THE DYNAMIC CIPHERS - NEW CONCEPT OF LONG-TERM CONTENT PROTECTING

Author **Grzegorz Szewczyk**
N/A

Abstract:

In the paper the original concept of a new cipher, targeted at this moment for civil applications in technology (e.g. measurement and control systems) and business (e.g. content protecting, knowledge-based companies or long-term archiving systems) is presented. The idea of the cipher is based on one-time pads and linear feedback shift registers. The rapidly changing hardware and software environment of cryptographic systems has been taken into account during the construction of the cipher. The main idea of this work is to create a cryptosystem that can protect content or data for a long time, even more than one hundred years. The proposed algorithm can also simulate a stream cipher which makes it possible to apply it in digital signal processing systems such as those within audio and video delivery or telecommunication.

Keywords: *Content protection, Cryptosystem, Dynamic cryptography, Linear Feedback Shift Registers, Object-oriented programming, One-time pad, Random key, random number generators, Statistical evaluation of ciphers.*

JEL codes:: *D83*