RESEARCH PAPER | Computer Science | Volume : 5 | Issue : 9 | September 2015 | ISSN - 2249-555X

Statistical Methods for Cryptography

KEYWORDS

Dr.Kishor H Atkotiya

Head, Dept. of Computer Science, J.H. Bhalodia Women's College, Rajkot

ABSTRACT *In this paper, after recalling certain results regarding prime numbers, we will present the following theorem of interest to cryptography: Let two discrete s.v.'s (statistical variable) X, Y assume the value: 0,1,2….; m - . Let X be uniformly distributed, that is, it assumes the value i(i=0,1,….m-1)with probability 1/m and let the second s.v. Y assume the value i with probability .* $(p_i : \sum_{i=1}^{m-1} p_i = 1, p_i \geq 0)$. *If the s.v. Z=X+Y (mod m) is uniformly distributed and m is a prime number, at least one of the two s. v. X and Y is uniformly distributed.*

1 Introduction

In today's world the need to protect vocal and written communication between individuals, institutions, entities and commercial agencies is ever present and growing. Digital communication has, in part, been integrated into our social life. For many, the day begins with the perusal of e-mail and the tedious task of eliminating spam and other messages we do not consider worthy of our attention. We turn to the internet to read newspaper articles, to see what's on at the cinema, to check flight arrivals, the telephone book, the state of our checking account and stock holdings, to send and receive money transfers, to shop on line, for students' research and for many other reasons. But the digital society must adequately protect communication from intruders, whether persons or institutions which attack our privacy. Cryptography (hidden), the study and creation of secret writing systems in numbers or codes, is essential to the development of digital communication which is absolutely private insofar as being impossible to be read by anyone to whom it is not addressed. Cryptography seeks to study and create systems for ciphering and to verify and authenticate the integrity of data. One must make the distinction between cryptanalysis, the research of methods an "enemy" might use to read the messages of others and cryptography. Cryptography and cryptoanalysis are what make up cryptology.

Until the 1950s cryptography was essentially used only for military and diplomatic communication. The decryption of German messages by the English and of Japanese messages by the Americans played a very important role in the outcome of the Second World War. The great mathematician Alan Touring made an essential contribution to the war effort with his decryption of the famous Enigma machine which was considered absolutely secure by the Germans. It was the Poles, however, who had laid the basis for finding its weak link. Cryptography also played a vital role in the Pacific at the battle of Midway Regarding Italy, the naval battles of Punta Stilo and of Capo Matapan were strongly influenced by the interception and decryption of messages.

1.1 Different disciplines in cryptography

There are four disciplines which have important roles in cryptography:

1. Linguistics, in particular Statistical Linguistics
2. Statistics, in particular the Theory of the Tests for the Analysis of Randomness and of Primality and Data Mining
3. Mathematics, in particular Discrete Mathematics
4. The Theory of Information

The technique of Data Mining seems to be of more use in the analysis of a great number of data which are exchanged on a daily basis such as satellite data. Technical developments are largely inter-disciplinary. This suggests that new applications will be found which will, in turn, lead to new queries and problems for the scholars of Number Theory,Modular Arithmetic, Polynomial Algebra, Information Theory and Statistics to apply to cryptography.

Until the 1950s the decryption of messages was based exclusively on statistical methods and specific techniques of cryptography. In substance, the working instruments of cryptography, both for the planning of coding systems and for reading messages which the sender intended remain secret, were statistical methods applied to linguistics. The key to decoding systems using poly-alphabetic substitution and simple and double transposition has always been the analysis of the statistical distribution of graphemes (letters, figures, punctuation marks, etc.). Mathematics was not fundamental to the work of the cryptoanalyst.

Today,with the advent of data processing technology, coding of messages is done by coding machines. The structure of reference is the algebra of Galois (GF(q)). The search for prime numbers, in particular tests of primality, are of notable interest to modern cryptology.

2 Prime Numbers

The questions regarding prime numbers have interested many scholars since the dawn of mathematics. We need only recall Euclid in ancient times and Fermat, Eulero, Legendre, Gauss and Hilbert in the last four hundred years. Gauss, in 1801, in Disquisitiones Arithmeticae, stated that the problem of distinguishing prime numbers from composite numbers and that of the factorization of these composite numbers were among the most important and useful in arithmetics. Moreover, he added, the very dignity of science itself seemed to require that such an elegant problem be explored from every angle which might help clarify it.

The great calculation resources which are today available to scholars all over the world have led many to deal with questions relative to primes and some to try and falsify certain conjectures. Numerous are the web sites devoted

Volume : 5 | Issue : 9 | September 2015 | ISSN - 2249-555X

to these numbers.

The most noteworthy fact of this situation is that information arrives on the web in real time, not only in print and these are among the most frequented sites. This leads many to confront questions regarding primes which are of limited importance.

A form of emulation is stimulated in which we see many universities in the entire world, but particularly the United States, make great efforts to find a new prime and so become the "leader of the pack", if only for a short while as with setting a record in a sport. This happened, and is happening in the efforts to find the largest known prime to which some universities devote massive calculation resources for many years as occurred with the confirmation of the famous theorem of four colors in postal zones at the University of Illinois and the proof that the 23rd Mersenne number is prime. When speaking of research in prime numbers reference is often made to possible applications in cryptography and in particular cryptographic systems with an RSA public key. The RSA system is based on the choice of two primes of sufficient size and on the relations introduced by Eulero in 1700.

REFERENCE Agrawal, M., Kayal, N., & Saxena, N. (2004). Primes in p. Annals of Mathematics, 160, 781–793. | Goldwasser, S., & Kilian, J. (1986) Almost all primes can be quickly certified. In Proceedings | of the eighteenth annual ACM symposium on Theory of Computing (pp. 316–329). New York: | ACM Press. | Pomerance, C., Selfridge, J. L., & Wagstaff, Jr., S. S. (1980). The pseudoprimes to 25 _ 109. | Mathematics of Computation, 35, 1003–1026. | Rizzi, A. (1990). Some theorem on the sum modulo m of two independent random variables. | Metron, 48, 149–160. | Scozzafava, P. (1991). Sum and difference modulo m between two independent random variables. | Metron, 49, 495–511. | |