Exercise 2 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-10-31

Problem 4. *(calculating the basis)* Given $a^{13} \equiv 17 \mod 31$, calculate the basis a.

Problem 5. *(Rabin cryptosystem)* Alice and Bob are using the Rabin Cryptosystem. Bob uses the public key $n = 4757 = 67 \cdot 71$. All integers in the set $\{1, \ldots, n-1\}$ are represented as a bit sequence of 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Problem 6. *(modified Rabin cryptosystem)* Consider the modification of the Rabin Cryptosystem in which $e_K(m) = c = m \cdot (m + B) \mod n$, where $B \in \mathbb{Z}_n$ is part of the public key. Supposing that $p = 199$, $q = 211$, $n = pq$, and $B = 1357$, perform the following computations.

a) Compute the encryption $y = e_K(32767)$.

b) Determine the four possible decryptions of this given ciphertext y.