# ABSTRACT

A smart home is a place to live in which there is a combination of several tools that have certain abilities or skills depending on the application. Encryption has recently become a hot topic of discussion. Encryption can modify information by scrambling or encoding the data we send so that it cannot be read by anyone, except for people who have a special key (key) to change the information back to its original form so that it can be read. Currently, many internet or cell phone users and companies are being targeted by cyber crimes.

One approach that is believed to have the ability to overcome cyber crime is cryptography techniques. The purpose of cryptography itself is to provide a method to prevent attacks on data. Homomorphic encryption can be one of the cryptographic techniques for data security. Homomorphic characteristics themselves in the encryption and decryption stages. The Schmidt-Takagi algorithm can make the ciphertext workable computationally even though it has not been described beforehand. The supported computations are usually addition, subtraction, or even multiplication with certain constants.

The final result of this final project is the time needed to generate the average data encrypt time is 0.0436362265201993 seconds. While the time to decrypt the data obtained is 0.0016459010282875 seconds. The result of this average time is obtained from the key length of 256 bits.


**Key Words:** *Homomorphic, Schmidt-Takagi, Encryption, Decryption*