Cryptographic protection for military radio communications

ISBN/ISSN
eISSN: 2300-1933, ISSN: 2081-8491

Informacje dodatkowe
IJET International Journal of Electronics and Telecommunications
(A periodical of Electronics and Telecommunications Committee of Polish Academy of Sciences)
Vol 66, No 4 (2020)
DOI: 10.24425/ijet.2020.134028

Abstract: Protecting the confidentiality, integrity and availability of information is very important in any telecommunications system. Information protection requires use of necessary physical, personal, information and communication technologies and above all – electromagnetic and cryptographic security measures. Equipment and tools for cryptographic protection should be examined and assessed in terms of resistance to known threats. Additional requirements are put on information protection for radio communication, especially military, where radio transmission is characterized by uncertainty of establishing and maintaining connections, bit rates are relatively low, often without full duplex. All this has an impact on the methods of cryptographic

synchronization and implementation of cryptographic functions. A different approach to information protection is required by classic narrowband radio communications, a different one in time-division multi-access modes, and another one in broadband packet data transmission. Systems designed for information protection in radio communications implement appropriate operating modes of operation for cryptographic algorithms and protocols. Latest threats from quantum computers pose new challenges, especially in systems using public-key cryptography, because there are algorithms that can be used to attack these schemes with polynomial complexity.
Keywords: cryptography, cryptanalysis, radio communication, quantum computers

Powiązane publikacje

-

Adres url strony

http://ijet.pl/index.php/ijet/article/view/10.24425-ijet.2020.134028

Plik