Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

ANALISIS KINERJA SOLVER DALAM MENYELESAIKAN EKSPRESI BOOLEAN CIPHER S-DES PADA CIPHERTEXT-ONLY-ATTACK

[1]Fritz Gamaliel*, [2] P. Yudi Dwi Arliyanto

[1]Prodi Teknologi Rekayasa Perangkat Lunak, Politeknik META Industri Cikarang, Jalan Inti 1 Blok C1 No 7 Lippo Cikarang Indonesia
[2]Prodi Teknik Industri, Politeknik META Industri Cikarang, Jalan Inti 1 Blok C1 No 7 Lippo Cikarang Indonesia

*e-mail: fritzgamaliel@gmail.com

Abstrak

Ekspresi Boolean dapat digunakan untuk merepresentasikan hubungan logika antara plaintext, kunci, dan ciphertext pada algoritma kriptografi. Penelitian ini bertujuan mengekstrak ekspresi Boolean dari algoritma *Simplified Data Encryption Standard* (S-DES) dan mengevaluasi kinerja beberapa metode *solving* dalam menyelesaikan ekspresi tersebut pada skenario *Ciphertext-Only Attack* (COA). Ekspresi Boolean diekstrak dari proses enkripsi S-DES untuk merepresentasikan hubungan antara bit plaintext, bit kunci, dan setiap bit ciphertext, kemudian direpresentasikan dalam dua bentuk, yaitu *Conjunctive Normal Form* (CNF) dan *Algebraic Normal Form* (ANF). Ekspresi dalam bentuk CNF digunakan sebagai masukan untuk metode *Binary Decision Diagram* (BDD) dan *Boolean Satisfiability* (SAT) menggunakan *modern SAT solver*, sedangkan ekspresi dalam bentuk ANF digunakan untuk metode *Brute Force* dan *Gröbner Basis*. Pada skenario COA, ciphertext diketahui dan setiap metode digunakan untuk mencari kombinasi plaintext dan kunci yang memenuhi ekspresi Boolean hasil ekstraksi. Kinerja masing-masing metode dievaluasi berdasarkan waktu komputasi dan keberhasilannya dalam menemukan solusi. Hasil penelitian diharapkan dapat memberikan perbandingan kinerja berbagai metode *solving* terhadap representasi CNF dan ANF yang diekstrak dari algoritma S-DES.

Kata kunci: boolean expression, brute force, binary decision diagram, sat solver, grobner basis

Abstract

Boolean expressions can be used to represent logical relationships among plaintext, key, and ciphertext in cryptographic algorithms. This study aims to extract Boolean expressions from the Simplified Data Encryption Standard (S-DES) algorithm and evaluate the performance of several solving methods in solving these expressions under a Ciphertext-Only Attack (COA) scenario. Boolean expressions are extracted from the S-DES encryption process to represent the relationships among plaintext bits, key bits, and each ciphertext bit, and are then represented in two forms: Conjunctive Normal Form (CNF) and Algebraic Normal Form (ANF). The CNF expressions are used as inputs for Binary Decision Diagram (BDD) and Boolean Satisfiability (SAT) methods using a modern SAT solver, while the ANF expressions are solved using Brute Force and Gröbner Basis methods. In the COA scenario, the ciphertext is known, and each method is used to find a combination of plaintext and key values that satisfies the extracted Boolean expressions. The performance of each method is evaluated based on computational time and its ability to find a solution. The results are expected to provide a comparison of the performance of various solving methods on CNF and ANF representations extracted from the S-DES algorithm.

Keywords: *boolean expression, brute force, binary decision diagram, sat solver, grobner basis*

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

1 Pendahuluan

Kriptografi dapat direpresentasikan dalam bentuk ekspresi Boolean untuk menggambarkan hubungan antara plaintext, kunci, dan ciphertext. *Simplified Data Encryption Standard* (S-DES) merupakan algoritma kriptografi blok sederhana dengan plaintext dan ciphertext berukuran 8 bit serta kunci berukuran 10 bit, sehingga sesuai digunakan sebagai objek penelitian untuk mengekstrak dan menyelesaikan ekspresi Boolean dari proses enkripsinya. Setiap bit ciphertext dapat direpresentasikan sebagai fungsi Boolean yang bergantung pada bit plaintext dan bit kunci.

