AVOIDING RIGHT ANSWERS BY FOLLOWING A WRONG METHOD

Dolantina Hyka[1], Ardi Benusi[2]

[1]Faculty of Natural Sciences, University of Tirana, Albania
E mail: dolantina.hyka@fshn.edu.al
[2]Faculty of Natural Sciences, University of Tirana, Albania
E mail: ardi.benusi@fshn.edu.al

Abstract

In the process of learning cryptography students exercise their skills on encrypting and decrypting through different examples on several cryptosystems. Sometimes even when they follow a wrong method they may get the right answer. To avoid this problem we are considering a method that consists on generating examples that can be solved only by following the right steps of the algorithm and cannot take the right answer if one of the steps of the algorithm is not followed correctly. In this paper it is considered the El – Gamal cryptosystem over finite fields Z_q and over Elliptic Curves. Firstly are presented its weakness and its computational most common errors. In each case there is a specified algorithm to avoid that error. As seen in the previous work with Massey – Omura and RSA cryptosystems, this conclusion can also be used even in constructing algorithms not only in cryptography but also in other disciplines for example generating different types of differential equations without solving them firstly or generating matrix equations and being sure about the number of solutions, financial mathematics, micro-economy, finance and in other modules.

Keywords: *El-Gamal, ECC, diagnostic examples, strong examples, algorithms.*