A construction of a key exchange protocol

Luigia Berardi *
Dipartimento di Ingegneria Elettrica e dell'Informazione
Università degli Studi de L'Aquila
Monteluco di Roio
67040 L'Aquila
Italy

Rosaria Rota †
Dipartimento di Matematica
Università degli Studi di Roma Tre
Largo San Leonardo Murialdo 1
00146 Roma
Italy

Abstract

In this paper we construct a key exchange protocol for four users using a function with a particular property. The construction can be generalized to many users. In [1] and [3] there is a key exchange protocol for two or three users based on 2-cocycles.

Keywords : *Cryptography, cocycle.*

1. Introduction

Cryptography is the science that studies methods for sending messages in secret (i.e. in enciphered or disguised form) over an insecure channel, so that only the intended recipient can remove the disguise and read the message. Until the beginning the aim was to obtain confidentiality, integrity and authenticity of message. We can get this through a cryptographic system, or cryptosystem, which uses encryption and decryption algorithms (cf. [4]).

Cryptography is fundamental in order to protect information against wiretapping, unauthorised changes and other measure of information, in

* *E-mail*: berardi@ing.univaq.it
† *E-mail*: rota@mat.uniroma3.it

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 2, pp. 171–174