

INTISARI

Salah satu tes pada penerimaan POLRI adalah *shuttle run*, proses tes tersebut masih manual dan rentan terhadap keamanan data. Penulis mendapat ide merancang dan membuat suatu alat *wireless sensor network*, alat tersebut menggunakan sensor *LDR* dan *dioda* laser sebagai masukan data yang kemudian akan diproses oleh sistem arduino yang dikirim oleh *xbee* dalam bentuk pesan terenkripsi/disamarkan, kemudian akan ditampung pada *database*. Pengiriman data menggunakan komunikasi serial, permasalahan berikut ini diperlukan suatu metode adalah kriptografi. Kriptografi algoritme *Data Encryption Standard (DES)* dianggap algoritme yang paling efektif dan baik karena memiliki waktu proses enkripsi dekripsi dengan cepat dan aman. Kriptografi algoritme DES menggunakan *cipher* blok tiap proses 8 karakter, data yang dikirim dalam bentuk *char* pada *ASCII*. Rerata *Computation time* proses enkripsi, dekripsi *DES* adalah 2.200 *us/char*, 280 *us/char* dan *TDES* adalah 6.600 *us/char*, 960 *us/char*. Algoritme *TDES* lebih membutuhkan waktu yang lebih lama dan lebih aman dari pada algoritme *DES* karena menggunakan panjang kunci 8 karakter sedangkan *TDES* 24 karakter, dengan 3 kali putaran *DES*.

Kata Kunci: *wireless sensor network*, kriptografi, algoritme, *DES*, *TDES*.

ABSTRACT

Shuttle run is one of the entrance tests in POLRI, it still manual and vulnerable to data security. The author got idea of the design wireless sensor network devices, this tool uses LDR sensor and laser diode as input data which will be processed by arduino system sent by Xbee in the form of message encrypted/ disguised, it will be put in the database. This data transmission using serial communication, the problem required a cryptography method. The Data Encryption Standard (DES) algorithm cryptography is considered with the most effective and good algorithm because it has the time of encryption process of decryption quickly and safely. DES algorithm cryptography uses block cipher per 8 character in process, data sent in char form on ASCII. The encryption process averages with computation time, DES is 2,200 us/char, 280 us/char and TDES is 6,600 us/char, 960 us/char. The TDES algorithm takes more than and safer than the DES algorithm because uses 8 character key length while the TDES is 24 characters, with 3 rounds of DES.

Keywords: *wireless sensor network, cryptography, algorithm, DES, TDES.*