. Hint: Consider a single block message \( m \) with authentication tag \( t \) and show that \( m \| (m \oplus t) \) has also authentication tag \( t \). Here the symbol \( \| \) denotes concatenation of bit-strings.
(ii) Construct an explicit distinguishing attack under chosen messages on CBC-encryption, when used beyond the birthday limit. Hint: Consider two (carefully selected) long messages whose encryption will, by the birthday paradox, contain two identical blocks with high probability.

Exercise 2.4 (baby-step giant-step for DL). (4 points)
Consider the cyclic group \( G = \mathbb{Z}_{23}^\times \) with generator \( g = 5 \) and compute the discrete logarithm of \( x = 17 \) using the baby-step giant-step algorithm from the lecture. Document your steps and set up a table with the values computed for \( xg^k \) and \( g^{km} \).