# Modifikasi Elliptic Curve Digital Signature Algorithm untuk Mencegah Eksploitasi ECDSA Weak Randomness dan Rho Method Attack = A modification of Elliptic Curve Digital Signature Algorithm to Prevent ECDSA Weak Randomness Exploitations and the Rho Method Attack

Amira Zahra, author



---

Abstrak

Elliptic Curve Digital Signature Algorithm (ECDSA) adalah algoritma penandatanganan digital yang menggunakan elliptic curve. ECDSA terdiri dari tiga tahapan, pembentukan kunci, pembentukan tanda tangan digital, dan algoritma verifikasi tanda tangan digital. ECDSA digunakan pada transaksi dengan Bitcoin. Ada penelitian terkait ECDSA weak randomness yang dapat dieksploitasi untuk mengungkap kunci privat pengguna. ECDSA weak randomness adalah melakukan generating pada bilangan random yang tidak aman secara kriptografi. Ada beberapa modifikasi yang dilakukan untuk mencegah eksploitasi ECDSA weak randomness. Namun, modifikasi tersebut rentan terhadap Rho method attack yang bisa memecahkan Elliptic Curve Discrete Logarithm Problem (ECDLP). Jika ECDLP diselesaikan, kunci privat pengguna dapat terungkap. Oleh karena itu, pada penelitian ini, akan dikonstruksi ECDSA yang tahan terhadap eksploitasi ECDSA weak randomness dan Rho method attack dengan menggunakan tiga kunci privat. .....Elliptic Curve Digital Signature Algorithm (ECDSA) is a digital signature algorithm that utilizes an elliptic curve. ECDSA consists of three steps, which are key generation, signature generation, and verification algorithm. ECDSA is used on Bitcoin transactions to generate the user’s public key, private key, and signature, and also to verify a Bitcoin user’s signature. There are some researches on ECDSA weak randomness which can be exploited by attackers to reveal the user’s private key, and causes thefts of the user’s money. ECDSA weak randomness is generating a random number that is not cryptographically secure. Some modifications of ECDSA to overcome this problem have been done, such as generating the digital signature by using two private keys. Although those modified algorithms overcome ECDSA weak randomness exploitations, it is not resistant to the Rho method attack which can solve elliptic curve discrete logarithm problem (ECDLP). In case ECDLP can be solved, the user’s private key can be revealed. Therefore, in this research, we modify an ECDSA algorithm that overcomes the exploitation of ECDSA weak randomness and is also resistant to the Rho method attack by using three private keys.