# Implementasi Kunci Asimetris pada Teknik Kriptografi Permutasi Chaotic Multiputaran = Implementation of Asymmetric Key in Multicircular Chaotic Permutation Cryptography Technique

Aria Lesmana, author



---

Abstrak

Pengamanan data digital bertujuan untuk mencegah bocornya isi informasi dalam sebuah komunikasi maupun penyimpanan. Pengamanan data baik dalam komunikasi maupun penyimpanan dapat dicapai menggunakan sebuah teknik kriptografi. Dalam sistem digital, kriptografi sudah umum diterapkan secara simetris dan asimetris. Dalam penelitian ini, digunakan sistem kriptografi yang belum diimplementasi secara luas, yaitu Chaos Cryptography, sistem kriptografi yang menerapkan teori sifat Chaos dalam matematika. Penelitian ini membahas penerapan enkripsi menggunakan teknik kriptografi simetris berbasis permutasi yang dinamakan Permutasi Chaotic Multiputaran (PCMP) untuk diimplementasikan sebagai kriptografi asimetris. PCMP merupakan algoritma permutasi himpunan yang menggunakan perputaran elemen untuk menggeser dan mengacak urutannya menggunakan kunci yang dibuat dengan syarat matematis khusus yang menghasilkan sifat chaotic. Sifat chaos teknik PCMP didapat dari penerapan matematis pembuatan kuncinya yang menggunakan aturan basis modulus dan KPK pada setiap elemen dari sebuah set barisan bilangan bulat positif menurut nilainya dalam urutan sebelum dikalkulasikan dengan seed input, hal ini juga menghasilkan nilai berbeda pada ukuran kunci berbeda walaupun nilainya tetap, sehingga memungkinkan sifat pengacakan yang memenuhi syarat sifat chaotic. Teknik PCMP pada dasarnya berupa kriptografi simetris sehingga menggunakan satu kunci dan dua algoritma berbeda untuk melakukan enkripsi dan dekripsi, tetapi sebagai teknik permutasi algoritma tersebut mengubah urutan sebuah himpunan tanpa mengubah komposisinya, karena itu algoritma PCMP juga dapat mengembalikan himpunan yang dipermutasi ke susunan semula menggunakan fungsi yang sama dengan kombinasi kunci yang cocok. Dalam penelitian tesis ini, diusulkan sebuah metode untuk menghasilkan pasangan kunci asimetris dari teknik PCMP, dengan merancang sebuah algoritma yang memungkinkan untuk membuat kunci dari pasangan suatu himpunan dengan hasil permutasi PCMPnya, dapat dihasilkan sebuah pasangan kunci untuk enkripsi dan dekripsi secara terpisah. Algoritma Pencari Kunci PCMP berfungsi mencari kunci PCMP yang dapat menghasilkan permutasi dari sebuah himpunan awal ke himpunan lain yang berisi nilai elemen sama dengan susunan berbeda. Algoritma ini menghasilkan kunci pasangan asimetris dengan mencari kunci PCMP yang dapat mengubah hasil permutasi kembali ke susunan awalnya, melalui pengujian iteratif dengan algoritma enkripsi dari teknik PCMP, yaitu PCMP Mengecil (PCMP-K). Kunci pasangan yang dihasilkan dapat mempermutasi himpunan hasil enkripsi PCMP kembali ke bentuk awal menggunakan fungsi yang sama. Dalam implementasinya, pasangan kunci asimetris PCMP dapat dihasilkan dengan mencari kunci pembalik untuk hasil permutasi kunci buatan generator kunci PCMP dasar, atau dari sepasang himpunan acak yang merupakan permutasi satu sama lain. Syarat untuk pembuatan kunci pasangan PCMP ini adalah himpunan awal untuk pencarian kunci harus terdiri dari elemen dengan nilai unik tanpa duplikat. Perbedaan metode kunci asimetris PCMP dengan implementasi PCMP dasar adalah penggunaan fungsi tunggal untuk enkripsi dan dekripsi, yang dapat menyederhanakan dan mempercepat proses kriptografi, melalui penggunaan algoritma PCMP Mengecil sebagai fungsi enkripsi yang juga berperan sebagai fungsi dekripsi menggunakan pasangan kunci yang

dihasilkan. Dari penggunaan PCMP Mengecil sebagai fungsi kriptografi tunggal didapat peningkatan performa pada waktu dekripsi sebesar 75.87%. Selain itu, hasil enkripsi dari kunci pasangan menghasilkan tingkat kerandoman lebih baik dilihat dari hasil pengukuran Entropi, Chi-Square, Arithmetic Mean, Monte Carlo untuk Pi dan Serial Correlation.

.....Digital data security aims to prevent the leakage of information content in a communication or storage. Data security both in communication and storage can be achieved using a cryptographic technique. In digital systems, cryptography is generally applied symmetrically and asymmetrically. In this study, a cryptographic system that has not been widely implemented is used, namely Chaos Cryptography, a cryptographic system that applies the theory of Chaos properties in mathematics. This study discusses the application of encryption using a permutation-based symmetric cryptography technique called Multicircular Chaotic Permutation (PCMP) to be implemented as asymmetric cryptography. PCMP is a set permutation algorithm that uses rotating elements to shift and scramble the order using a key that is created with special mathematical conditions that produce chaotic properties. The chaotic nature of the PCMP technique is derived from the mathematical application of key generation that uses the basic modulus and LCM rules on each element of a set of positive integer sequences according to their values in the order before being calculated with the input seed, this also results in different values at different key sizes even though the values are fixed. , thus enabling randomization properties that meet the chaotic properties condition. The PCMP technique is basically symmetric cryptography so that it uses one key and two different algorithms to perform encryption and decryption, but as a permutation technique the algorithm changes the order of a set without changing its composition, therefore the PCMP algorithm can also return the permuted set to its original arrangement using the function which is the same as the matching key combination. In this thesis research, a method is proposed to generate asymmetric key pairs from PCMP technique, by designing an algorithm that allows to generate a key from a set pair with the PCMP permutation result, can generate a key pair for encryption and decryption separately. The PCMP Key Finder Algorithm functions to find PCMP keys that can produce permutations from an initial set to another set containing the same element values with different arrangements. This algorithm generates an asymmetric key pair by looking for a PCMP key that can change the permutation result back to its initial arrangement, through iterative testing with an encryption algorithm from the PCMP technique, namely Shrinking PCMP (PCMP-K). The resulting key pair can permute the resulting set of PCMP encryption back to its original form using the same function. In its implementation, PCMP asymmetric pair key can be generated by finding the reverser key for permutations made by key generated from the basic PCMP key generator, or from a pair of random sets which are permutations of each other. The condition for generating this PCMP key pair is that the initial set for key searches must consist of elements with unique values without duplicates. The difference between the PCMP asymmetric key method and the basic PCMP implementation is the use of a single function for encryption and decryption, which can simplify and speed up the cryptographic process, through the use of the Shrinking PCMP algorithm as an encryption function which also acts as a decryption function using the generated key pair. By using Shrinking PCMP as a single cryptography function, the performance increase in decryption time is 75.87%. In addition, the encryption results from the paired keys produce a better level of randomness seen from the results of the Entropy, Chi-Square, Arithmetic Mean, Monte Carlo for Pi and Serial Correlation measurements.