Homework 7 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
27.11.2012

Solution to Exercise 20.

(a) For the MRPT (Miller Rabin primality test) the number n shall be displayed as $n = 1 + q \cdot 2^k$. Then, there are k squarings (iterations in the for loop). Consequently, the worst case occurs for $q = 1$, i.e., $n = 1 + 2^k$. It follows

$$n - 1 < 10^{301} = 2^{\log_2(10)\cdot 301} < 2^{1000}.$$

In worst case less than 1000 squarings are needed.

(b) By assumption $P(\text{MRPT states „}n \text{ is prime“} \mid \text{„}n \text{ is composite“}) = \frac{1}{4}$. Let X be a random variable describing the number of tests until „n is composite“ is stated for the first time. As the repetitions for MRPT evaluations are independent, X follows a geometric distribution with parameter $p = \frac{3}{4}$, i.e.,

$$P(X = M) = \left(\frac{1}{4}\right)^{M-1} \frac{3}{4} \text{ and } E(X) = \frac{1}{p} = \frac{4}{3}.$$