Homework 7 in Advanced Methods of Cryptography

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

27.11.2012

Exercise 18. A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR.

(a) Exactly one bit changes during transmission. How many bits are decrypted wrongly in the worst case?

(b) What happens, if one bit of the ciphertext is lost or an additional bit is inserted?

Exercise 19.

(a) Use Fermat's Primality Test to prove that 341 is composite.

(b) Use the Miller-Rabin Primality Test to prove that 341 is composite.

Hint: It holds $3^{10} \mod 341 = 56$.

Exercise 20.

(a) The Miller-Rabin Primality Test (MRPT) comprises a number of successive squarings. Suppose a 300-digit number n is given. How many squarings are needed in the worst case during a single run of this primality test?

(b) Let $n \in \mathbb{N}$ be odd and composite. Repeat the MRPT with uniformly distributed random numbers $a \in \{2, \dots, n-1\}$ until the output is „n is composite“. Assume that the probablity of the test outcome „n is prime“ is $\frac{1}{4}$.

Compute the probability, that the number of such tests is equal to M, $M \in \mathbb{N}$. What is the expected value of the number of tests?

Exercise 21. The Miller-Rabin Primality Test (MPRT) is applied m, $m \in \mathbb{N}$, times to check, whether n is prime, where n is chosen according to a uniform distribution on the odd numbers in $\{N, \dots, 2N\}$, $N \in \mathbb{N}$.

(a) Show that

$$P(\text{„}n\text{ is composite“} \mid \text{MRPT returns } m \text{ times „}n\text{ is prime“}) \leq \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}}.$$

(b) How many repetitions m of the test are needed to ensure that the above probabilty stays below $1/1000$ for $N = 2^{512}$?

Hint: Assume $P(\text{„}n\text{ is prime“}) = 2/\ln(N)$.