Penelitian ini mengekstrak ekspresi Boolean dari proses enkripsi S-DES dalam dua bentuk, yaitu *Conjunctive Normal Form* (CNF) dan *Algebraic Normal Form* (ANF). Representasi CNF digunakan sebagai masukan untuk *Binary Decision Diagram* (BDD) dan *modern SAT solver*, sedangkan representasi ANF digunakan untuk metode *Brute Force* dan *Gröbner Basis*. Seluruh metode diterapkan dalam skenario *Ciphertext-Only Attack* (COA), dengan ciphertext diketahui dan plaintext serta kunci dicari sebagai variabel yang memenuhi ekspresi Boolean hasil ekstraksi.

Penelitian ini bertujuan mengevaluasi kinerja berbagai metode *solving* dalam menyelesaikan ekspresi Boolean yang diekstrak dari S-DES. Evaluasi dilakukan berdasarkan waktu komputasi dan keberhasilan metode dalam menemukan kombinasi plaintext dan kunci yang sesuai dengan ciphertext yang diberikan. Hasil penelitian diharapkan memberikan perbandingan kinerja BDD, *modern SAT solver*, *Brute Force*, dan *Gröbner Basis* dalam menyelesaikan representasi CNF dan ANF pada analisis kriptografi berukuran kecil.

2 Tinjauan Literatur

Penelitian ini membahas ekstraksi ekspresi Boolean dari algoritma kriptografi sebagai representasi hubungan logika antara *plaintext*, kunci, dan *ciphertext*. Ekspresi Boolean yang dihasilkan direpresentasikan dalam bentuk *Conjunctive Normal Form* (CNF) dan *Algebraic Normal Form* (ANF), kemudian diselesaikan menggunakan beberapa metode, yaitu *Binary Decision Diagram* (BDD) dan *Boolean Satisfiability* (SAT) solver untuk CNF, serta *Brute Force* dan *Gröbner Basis* untuk ANF. Berdasarkan fokus tersebut, studi pustaka dilakukan dengan mengkaji penelitian-penelitian terdahulu yang berkaitan dengan ekstraksi dan representasi ekspresi Boolean pada algoritma kriptografi serta penggunaan berbagai metode *solving* untuk menyelesaikan permasalahan Boolean. Kajian terhadap penelitian-penelitian tersebut digunakan untuk mengidentifikasi perkembangan pendekatan yang telah digunakan, karakteristik metode yang diterapkan, serta celah penelitian (*research gap*) yang menjadi dasar pelaksanaan penelitian ini. Hasil studi pustaka disajikan sebagai berikut. Curtis Brigh et al menunjukkan bahwa ketika permasalahan komputasional dimodelkan sebagai formula Boolean dan diselesaikan dengan menggunakan SAT solver [1]. Sahu et al. menerapkan Reduced Ordered Binary Decision Diagram (ROBDD) untuk melakukan kriptanalisis terhadap stream cipher E0 [2]. Ashutosh Dhar Dwivedi et all menerapkan SAT Solver untuk melakukan kriptanalisis terhadap cipher dari kompetisi CAESAR [3]. Michel Dubois dan Eric Filiol menggunakan fungsi Boolean untuk merepresentasikan dan menganalisis struktur AES [4]. Artur Soboń et al memodelkan algoritma RC5 sebagai formula logika proposisional dan menerapkan beberapa SAT solver untuk melakukan kriptanalisis terhadapnya[5]. Yash Makwana et al mengimprove penerapan Binary Decision Diagram (BDD) dalam melakukan kriptanalisis terhadap stream cipher Trivium[6]. Ilya Mironov et al memberikan contoh pertama menerapkan kriptanalisis berbasis SAT Solver terhadap kriptografi primitif non-trivial [7]. Ekaterina Maro memodelkan analisis aljabar terhadap cipher PRESENT sebagai masalah SAT dan menggunakan algoritma DPLL untuk mencari himpunan solusi dari formula Boolean yang dihasilkan [8]. Sylwia Stachowiak et al menerapkan SAT-based cryptanalysis terhadap cipher Salsa20 [9]. Artur Soboń et al menerapkan SAT-based cryptanalysis terhadap cipher ChaCha20 [10]. Sean Simmons menggunakan metode kriptanalis aljabar untuk menyerang Simplified-AES[11]. Orna Grumberg et al menegaskan bahwa urutan variabel merupakan faktor kritis dalam ukuran dan performa BDD serta mengusulkan pendekatan *learning* untuk menemukan urutan variabel [12]. Xu et al menegaskan bahwa tidak ada satu SAT solver yang selalu unggul pada seluruh instance sehingga

This work is licensed under a Creative Commons Attribution 4.0 International License.

