

PRACTICAL APPLICATION OF OPEN SOURCE SOFTWARE TOOLS IN CRYPTOGRAPHY

Dragan Randjelovic

The Academy for Criminalistic and Police Studies, Belgrade

Milos Randjelovic Help, Nis

Zeljko Kuzmanovic

City of Banja Luka, City Administration

Summary: Security of computer systems is becoming more important, because more users in more ways use more information in the computer world. With the development of information technologies and telecommunication systems and a greater diffusion in the geographical sense growing is also the possibility of misuse of data which are transferred through open and insecure communication paths which requires a more efficient protection. In the system of data transfer attackers can easily destroy data, modify them or the information can come into possession of unauthorized persons or organizations which can often have very heavy consequences. The problem is especially expressed in some organizations such as state administrations, banking, judicial, military, medical and other administrations. In this paper explained are basic terms related to crypts and algorithms which were used and which are used, as well as methods of data protection in computer networks based on cryptography in order to protect privacy inside a network of computers. Explained are symmetrical and asymmetrical cryptosystems and the technique of digital signature. Also, the subject of this paper is the presentation of the program CrypTool and CryptoWorkflow, which belong to the most famous free ie. shareware software in the field of cryptography, with special emphasis on the possibility of applying different algorithms and comparative analysis of their work and are given concrete examples of their use.

Keywords: cryptography, symmetric and asymmetric systems, digital signature, CrypTool, CryptoWork flow.

Pages 115-135