

RINGKASAN

Nomor Pokok Wajib Pajak (NPWP) merupakan 20 karakter kode unik bersifat rahasia yang hanya dimiliki Wajib Pajak yang bersangkutan guna melakukan transaksi perpajakan. Banyaknya Wajib Pajak yang menggunakan NPWP orang lain dalam melakukan kegiatan usahanya menyebabkan NPWP menjadi aspek yang sangat penting dijaga kerahasiaan dan keaslian datanya. Oleh karena itu, diperlukan solusi yang bisa membantu agar informasi yang diperlukan bersifat aman. Kriptografi merupakan ilmu menulis kode secara rahasia menggunakan model matematika tertentu. Penelitian ini membahas tentang enkripsi NPWP menggunakan kombinasi algoritma *One Time Pad (OTP)* dan operasi *Exclusive-OR (XOR)*. Proses enkripsi dilakukan dengan cara membangkitkan bilangan acak untuk algoritma *OTP*, setelah itu dilanjutkan dengan pengoperasian *XOR*. Kunci pada enkripsi *XOR* dihasilkan dari algoritma pembangkit bilangan acak Blum-Blum Shub. Kunci enkripsi yang dihasilkan sebanyak jumlah karakter plainteks. Sehingga kunci enkripsi yang digunakan setiap karakter akan berbeda-beda dan tidak terjadi perulangan. Maka dari itu, *ciphertext* yang dihasilkan dari proses enkripsi menggunakan algoritma *OTP* dan operasi *XOR* lebih rumit dan lebih susah untuk dipecahkan oleh kriptanalis.

SUMMARY

Nomor Pokok Wajib Pajak (NPWP) is the 20 distinct code characteristics that are confidential only to the taxpayer when it comes to making tax transactions. The many tax payers who use NPWP others in their business activities make NPWP a very important aspect of maintaining confidentiality and the authenticity of their data. Therefore, solutions are needed that can be used to make the necessary information secure. Cryptography involves the secret science of code writing using certain mathematical models. The study discusses NPWP encryption using a combination algorithm One Time Pad (OTP) and an operation Exclusive-OR (XOR). The encryption process involves generating random numbers for an OTP algorithm, after which it is followed by an XOR operation. The key on XOR encryption is generated from an algorithm generating random numbers Blum Blum Shub. Encryption keys generated as much as the number of plaquic characters. So the encryption keys used by each character would vary and not occur again. Therefore, ciphertext results from an encrypted process using an OTP algorithm and an XOR operation more complicated and more difficult to decipher by crypts.