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

karakteristik setiap instance dapat digunakan untuk memilih solver yang paling sesuai [13]. Penelitian Fadila Paradise dan Santi Indarjani menggunakan plaintext 01101101 dalam proses mendapatkan 8 persamaan aljabar S-DES [14]. Penelitian Nadya Marta Matanggwan dan Sa'aadah Sajjana Carita salah satunya menggunakan plaintext 01010010 dalam proses mendapatkan 8 persamaan aljabar miniatur S-IDEA [15]. Adapun yang menjadi pembeda antara penelitian ini dengan penelitian-penelitian sebelumnya adalah proses ekstraksi ekspresi Boolean untuk setiap bit keluaran (*ciphertext*) algoritma *Simplified Data Encryption Standard* (S-DES) berdasarkan hubungan logika antara *plaintext*, kunci, dan *ciphertext*. Ekspresi Boolean yang dihasilkan kemudian direpresentasikan dalam bentuk *Conjunctive Normal Form* (CNF) dan *Algebraic Normal Form* (ANF). Ekspresi CNF diselesaikan menggunakan metode *Binary Decision Diagram* (BDD) dan *Boolean Satisfiability* (SAT) solver, sedangkan ekspresi ANF diselesaikan menggunakan metode *Brute Force* dan *Gröbner Basis*. Seluruh metode diterapkan pada skenario *Ciphertext-Only Attack* (COA) dan dibandingkan berdasarkan waktu komputasi serta keberhasilan dalam menemukan kombinasi *plaintext* dan kunci yang memenuhi *ciphertext* yang diberikan.

3 Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental yang diawali dengan tinjauan literatur untuk mengkaji teori terkait algoritma kriptografi Simplified Data Encryption Standard (S-DES), ekspresi Boolean, dan metode penyelesaian menggunakan berbagai solver. Tahapan penelitian meliputi tinjauan literatur, ekstraksi ekspresi Boolean S-DES, proses penyelesaian, serta pengukuran kinerja masing-masing solver pada skenario Ciphertext-Only Attack.

3.1 Ekstraksi Ekspresi Boolean S-DES

Ekstraksi Ekspresi Boolean S-DES dilakukan dengan menghasilkan ekspresi Boolean berdasarkan hubungan antara variabel plaintext, kunci, dan ciphertext pada algoritma S-DES. Ekspresi Boolean yang dihasilkan disesuaikan dengan metode penyelesaian yang digunakan. Representasi Conjunctive Normal Form (CNF) digunakan untuk BDD dan SAT Solver, sedangkan Algebraic Normal Form (ANF) digunakan untuk Brute Force dan Gröbner Basis.

3.2 Pengujian dan Evaluasi Kinerja Solver

Pengujian dilakukan dengan menjalankan setiap solver pada ekspresi Boolean S-DES yang telah dibangkitkan. Kinerja solver dievaluasi berdasarkan waktu eksekusi yang berhasil ditemukan. Hasil pengujian kemudian dibandingkan untuk mengetahui perbedaan kinerja setiap pendekatan dalam menyelesaikan ekspresi Boolean.

4 Hasil dan Pembahasan (or Results and Analysis)

4.1 Ekstraksi Ekspresi Boolean S-DES

Ekspresi Boolean S-DES diekstrak dari proses enkripsi dengan merepresentasikan setiap bit keluaran *ciphertext* sebagai fungsi Boolean yang bergantung pada 8 bit *plaintext* dan 10 bit kunci. Proses tersebut menghasilkan delapan fungsi Boolean, yaitu (F_1) hingga (F_8), yang masing-masing merepresentasikan satu bit keluaran *ciphertext*. Fungsi Boolean yang diperoleh kemudian direpresentasikan dalam dua bentuk, yaitu *Conjunctive Normal Form* (CNF) dan *Algebraic Normal Form* (ANF).

