A POSSIBLE KEY EXCHANGE PROTOCOL OVER GROUP RINGS

Ömer KÜSMÜŞ[1], Turgut HANOYMAK[2]

[1] *Yuzuncu Yil University, Van, Turkey*
[2] *Yuzuncu Yil University, Van, Turkey*

MSC 2000: 94A60, 11T71, 14G50

Abstract

Key exchange protocols are such methods for parties who want to generate shared cryptographic keys that they can send secret messages to each other securely through an insecure channel. In this paper, we first construct a possible key exchange protocol over group rings by giving a concrete example and discuss the security of the system.

Keywords: group rings, units, cryptographic keys, security

References

[1] Katz J., Lindell Y., Intoduction to Modern Cryptography, (2007)

[2] Milies C. P., Sehgal S. K., An Introduction to Group Rings, *Kluwer Acad. Publ.*, (2002)

[3] Hurley B., Hurley T., Group Ring Cryptography, *J. Pure and Appl. Math.*, 69, 67-86, (2011)

[4] Koblitz N., A Course in Number Theory and Cryptography, Springer-Verlag, New York (1994)

[1] omerkusmus@yyu.edu.tr
[2] turguthanoymak@gmail.com