Metode pollard rho dan aplikasinya pada penyelesaian IFP (Integer Factorization Problem) dan ECDLP (Elliptic Curve Discrete Logarithm Problem)

Toni Sutomo, author

Abstrak

Tugas Akhir ini memberikan pemaparan tentang penyelesaian masalah pemfaktoran bilangan bulat (integer factorization problem, IFP) dan masalah logaritma diskret dari suatu kurva eliptik (elliptic curve discrete logarithm problem, ECDLP) dengan menggunakan metode Pollard Rho. Kedua masalah tersebut merupakan dasar keamanan sistem kriptografi kunci publik (public key cryptography, PKC). Ide dasar metode Pollard Rho dalam menyelesaikan IFP adalah dengan mendapatkan suatu faktor dari sebuah bilangan n dengan memanfaatkan sifat pembagi yaitu dengan hanya mengetahui bahwa n mempunyai pembagi tanpa harus mengetahui apa pembagi itu. Sedangkan dalam menyelesaikan ECDLP, ide dasarnya adalah membuat barisan elemen dalam medan berhingga dari kurva eliptik yang bersangkutan. Elemen awal dipilih secara random, kemudian elemen berikutnya dibuat menggunakan pemetaan iteratif. Untuk himpunan berhingga, barisan tersebut menjadi periodik. Setelah sejumlah iterasi akan diperoleh elemen yang sama dan dapat diterapkan metematika diskret untuk menyelesaikannya. Implementasi dilakukan dengan bahasa pemrograman Java 2 SDK Standard Edition versi 1.4.2. Pengujian IFP dilakukan pada bilangan bulat dengan ukuran sampai 120 bit menggunakan komputer dengan sistem operasi Windows XP Professional, prosesor 1.5 GHz Intel Pentium 4, dan memori 256 MB SDRAM. Sedangkan pengujian ECDLP dilakukan pada kurva eliptik dalam medan berhingga Fp dengan order sampai 35 bit menggunakan komputer dengan sistem operasi Windows XP Professional, prosesor 1.7 GHz Intel Pentium 4, dan memori 256 MB DDRAM.. Hasil pengujian menunjukkan bahwa kompleksitas waktu metode Pollard Rho dalam menyelesaikan IFP dan ECDLP sesuai perkiraan teoretis dengan akurasi sekitar 85% untuk IFP dan sekitar 91% untuk ECDLP. Untuk masalah praktis dibutuhkan waktu yang masih sangat besar. Semakin lama waktu yang dibutuhkan berarti keamanan sistem kripto dengan kunci publik berdasarkan IFP dan ECDLP semakin baik.