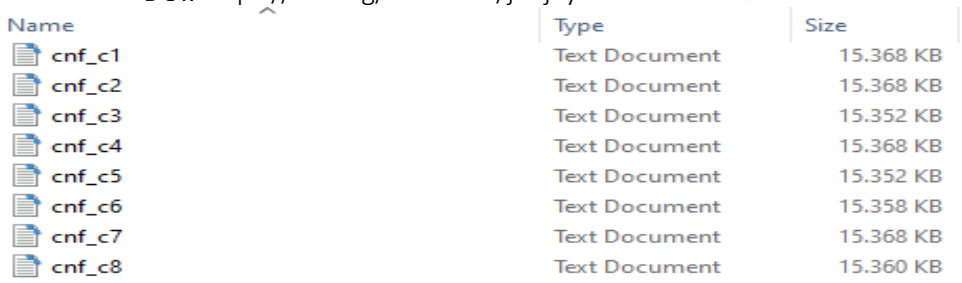
Pada bentuk CNF, setiap fungsi Boolean direpresentasikan sebagai konjungsi (*AND*) dari sejumlah klausa, dengan setiap klausa merupakan disjungsi (*OR*) dari literal. Dengan demikian, diperoleh delapan ekspresi CNF yang merepresentasikan hubungan logika antara *plaintext*, kunci, dan masing-masing bit *ciphertext* S-DES. Karena ukuran ekspresi yang dihasilkan cukup panjang, gambar berikut menunjukkan potongan ekspresi CNF yang diperoleh dari proses ekstraksi untuk (F_1) hingga (F_8).

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678



Name	Type	Size
cnf_c1	Text Document	15.368 KB
cnf_c2	Text Document	15.368 KB
cnf_c3	Text Document	15.352 KB
cnf_c4	Text Document	15.368 KB
cnf_c5	Text Document	15.352 KB
cnf_c6	Text Document	15.358 KB
cnf_c7	Text Document	15.368 KB
cnf_c8	Text Document	15.360 KB

Gambar 1 File CNF Cipher S-DES



Gambar 2 Ekspresi CNF Bit ke-1 Ciphertext S-DES



Gambar 3 Ekspresi CNF Bit ke-2 Ciphertext S-DES



Gambar 4 Ekspresi CNF Bit ke-3 Ciphertext S-DES



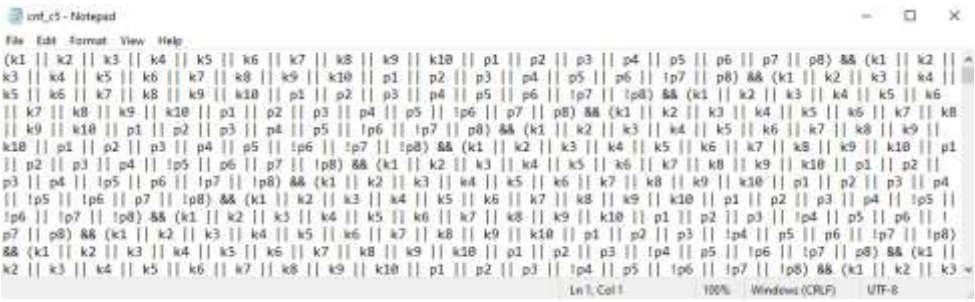
Gambar 5 Ekspresi CNF Bit ke-4 Ciphertext S-DES

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

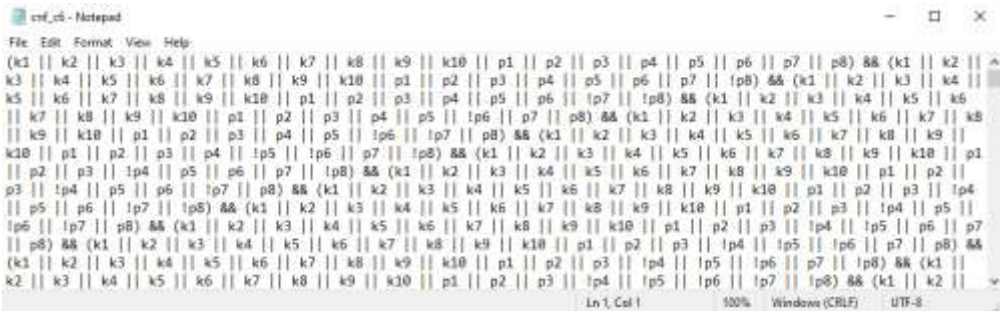
Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678



