ANALISIS KETAHANAN ALGORITMA ENKRIPSI KTANTAN64 TERHADAP SERANGAN BERBASIS *DEEP LEARNING*

FERDY ALIANSYAH HASYIM

PROGRAM STUDI MATEMATIKA
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2026

PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa skripsi dengan judul "Analisis Ketahanan Algoritma Enkripsi KTANTAN64 terhadap Serangan Berbasis *Deep Learning*" adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Juli 2026

Ferdy Aliansyah Hasyim
G5401221090

ABSTRAK

FERDY ALIANSYAH HASYIM. Analisis Ketahanan Algoritma Enkripsi KTANTAN64 terhadap Serangan Berbasis *Deep Learning*. Dibimbing oleh MOCHAMAD TITO JULIANTO dan MOHAMAD KHOIRUN NAJIB.

Enkripsi merupakan proses transformasi pesan asli (*plaintext*) menjadi teks sandi (*ciphertext*) untuk menjaga kerahasiaan informasi sehingga ketahanan algoritmanya perlu dievaluasi. Penelitian ini bertujuan mengembangkan model *deep learning* untuk mensimulasikan serangan pemulihan *plaintext* tanpa kunci pada algoritma KTANTAN64 dan menganalisis ketahanan algoritma tersebut berdasarkan jumlah ronde enkripsinya. Metode *deep learning* yang diusulkan menggunakan arsitektur *Bidirectional Long Short-Term Memory* (BiLSTM) dengan *Gated Linear Unit* (GLU) serta teknik bipolarisasi data. Hasilnya, model mencapai *Bit Accuracy Probability* (BAP) 91,09% dan *Character Accuracy Probability* (CAP) 66,27% pada 50 ronde enkripsi yang memiliki tingkat pengacakan 24,26%. Pada ronde maksimal (254 ronde), pengacakan menyentuh kriteria ideal 50,01% sehingga BAP turun ke angka 89,91% dan CAP tertahan di 65,05%. Hal ini membuktikan peningkatan efek pengacakan menurunkan performa model. Dengan demikian, algoritma KTANTAN64 tangguh terhadap serangan pemulihan *plaintext*, terutama pada jumlah ronde maksimal.

Kata kunci: *avalanche effect*, *deep learning*, kriptanalisis neural, KTANTAN64, pemulihan *plaintext*.

ABSTRACT

FERDY ALIANSYAH HASYIM. Vulnerability Analysis of the KTANTAN64 Encryption Algorithm Against Deep Learning-Based Attacks. Supervised by MOCHAMAD TITO JULIANTO and MOHAMAD KHOIRUN NAJIB.

Encryption is the process of transforming an original message (plaintext) into ciphertext to maintain information confidentiality, making it necessary to evaluate its algorithmic resistance. This study aims to develop a deep learning model to simulate plaintext recovery attacks on the KTANTAN64 algorithm and analyze the algorithm's resistance based on the number of its encryption rounds. The proposed deep learning method employs a Bidirectional Long Short-Term Memory (BiLSTM) architecture with a Gated Linear Unit (GLU) and a data bipolarization technique. The model achieves a Bit Accuracy Probability (BAP) of 91.09% and a Character Accuracy Probability (CAP) of 66.27% at 50 encryption rounds, which exhibit an avalanche effect of 24.26%. The maximum rounds (254 rounds), the avalanche reaches the ideal criterion of 50.01%, causing the BAP to drop to 89.91% and the CAP to plateau at 65.05%. This proves the increase in the avalanche effect degrades the performance of the model. Thus, the KTANTAN64 algorithm is robust against plaintext recovery attacks, especially at the maximum number of rounds.

Keywords: *avalanche effect*, *deep learning*, KTANTAN64, *neural cryptanalysis*, *plaintext recovery*.

ANALISIS KETAHANAN ALGORITMA ENKRIPSI KTANTAN64 TERHADAP SERANGAN BERBASIS *DEEP LEARNING*

FERDY ALIANSYAH HASYIM

Skripsi
sebagai salah satu syarat untuk memperoleh gelar
Sarjana Matematika pada
Program Studi Matematika

PROGRAM STUDI MATEMATIKA
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2026

Tim Penguji pada Ujian Skripsi:
Prof. Dr. Ir. Sri Nurdiati, M.Sc.

Judul Skripsi : Analisis Ketahanan Algoritma Enkripsi KTANTAN64 terhadap Serangan Berbasis *Deep Learning*
Nama : Ferdy Aliansyah Hasyim
NIM : G5401221090

Disetujui oleh

Pembimbing 1:
Mochamad Tito Julianto, S.Si., M.Kom.

Pembimbing 2:
Mohamad Khoirun Najib, S.Si., M.Mat.

Diketahui oleh

Ketua Program Studi:
Dr. Donny Citra Lesmana, S.Si., M.Fin.Math.
NIP 197902272005011001

Tanggal Ujian:
13 Juli 2026

Tanggal Lulus:

PRAKATA

Puji dan syukur penulis panjatkan kepada Allah *subhanaahu wa ta'ala* atas segala karunia-Nya sehingga karya ilmiah ini berhasil diselesaikan. Tema yang dipilih dalam penelitian yang dilaksanakan sejak bulan September 2025 sampai bulan Juli 2026 ini ialah kriptanalisis neural, dengan judul "Analisis Ketahanan Algoritma Enkripsi KTANTAN64 terhadap Serangan Berbasis *Deep Learning*". Terima kasih penulis ucapkan kepada:

1. Alm. Bapak Masrur dan Ibu Peni serta Fahri selaku kedua orang tua dan kakak yang selalu menyertai dalam bentuk kasih sayang, doa, dan dukungan baik dari finansial maupun emosional.
2. Bapak Mochamad Tito Julianto, S.Si., M.Kom. selaku dosen pembimbing 1, Bapak Mohamad Khoirun Najib selaku dosen pembimbing 2, dan Ibu Prof. Dr. Ir. Sri Nurdiati, M.Sc. selaku dosen penguji yang telah meluangkan waktunya untuk membimbing, memotivasi, dan memberikan ilmu kepada penulis selama melakukan penelitian dari awal sampai akhir.
3. Seluruh dosen dan tenaga kependidikan Program Studi S1 Matematika SSMI IPB yang telah memberikan ilmu dan bantuannya selama masa perkuliahan.
4. Zelisha, Abel, Zaidan, dan sahabat-sahabat terdekat penulis lainnya yang mewarnai masa perkuliahan dan selalu mendengar keluh kesah serta turut memberikan kritik serta sarannya dalam penyempurnaan karya ilmiah ini.
5. Kelompok MBL, Warga PSDM, Guild keilmuan, dan REPO yang telah memberikan banyak pengalaman dan kesan berharga semasa perkuliahan.
6. Teman-teman Matematika 59 yang menemani dan mendukung penulis selama perkuliahan dan penyusunan karya ilmiah ini.
7. Pihak-pihak lain yang telah mendukung penulis dalam bentuk apa pun.

Semoga karya ilmiah ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Juli 2026

Ferdy Aliansyah Hasyim

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN