

Research Article

A Comparative Evaluation of Algorithms in the Implementation of an Ultra-Secure Router-to-Router Key Exchange System

Nishaal J. Parmar and Pramode K. Verma

Telecommunications Engineering Program, School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK, USA

Correspondence should be addressed to Nishaal J. Parmar; nishaal.parmar@ou.edu

Received September ; Accepted October ; Published January

Academic Editor: Vincente Martin

Copyright © N. J. Parmar and P. K. Verma. is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper presents a comparative evaluation of possible encryption algorithms for use in a self-contained, ultra-secure router-to-router communication system, first proposed by El Rifai and Verma. The original proposal utilizes a discrete logarithm-based encryption solution, which will be compared in this paper to RSA, AES, and ECC encryption algorithms. RSA certificates are widely used within the industry but require a trusted key generation and distribution architecture. AES and ECC provide advantages in key length, processing requirements, and storage space, also maintaining an arbitrarily high level of security. This paper modifies each of the four algorithms for use within the self-contained router-to-router environment system and then compares them in terms of features offered, storage space and data transmission needed, encryption/decryption efficiency, and key generation requirements.

1. Introduction

With the rise of globalization, microelectronics, and the information age, the need for rapid, long-distance transmission of unconditionally secure information has never been greater. Whether dealing with military intelligence, corporate secrets shared between two (or more) companies, remote control of vital national infrastructure components such as power and traffic control systems, or mechanical instructions transmitted to on-site medical devices for telesurgery, device updates, and health reports, there are many situations where the rapid, accurate, and secure transmission of information between two parties is a basic necessity. In extreme cases, alteration or even decryption of this information by unauthorized parties may result in damages of billions of dollars and the lives of others.

Historically, only two encryption schemes have been proposed which offer unconditional security, both unsuitable for practical telecommunications. The first, the one-time pad, proposed by Gilbert Vernam in [1], utilizes a single-use encryption key equal to the message length which both the sending and receiving parties may use to encrypt and decrypt the message. The disadvantages of this system in a long-term high data rate communication system are obvious,

with each message requiring a preshared key equal to the message length. The second, recently proposed unconditional cryptographic system is quantum cryptography, where security is achieved through the laws of quantum mechanics, which allow for very accurate determination of eavesdroppers along a quantum channel, as well as the simultaneous determination of small shared and secure random values. Currently available quantum encryption protocols include BB84, proposed in [2] by Bennett and Brassard [3], the variant SARG [4], and the later-developed B92 [5]. All three solutions, while unconditionally secure, possess severe limitations which make them unsuitable for general commercial use, including reliance on single-photon generators (greatly limiting practical data rate) and, most importantly, the presence of a physical, well characterized quantum channel between endpoints, with a maximum practical distance of a few hundred km. While some research has been proposed in the use of multiphoton quantum sources [6] and channel extension [7], this technology remains extremely expensive and unfeasible for general commercial use.

While unconditional security may be an unachievable goal, it may be realized to an arbitrarily high level via existing symmetric and asymmetric encryption systems. Currently, the most widely used form of global network communication