Gambar 6 Ekspresi CNF Bit ke-5 Ciphertext S-DES



Gambar 7 Ekspresi CNF Bit ke-6 Ciphertext S-DES



Gambar 8 Ekspresi CNF Bit ke-7 Ciphertext S-DES



Gambar 9 Ekspresi CNF Bit ke-8 Ciphertext S-DES

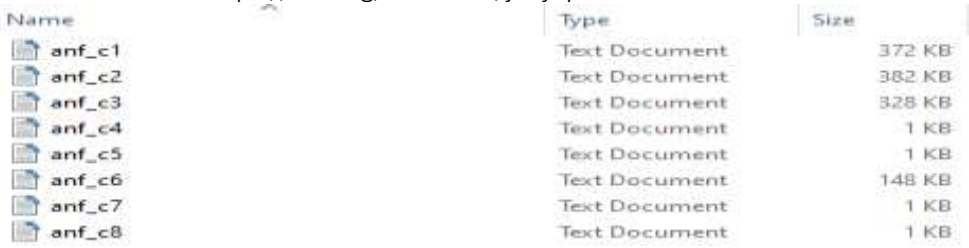
Selain CNF, fungsi Boolean yang sama juga direpresentasikan dalam bentuk ANF. Pada bentuk ini, setiap fungsi dinyatakan sebagai polinomial Boolean dengan operasi penjumlahan modulo 2 (*XOR*) dan perkalian antarvariabel (*AND*). Delapan fungsi (F_1) hingga (F_8) menghasilkan delapan persamaan ANF yang merepresentasikan hubungan antara *plaintext*, kunci, dan *ciphertext*. Karena ekspresi ANF yang dihasilkan juga memiliki ukuran yang cukup panjang, gambar berikut menunjukkan potongan ekspresi ANF yang diperoleh dari proses ekstraksi untuk (F_1) hingga (F_8).

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

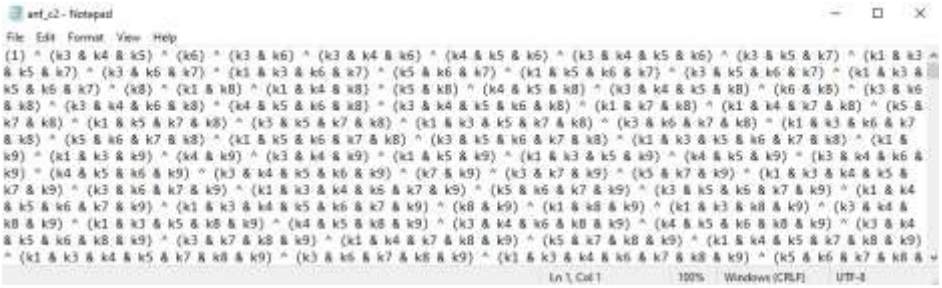


Name	Type	Size
anf_c1	Text Document	372 KB
anf_c2	Text Document	382 KB
anf_c3	Text Document	328 KB
anf_c4	Text Document	1 KB
anf_c5	Text Document	1 KB
anf_c6	Text Document	148 KB
anf_c7	Text Document	1 KB
anf_c8	Text Document	1 KB

Gambar 10 File ANF Cipher S-DES



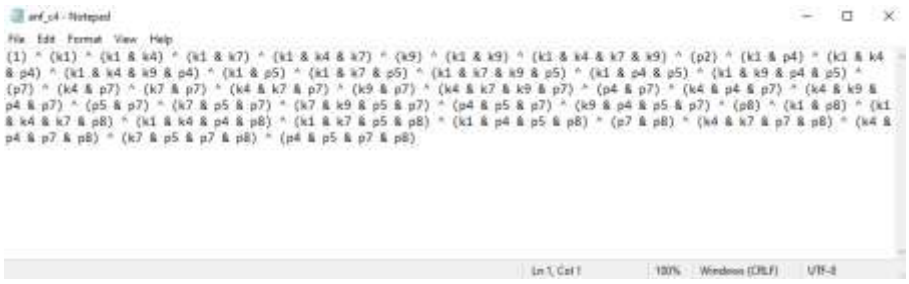
Gambar 11 Ekspresi ANF Bit ke-1 Ciphertext S-DES



Gambar 12 Ekspresi ANF Bit ke-2 Ciphertext S-DES



Gambar 13 Ekspresi ANF Bit ke-3 Ciphertext S-DES



Gambar 14 Ekspresi ANF Bit ke-4 Ciphertext S-DES

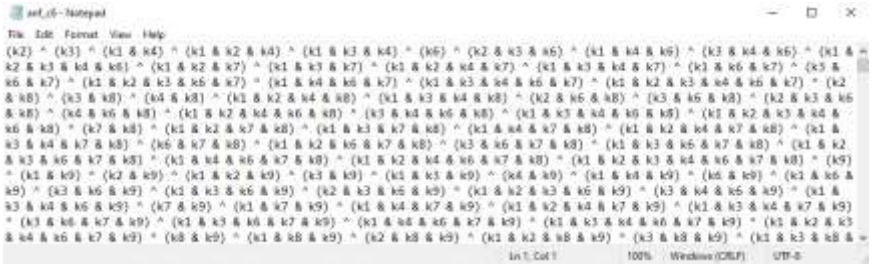
This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59
P-ISSN: 2746-5985
e-ISSN: 2797-0930

