Chapter 48
Problems in Cryptography and Cryptanalysis

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

Rajakani M.
Mepco Schlenk Engineering College, India

ABSTRACT

The integer factorization problem used in the RSA cryptosystem, the discrete logarithm problem used in Diffie-Hellman Key Exchange protocol and the Elliptic Curve Discrete Logarithm problem used in Elliptic Curve Cryptography are traditionally considered the difficult problems and used extensively in the design of cryptographic algorithms. We provide a number of other computationally difficult problems in the areas of Cryptography and Cryptanalysis. A class of problems called the Search problems, Group membership problems, and the Discrete Optimization problems are examples of such problems. A number of computationally difficult problems in Cryptanalysis have also been identified including the Cryptanalysis of Block ciphers, Pseudo-Random Number Generators and Hash functions.

INTRODUCTION

Cryptography is the science of 'hidden writing' meaning ability to transform the original text into a form that is not intelligible to other parties. Cryptanalysis is the science of uncovering the plaintext from the ciphertext or guessing the key given sufficient plaintext-ciphertext pairs. The problems in distributing the key in symmetric Key Cryptosystems led to the invention of Public Key Cryptosystems which are usually based on a mathematically and computationally difficult problem. This chapter surveys the mathematical basis on which most of the cryptography algorithms are based on. This chapter also surveys the different types of attacks on cryptosystems and the threat models which cryptanalysts in analyzing the strength of the cryptographic algorithms. The fields of Cryptography and Cryptanalysis present a number of problems that are both computational and information-theoretic in nature. Those problems are discussed in the following paragraphs.

DOI: 10.4018/978-1-7998-5351-0.ch048

PROBLEMS IN CRYPTOGRAPHY

In search for more efficient and/or secure alternatives to established cryptographic protocols (such as RSA which is based on the factorization problem), there have been proposals for public key establishment protocols as well as with public key cryptosystems based on hard search problems from combinatorial (semi) group theory. These problems include the conjugacy search problem (Anshel et al.,1999; Ko, 2000), the homomorphism search problem (Grigoriev et al., 2006; Shpilrain, 2006a), the decomposition search problem (Cha et.al, 2001; Ko, 2000; Shpilrain, 2005) and the subgroup membership search problem (Shpilrain, 2006b). All these are problems of the following nature: given a property P and the information that there are objects with the property *P*, find at least one particular object with the property *P* from a pool *S* of objects.

The following problems have been considered difficult problems and used in cryptography.

The RSA Problem: Given a positive integer n that is a product of two distinct odd primes p and q and a positive integer e such that $\gcd(e,(p-1)(q-1)) = 1$ and an integer c, find an integer m such that $m^e \equiv c \pmod{n}$.

The RSA Problem is that of finding the e^{th} roots modulo a composite integer n. The underlying one-way function $f(x) = x^e \pmod{n}$ ($f: Z_n \rightarrow Z_n$) is called the RSA function. Z_n is the set of integers modulo n i.e., $Z_n = \{0, 1, 2, \ldots n-1\}$. Addition, Subtraction and Multiplication are performed modulo n. The inverse is $f(x)^{-1} = x^d \pmod{n}$, where $d \equiv e^{-1} \pmod{\varphi(n)}$

The Quadratic Residuosity Problem: Given an odd composite integer n and integer having Jacobi symbol $\left(\frac{a}{n}\right) = 1$, decide whether or not a is a quadratic residue modulo n. The integer a is said to be a quadratic residue if there exists an x such that $x^2 \equiv a \pmod{n}$.

If the prime factorization is $n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$. then the Jacobi symbol is evaluated as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \ldots \left(\frac{a}{p_m}\right)^{e_m}$$

where $\left(\frac{a}{p_i}\right)$ evaluates to 0, 1, or -1 if a divides p_i or a is a quadratic residue or if a is a quadratic non-residue of p_i.

The Square Root Modulo n Problem: Given a composite integer n and $a \in Q_n$ (the set of quadratic residues modulo n), find a square root of a modulo n.

If the factors p an q of are known, then the square root problem can be efficiently by first finding square roots of a modulo p and a modulo q and then combining them using Chinese Remainder Theorem (Zhu, 2001).

The subset-sum problem: Given positive integers (or weights) $s_1, s_2, \ldots s_n$, and T, determine whether there is a subset of the s_i's that sums to T. This is equivalent to determining a (0-1) vector $x = (x_1, x_2, \ldots x_n)$ such that