INTISARI

PENYELESAIAN MASALAH LOGARITMA DISKRIT PADA $\mathbb{Z}_p^*$

Oleh

NABILA PRATIWI

16/394176/PA/17267

Keamanan dari sistem kripto El-Gamal terletak pada fungsi enkripsi dan fungsi dekripsinya yang memanfaatkan nilai logaritma diskrit dari kunci publik β. Beberapa metode yang dapat digunakan untuk menyelesaikan masalah logaritma diskrit pada $\mathbb{Z}_p^*$ dengan p bilangan prima antara lain algoritma Pohlig-Hellman, metode *index calculus* dan metode yang memanfaatkan bilangan *smooth* atas ± 1 pada $\mathbb{Z}_p^*$. Tupel-4 (a, b, c, d) di $\mathbb{Z}_p^*$ dikatakan bilangan *smooth* atas ± 1 jika memenuhi $ab \equiv 1 \ (mod\ p)$, $cd \equiv 1 \ (mod\ p)$, $ac \equiv -1 \ (mod\ p)$ dan $bd \equiv -1 \ (mod\ p)$. Terdapat dua metode yang memanfaatkan bilangan *smooth* atas ± 1 yaitu Algoritma I dan Algoritma II. Dari keempat metode tersebut diperoleh bahwa algoritma Pohlig-Hellman membutuhkan waktu yang lebih singkat dalam menyelesaikan masalah logaritma diskrit pada $\mathbb{Z}_p^*$ dibandingkan dengan tiga metode lainnya.

Kata kunci : masalah logaritma diskrit di $\mathbb{Z}_p^*$, algoritma Pohlig-Hellman, metode *index calculus*, bilangan *smooth* atas ± 1.

ABSTRACT

A SOLUTION OF DISCRETE LOGARITHM PROBLEM OVER $\mathbb{Z}_p^*$

By

NABILA PRATIWI

16/394176/PA/17267

The security of El-Gamal cryptosystem lies on the encryption and decryption function which use the discrete logarithm value of public key β. Several methods that can be used to solve the discrete logarithm problem in $\mathbb{Z}_p^*$ with prime number p are the Pohlig-Hellman algorithm, index calculus method, and method that use the smooth number of ± 1 in $\mathbb{Z}_p^*$. The 4-tuple (a, b, c, d) in $\mathbb{Z}_p^*$ is called smooth number of ± 1 if $ab \equiv 1 \ (mod\ p)$, $cd \equiv 1 \ (mod\ p)$, $ac \equiv -1 \ (mod\ p)$, and $bd \equiv -1 \ (mod\ p)$. There are two methods which use those characteristics, namely Algorithm I and Algorithm II. Among those methods, the Pohlig-Hellman algorithm is quicker in solving the discrete logarithm problem on $\mathbb{Z}_p^*$ in comparison with the other three methods.

Keywords : discrete logarithm problem in $\mathbb{Z}_p^*$, Pohlig-Hellman algorithm, *index calculus* method, smooth number of ± 1.