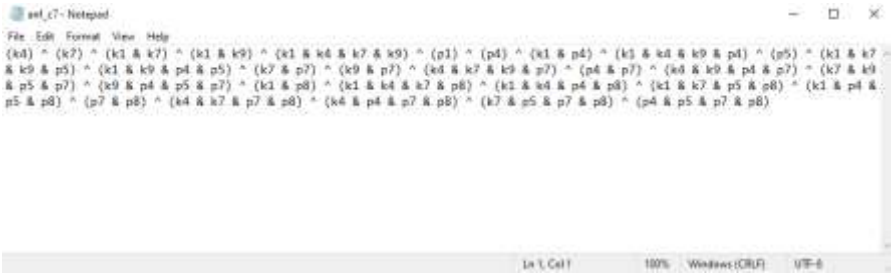
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678



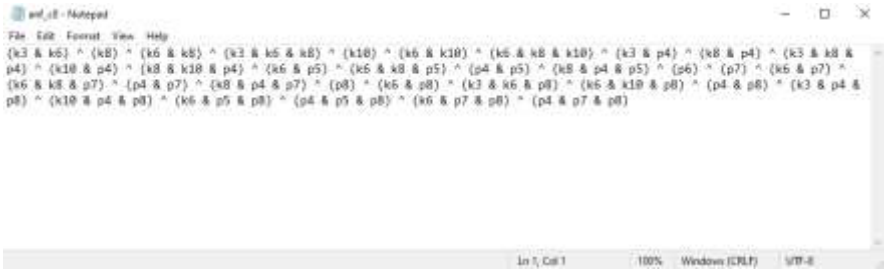
Gambar 15 Ekspresi ANF Bit ke-5 Ciphertext S-DES



Gambar 16 Ekspresi ANF Bit ke-6 Ciphertext S-DES



Gambar 17 Ekspresi ANF Bit ke-7 Ciphertext S-DES



Gambar 18 Ekspresi ANF Bit ke-8 Ciphertext S-DES

Representasi CNF selanjutnya digunakan dalam proses *solving* menggunakan BDD dan *SAT solver*, sedangkan representasi ANF digunakan untuk *Brute Force* dan *Gröbner Basis*.

4.2 Analisis Ekspresi Boolean Cipher Dengan Menggunakan Brute Force

Metode *Brute Force* digunakan untuk menyelesaikan sistem persamaan Boolean dalam bentuk Algebraic Normal Form (ANF) yang diperoleh dari delapan fungsi F1 hingga F8 hasil ekstraksi S-DES. Pada skenario *Ciphertext-Only Attack* (COA), kedelapan persamaan ANF digunakan secara bersamaan dengan 8 bit *plaintext* dan 10 bit kunci sebagai variabel yang tidak diketahui. Proses penyelesaian dilakukan dengan melakukan enumerasi terhadap seluruh kemungkinan kombinasi nilai *plaintext* dan kunci, kemudian setiap kombinasi diuji terhadap kedelapan persamaan ANF untuk menentukan kombinasi yang memenuhi seluruh persamaan secara simultan dan

This work is licensed under a Creative Commons Attribution 4.0 International License.

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

menghasilkan ciphertext yang diketahui. Kinerja metode *Brute Force* selanjutnya dianalisis berdasarkan waktu komputasi dan keberhasilannya dalam menemukan kombinasi *plaintext* dan kunci yang sesuai dengan ciphertext. Hasil pengukuran waktu komputasi tersebut disajikan pada Tabel 1.

Tabel 1 Hasil Pengukuran Brute Force

Nama Metode	Jumlah Solusi	Waktu Komputasi
Brute Force	262.144	177,79 detik

4.3 Analisis Ekspresi Boolean Cipher Dengan Menggunakan BDD (Binary Decision Diagram)

Metode *Binary Decision Diagram* (BDD) digunakan untuk menyelesaikan gabungan ekspresi Boolean dalam bentuk *Conjunctive Normal Form* (CNF) yang diperoleh dari delapan fungsi F1 hingga F8 hasil ekstraksi S-DES. Pada skenario *Ciphertext-Only Attack* (COA), kedelapan ekspresi tersebut digabungkan menggunakan operasi AND sehingga membentuk satu ekspresi Boolean yang merepresentasikan seluruh bit ciphertext. Selanjutnya, ekspresi gabungan tersebut direpresentasikan ke dalam struktur BDD untuk mencari kombinasi 8 bit *plaintext* dan 10 bit kunci yang memenuhi seluruh fungsi F1 hingga F8 secara bersamaan. Kinerja metode BDD kemudian dianalisis berdasarkan waktu komputasi dan keberhasilannya dalam menemukan kombinasi *plaintext* dan kunci yang sesuai dengan ciphertext yang diketahui. Hasil pengukuran tersebut disajikan pada Tabel 2.

