THE CRYPTANALYSIS OF THE ENIGMA CIPHER

Anna Borowska

Faculty of Computer Science, Bialystok University of Technology, Białystok, Poland

Abstract: In this paper we study cryptanalysis of the military Enigma machine which was used by the German Army during the Second World War. We are interested in the problem of decoding secret messages transmitted after 15 September 1938. We give a complete algorithm which can be used to: generate the ring settings, guess what kinds of drums are chosen and determine the order of the drums on a shared shaft. The proposed algorithm is an optimization of the Zygalski's sheets method. Before we present it, we will describe the mystery which is hidden in the sheets (author's observations). In order to read the encrypted messages we need the plugboard settings. Connections of the plugboard influence neither Zygalski's method (which is a well-known fact) nor the presented algorithm. The missing (original) algorithm solving the problem of the plugboard along with an algebraic description will appear very soon.

Keywords: Zygalski's sheets method, Enigma machine, ring settings, message settings

KRYPTOANALIZA SZYFRU ENIGMY

Streszczenie Tematem pracy jest kryptoanaliza Enigmy wojskowej używanej przez siły zbrojne oraz inne służby państwowe Niemiec podczas II wojny światowej. Jesteśmy zainteresowani problemem dekodowania zaszyfrowanych depesz transmitowanych po 15 września 1983 roku. Prezentujemy pełny algorytm służący do generowania ustawień pierścieni, odgadywania które rodzaje bębenków zostały wybrane i wyznaczania ich porządku na wspólnej osi. Proponowany algorytm jest uzupełnieniem i optymalizacją metody płacht Zygalskiego. W pracy opisane są istotne własności płacht wynikające z konstrukcji maszyny i teorii permutacji (spostrzeżenia autora). Do czytania depesz zaszyfrowanych za pomocą Enigmy potrzebne są jeszcze ustawienia łącznicy wtyczkowej. Połączenia łącznicy nie mają wpływu ani na metodę Zygalskiego (znany fakt) ani na przedstawiony algorytm. Brakujący (oryginalny) algorytm rozwiązujący problem łącznicy (wraz z algebraicznym opisem) pojawi się niebawem.

Słowa kluczowe: metoda płacht Zygalskiego, ustawienia pierścieni, ustawienia depeszy

Advances in Computer Science Research, vol. 10, pp. 19-38, 2013.