Review — A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

Daniella Albuquerque dos Angelos

Universidade de Brasilia
daniaangelos@gmail.com

Abstract. **Keywords:** computational geometry, graph theory, Hamilton cycles

1 Introduction

2 RSA Encryption and Decryption Methods

To encrypt a message M, using a public encryption key (e, n), being e and n positive integers, proceed as follows.

First, use any standard representation to represent the message as an integer between 0 and $n-1$. The purpose here is not to encrypt the message but only to get it into the numeric form necessary for encryption.

Then, encrypt the message by raising it to the e-th power modulo n. That is, the ciphertext C is the remainder when M^e is divided by n.

To decrypt the ciphertext, raise it to another power d, again modulo n. The encryption and decryption algorithms E and D are thus:

$$C \equiv E(M) \equiv M^e \pmod{n}, \text{ for a message } M$$
$$D(C) \equiv C^d \pmod{n}, \text{ for a ciphertext } C$$

Note that encryption does not increase the size of a message.

The *encryption key* is thus the pair (e, n). Similarly, the *decryption key* is the pair (d, n). Each user makes his encryption key public, and keeps the corresponding decryption key private.

To choose the appropriate keys to use this method, one first needs to compute n as the product of two large random primes p and q:

$$n = p \cdot q$$

Although n will be made public, the prime factors p and q are both hidden due to the enormous difficulty of factoring n, that we are aware of. This also hides the way d can be derived from e. Then, a choice for d is any random large integer which is relatively prime to $(p-1)\cdot(q-1)$. That is, d satisfies:

$$\gcd(d, (p-1)(q-1)) = 1$$

where gcd means the greatest common divisor.

2.1 Algorithms

3 Complexity

4 Related Work

References

1. Clarke, F., Ekeland, I.: Nonlinear oscillations and boundary-value problems for Hamiltonian systems. Arch. Rat. Mech. Anal. 78, 315–333 (1982)
2. Clarke, F., Ekeland, I.: Solutions périodiques, du période donnée, des équations hamiltoniennes. Note CRAS Paris 287, 1013–1015 (1978)
3. Michalek, R., Tarantello, G.: Subharmonic solutions with prescribed minimal period for nonautonomous Hamiltonian systems. J. Diff. Eq. 72, 28–55 (1988)
4. Tarantello, G.: Subharmonic solutions for Hamiltonian systems via a $\mathbb{Z}_p$ pseudoindex theory. Annali di Matematica Pura (to appear)
5. Rabinowitz, P.: On subharmonic solutions of a Hamiltonian system. Comm. Pure Appl. Math. 33, 609–633 (1980)