Tabel 2 Hasil Pengukuran Binary Decision Diagram

Nama Metode	Jumlah Solusi	Waktu Komputasi
Binary Decision Diagram	1.024	2,62 detik

4.4 Analisis Ekspresi Boolean Cipher Dengan Menggunakan SAT Solver

Metode *Modern SAT Solver* digunakan untuk menyelesaikan gabungan ekspresi Boolean dalam bentuk *Conjunctive Normal Form* (CNF) yang diperoleh dari delapan fungsi F1 hingga F8 hasil ekstraksi S-DES. Pada skenario *Ciphertext-Only Attack* (COA), seluruh ekspresi F1 hingga F8 digabungkan menggunakan operasi AND sehingga membentuk satu permasalahan *Boolean Satisfiability* (SAT) yang merepresentasikan seluruh bit ciphertext. Ekspresi CNF gabungan tersebut kemudian dikonversi ke dalam format DIMACS CNF dan diselesaikan menggunakan *Modern SAT Solver* untuk mencari kombinasi 8 bit *plaintext* dan 10 bit kunci yang memenuhi seluruh klausa secara bersamaan. Kinerja *Modern SAT Solver* dianalisis berdasarkan waktu komputasi dan keberhasilannya dalam menemukan kombinasi *plaintext* dan kunci yang sesuai dengan ciphertext yang diketahui. Hasil pengukuran waktu komputasi tersebut disajikan pada Tabel 3.

Tabel 3 Hasil Pengukuran SAT Solver

Nama Metode	Jumlah Solusi	Waktu Komputasi
minisat22	1	37,32 detik
glucose3	1	51,98 detik

This work is licensed under a Creative Commons Attribution 4.0 International License.

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 50-59
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

glucose4	1	39,52 detik
glucose42	1	39,64 detik
cadical103	1	41,94 detik
cadical195	1	118,36 detik
maplesat	1	41,08 detik
lgl	1	59.78 detik

4.5 Analisis Ekspresi Boolean Cipher Dengan Menggunakan Grobner Basis

Metode *Gröbner Basis* digunakan untuk menyelesaikan sistem persamaan Boolean dalam bentuk Algebraic Normal Form (ANF) yang diperoleh dari delapan fungsi F1 hingga F8 hasil ekstraksi S-DES. Pada skenario *Ciphertext-Only Attack* (COA), kedelapan persamaan ANF digunakan secara bersamaan untuk membentuk sistem persamaan polinomial dengan 8 bit *plaintext* dan 10 bit kunci sebagai variabel yang tidak diketahui. Sistem persamaan tersebut kemudian diselesaikan menggunakan metode *Gröbner Basis* untuk memperoleh kombinasi nilai *plaintext* dan kunci yang memenuhi seluruh persamaan secara simultan dan menghasilkan ciphertext yang diketahui. Kinerja metode *Gröbner Basis* selanjutnya dianalisis berdasarkan waktu komputasi dan keberhasilannya dalam menemukan kombinasi *plaintext* dan kunci yang sesuai dengan ciphertext. Hasil pengukuran waktu komputasi tersebut disajikan pada Tabel 4.

Tabel 4 Hasil Pengukuran Grobner Basis

Nama Metode	Jumlah Solusi	Waktu Komputasi
Grobner Basis	1.024	9802 detik

5 Kesimpulan

Penelitian ini berhasil mengekstrak ekspresi Boolean dari algoritma S-DES yang merepresentasikan hubungan antara plaintext, kunci, dan ciphertext ke dalam delapan fungsi Boolean F1 hingga F8. Fungsi tersebut direpresentasikan dalam bentuk CNF dan ANF, kemudian digunakan untuk menyelesaikan permasalahan *Ciphertext-Only Attack* (COA) menggunakan empat metode, yaitu BDD dan *Modern SAT Solver* untuk representasi CNF serta *Brute Force* dan *Gröbner Basis* untuk representasi ANF. Hasil pengujian menunjukkan bahwa masing-masing metode memiliki karakteristik kinerja yang berbeda dalam menyelesaikan ekspresi Boolean S-DES, yang dapat dilihat dari waktu komputasi dan keberhasilannya dalam menemukan kombinasi plaintext dan kunci yang sesuai dengan ciphertext. Dengan demikian, penelitian ini menunjukkan bahwa ekstraksi ekspresi Boolean dapat digunakan sebagai pendekatan untuk menganalisis dan menyelesaikan permasalahan kriptografi berukuran kecil, serta memberikan dasar perbandingan kinerja berbagai metode solving terhadap representasi CNF dan ANF.

