

ABSTRAK

Smart home merupakan tempat tinggal yang didalamnya terdapat gabungan beberapa alat yang memiliki kemampuan atau kemahiran tertentu bergantung pada aplikasinya. Enkripsi belakangan ini menjadi topik yang hangat dibicarakan. Enkripsi dapat memodifikasi informasi dengan cara mengacak atau mengkodekan data yang kita kirim agar tidak bisa terbaca oleh siapapun, kecuali orang-orang yang memiliki kunci khusus (key) untuk mengubah informasi itu kembali ke bentuk aslinya agar bisa dibaca. Saat ini pengguna internet atau ponsel dan perusahaan banyak dijadikan target kejahatan cyber.

Salah satu pendekatan yang diyakini memiliki kemampuan untuk mengatasi kejahatan cyber yaitu teknik kriptografi. Tujuan kriptografi sendiri menyediakan metode untuk mencegah serangan pada data. Enkripsi homomorphic dapat menjadi salah satunya teknik kriptografi untuk hal pengamanan data. Karakteristik homomorphic sendiri pada tahapan encryption dan decryption Algoritma Schmidt-Takagi dapat membuat ciphertext dapat dikerjakan secara komputasi meskipun belum didekripsi terlebih dahulu. Komputasi yang didukung biasanya berupa penambahan, pengurangan, atau bahkan perkalian dengan konstanta tertentu.

Hasil akhir pada pengerjaan Tugas Akhir ini yaitu waktu yang dibutuhkan untuk menghasilkan waktu rata-rata data encrypt yaitu 0,0436362265201993 detik. Sedangkan waktu pada data decrypt diperoleh yaitu 0,0016459010282875 detik. Hasil waktu rata-rata ini didapatkan dari panjang key 256 bit.

Kata Kunci: Homomorfik, Schmidt-Takagi, Enkripsi, Dekripsi