INTISARI

T-FUNCTION SEBAGAI GENERATOR KEYSTREAM PADA STREAM CIPHER

Oleh

RIANTI AMANDA SAFITRI

12/331072/PA/14437

Kriptografi merupakan sarana untuk melindungi informasi pribadi dari akses pihak luar yang tidak sah. Dalam stream ciphers, plainteks dienkripsi secara bit per-bit. Dalam mengenkripsi plainteks yang akan dikirimkan, kunci diolah ke dalam algoritma yang disebut *pseudorandom keystream generator* untuk menghasilkan *keystream*. *"Keystream"* ini kemudian dienkripsi untuk menghasilkan cipherteks.

Linear Feedback Shift Register (LFSR) sangat umum digunakan untuk menghasilkan *keystream*. Alexander Klimov dan Adi Shamir memperkenalkan *T-function* sebagai penghasil *keystream* yang lebih baik. Pada skripsi ini akan difokuskan menganalisa sifat *T-function* sebagai penghasil *keystream* berdasarkan *Golomb's Randomness Postulates*.

Kata kunci: Stream cipher, generator bilangan Pseudorandom, register geser Linear feedback, T-function

ABSTRACT

T-FUNCTION AS KEYSTREAM GENERATOR ON STREAM CIPHER

By

RIANTI AMANDA SAFITRI

12/331072/PA/14437

Cryptography is tool to protect private information from unauthorized external access. In stream ciphers, plaintext is encrypted by bit per bit. The plaintext are encrypted, the key is processed into an algorithm called *pseudorandom keystream generator* to generate a *keystream*. This *keystream* is then encrypted to generate ciphertext.

Linear Feedback Shift Register (LFSR) are usually used to generate *keystream*. Alexander Klimov and Adi Shamir introduced T-function as a better *keystream* generator. In this thesis, it will be focused to analyze the properties of *T-function* as a *keystream* generator based on *Golomb's Randomness Postulates*

Keyword : *Stream cipher*, *Pseudorandom number generator*, *Linear feedback shift register*, *T-function*