Chapter 7
Modification of Traditional RSA into Symmetric-RSA Cryptosystems

Prerna Mohit
Indian Institute of Technology (Indian School of Mines), India

G. P. Biswas
Indian Institute of Technology (Indian School of Mines), India

ABSTRACT

This paper addresses the modification of RSA cryptography namely Symmetric-RSA, which seem to be equally useful for different cryptographic applications such as encryption, digital signature, etc. In order to design Symmetric-RSA, two prime numbers are negotiated using Diffie-Hellman key exchange protocol followed by RSA algorithm. As the new scheme uses Diffie-Hellman and RSA algorithm, the security of the overall system depends on discrete logarithm as well as factorization problem and thus, its security is more than public-key RSA. Finally, some new cryptographic applications of the proposed modifications are described that certainly extend the applications of the existing RSA.

1. INTRODUCTION

As the popularity of internet technology is increasing, more and more numbers of users are using it. In addition, its security protection is also very important. Hence, to provide security protection, data need to be encrypted before transmitting over a public channel. Two basic technologies are used for the encryption of data, i.e. symmetric key encryption and asymmetric key encryption (Mohit et al., 2015; Mohit et al., 2016; Sun et al., 2007). One of the very well-known cryptography scheme is RSA algorithm (Sun et al., 2007; Peng et al., 2016; Ambedkar et al., 2011; Minni et al., 2013). In broad terms the security of traditional public-key cryptosystem either depend on the factorization problem or the discrete logarithm problem. The RSA-type algorithm comes under the factorization problem and the Diffie-Hellman (DH) comes under discrete logarithm problem. We modify the RSA encryption technology using a combination

DOI: 10.4018/978-1-7998-1763-5.ch007

of DH, RSA and presented a more efficient encryption/decryption technology. In 1998, Takagi (Takagiet al., 1998) showed the extension of RSA to multi-prime algorithm with modulus $p^k q$ and reduced the decryption time by using Quisquater-Couvreur method. After a few years in 2002, Elkamchouchi et al. (Elkamchouchi et al., 2002) proposed extended RSA, where RSA algorithm is implemented using Gaussian integers over real and imaginary numbers.

Later on, several versions of the extended RSA are developed that shows the validity of executing RSA algorithm over the complex numbers (El-Kassar et al. 2005) (Verkhovsky et al., 2011), however its competence is lesser than the existing RSA. In 2015 M. Thangavel (Thangavel, 2015) proposed an enhanced version of RSA, which uses several parameters such as four prime numbers, three Euler functions, multiple public and private exponents that increase the overall computational complexity and overhead of the scheme.

In this paper, a modification of the RSA algorithm is proposed. The public-key RSA is converted into a Symmetric-key RSA (SYM-RSA) cryptosystem, where two prime numbers are securely exchanged using a hybrid of Diffe-Hellman key exchange, RSA and used them for the generation of a secret key between two participants.

The rest of the paper is presented as follows. Section 2 gives preliminaries of some existing schemes considered in order to understand the proposed protocol. Section 3 explains the proposed symmetric-RSA (SYM-RSA) followed by its security analysis in Section 4. Section 5 contains the conclusion of the paper.

2. PRELIMINARIES

Since the modifications of RSA are proposed using Diffie-Hellman (DH) key exchange protocol, thus DH and RSA techniques are introduced below.

2.1. Diffie-Hellman (DH) Protocol

In (Diffie et al., 1976), Whitfield Diffie and Martin Hellman published an elementary article for secure exchange of a contributory common key between two remote participants over public channels. It does not require any prior information and is known to be the first public-key cryptosystem. In DH protocol, a finite multiplicative group $<Z_P, \times>$ with a generator g are publicly assumed, and two public messages are exchanged for negotiation of a secret key. Let A and B are two participants, who exchange the following two public messages, where $A \rightarrow B$: C means A sends message C to B:

$A \rightarrow B$: $X = g^x \pmod P$, where $1 < x < P$ and x is a random secret chosen by A

$B \rightarrow A$: $Y = g^y \pmod P$, where $1 < y < P$ and y is a random secret chosen by B

The common contributory secret key K (say) is calculated by the participants independently as

$$K = Y^x \pmod P = (g^y)^x \pmod P = X^y \pmod p = (g^x)^y \pmod P$$