Wrocław University of Technology, WPPT 12.10.11

CRYPTOGRAPHY AND SECURITY, 2011 Assignments, list # 3

1. Change one bit of a plaintext for AES. Specify which bytes during the AES computation cannot be affected by this change.
2. Given specification of the AES encryption algorithm describe AES decryption algorithm.
3. Is it possible to apply fault analysis combined with differential cryptanalysis for AES?
4. CBC has the disadvantage that changing one block of plaintext results in necessity of updating all later blocks in the ciphertext. How to avoid it without falling back to ECB: we do not want an adversary to recognize that there are two identical blocks of the plaintext after reading the ciphertext.
5. Assume that we have a linear approximation of each of S-boxes of DES that holds with probability 0.9. based on that construct a linear approximation for 2 rounds of DES.
6. Find a way to modify the plaintext corresponding to a given ElGamal ciphertext without access to the encryption key. Propose some countermeasures!
7. Design an iterative algorithm based on Binary GCD for computing $x^{-1} \bmod p$ for an input x. Estimate the runtime of this algorithm.
8. Consider n which is not a prime number. Under which conditions an $x < n$ has an inverse y modulo n, i.e. an y such that $x \cdot y = 1 \bmod n$.

   Determine the number of such invertible elements for $n = pq$, where p and q are different prime numbers.
9. Find a reasonable choice of the parameters for finding discrete logarithm with baby-step giant-step algorithms on a typical PC.
10. Recall the Floyd method applied for Pollard rho algorithm for finding discrete logarithms. Assume that we would like to save time and instead of computing x_i and x_{2i} for $i = 1, 2, \ldots$, we postpone a little bit and start from some j: we compute x_{j+i} and x_{j+2i} for $i = 1, 2 \ldots$.
    How to choose j?
11. Estimate time and space complexity of Pohlig-Hellman method for finding discrete logarithms.

/-/ Mirosław Kutyłowski