Referensi (Reference)

[1] C. Bright, J. Gerhard, I. Kotsireas, and V. Ganesh, "Effective Problem Solving Using SAT Solvers," *Commun. Comput. Inf. Sci.*, vol. 1125 CCIS, pp. 205–219, 2020, doi: 10.1007/978-3-

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2678

030-41258-6_15.

[2] H. K. Sahu, I. Gupta, N. R. Pillai, and R. K. Sharma, "BDD-based cryptanalysis of stream cipher: A practical approach," *IET Inf. Secur.*, vol. 11, no. 3, pp. 159–167, 2017, doi: 10.1049/iet-ifs.2016.0076.

[3] A. D. Dwivedi, M. Klouček, P. Morawiecki, I. Nikolić, J. Pieprzyk, and S. Wójtowicz, "SAT-based cryptanalysis of authenticated ciphers from the CAESAR competition," *ICETE 2017 - Proc. 14th Int. Jt. Conf. E-bus. Telecommun.*, vol. 4, no. Icete, pp. 237–246, 2017, doi: 10.5220/0006387302370246.

[4] M. Dubois and É. Filiol, "Hacking of the AES with boolean functions," *ICISSP 2017 - Proc. 3rd Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2017-Janua, no. Icissp, pp. 599–609, 2017, doi: 10.5220/0006091305990609.

[5] A. Soboń, M. Kurkowski, and S. Stachowiak, "Complete SAT based Cryptanalysis of RC5 Cipher," *J. Inf. Organ. Sci.*, vol. 44, no. 2, pp. 365–382, 2020, doi: 10.31341/jios.44.2.10.

[6] Y. Makwana, A. Panigrahi, and S. K. Pal, "Improved BDD-based Cryptanalysis of Keystream Generators with application to Trivium," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 51, no. 2, pp. 1–23, 2026, doi: 10.1007/s12046-026-03094-9.

[7] I. Mironov and L. Zhang, "Applications of SAT Solvers to Cryptanalysis of Hash Functions," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4121 LNCS, pp. 102–115, 2006, doi: 10.1007/11814948_13.

[8] E. Maro, "Modeling of algebraic analysis of PRESENT cipher by SAT solvers," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 734, no. 1, 2020, doi: 10.1088/1757-899X/734/1/012101.

[9] S. Stachowiak, M. Kurkowski, and A. Soboń, "SAT-Based Cryptanalysis of Salsa20 Cipher," in *Progress in Image Processing, Pattern Recognition and Communication Systems*, 2022, pp. 252–266. doi: 10.1007/978-3-030-81523-3_25.

[10] A. Soboń and S. Stachowiak, "ChaCha20 Cipher Cryptanalysis through SAT Problem Solving," *2024 IEEE 17th Int. Sci. Conf. Informatics*, pp. 355–361, 2024, doi: 10.1109/Informatics62280.2024.10900867.

[11] S. Simmons, "Algebraic Cryptanalysis of Simplified AES," *Cryptologia*, vol. 33, no. 4, pp. 305–314, 2009, doi: 10.1080/01611190903185328.

[12] O. Grumberg, S. Livne, and S. Markovitch, "Learning to order BDD variables in verification," *J. Artif. Intell. Res.*, vol. 18, pp. 83–116, 2003, doi: 10.1613/jair.1096.

[13] L. Xu, F. Hutter, H. H. Hoos, and K. Leyton-Brown, "SATzilla: Portfolio-based Algorithm Selection for SAT," *J. Artif. Intell. Res.*, vol. 32, pp. 565–606, 2008, doi: 10.1613/jair.2490.

[14] F. Paradise and S. Indarjani, "ALGEBRAIC ATTACK PADA SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)," in *Seminar Nasional Matematika UI*, 2017, pp. 726–735.

[15] N. M. Matanggwan and S. S. Carita, "Serangan Aljabar pada Algoritme S-IDEA dan Miniatur S-IDEA," *J. Info Kripto*, vol. 15, no. 1, pp. 19–26, 2021, doi: 10.56706/ik.v15i1.16.

This work is licensed under a Creative Commons Attribution 4.0 International License.