ANALISIS PERBANDINGAN ALGORITMA ENKRIPSI SNOW 3GDAN ADVANCED ENCRYPTION STANDARD (AES) PADA TEKNOLOGI IOT

ANALYSIS OF SNOW 3G AND ADVANCED ENCRYPTION STANDARD(AES) ENCRYPTION ALGORITHM ON IOT TECHNOLOGY

Iriana[1], Ratna Mayasari[2], Arif Indra Irawan[3]

[1,2,3] Universitas Telkom, Bandung
[1]**anairi@student.telkomuniversity.ac.id**, [2]**ratnamayasari@telkomuniversity.ac.id**,
[3]**arifirawan@telkomuniversity.ac.id**

Abstrak

***Internet of Things* (IoT) memiliki kemampuan dalam menghubungkan berbagai objek untuk saling bertukar informasi dan bekerja sama mencapai suatu keputusan. Dalam implementasi IoT, keamanan data yang baik harus tetap terjaga walaupun memiliki sumber daya perangkat terbatas. Untuk mengatasi permasalahan tersebut, maka diusulkan berbagai algoritma enkripsi yang efektif dalam aplikasi IoT. Tugas Akhir ini membahas dan menganalisa performansi algoritma *stream cipher* dan *block cipher* yaitu SNOW 3G dan *Advanced Encryption Standard* (AES).**

Algoritma SNOW 3G dirancang dan digunakan sebagai algoritma dasar dalam kerahasiaan dan integritas untuk teknologi 3GPP. Serta, algoritma AES yang ditetapkan menjadi salah satu algoritma terbaik dalam penyimpanan data rahasia dan implementasi pada perangkat lunak maupun perangkat keras. Dari masing-masing algoritma kemudian dilakukan pengujian keacakan dan ketidakpastian data enkripsi melalui sebuah simulasi. Lalu, membandingkan kedua hasil tersebut untuk menentukan algoritma yang paling baik dan aman jika akan diimplementasikan pada teknologi IoT.

Setelah dilakukan pengujian, penelitian Tugas Akhir ini memperoleh hasil keacakan dan ketidakpastian data berupa nilai *avalanche effect* dan *entropy* dari masing-masing algoritma. Algoritma AES menghasilkan nilai *avalanche effect* dan *entropy* yang lebih tinggi, yaitu sebesar 50,695% dan 3,60603. Sedangkan, algoritma SNOW 3G menghasilkan nilai sebesar 49,574% dan 3,56136.

Kata kunci: *Internet of Things (IoT), Stream Cipher, Block Cipher,* algoritma SNOW 3G, algoritma *Advanced Encryption Standard (AES)*.

Abstract

Internet of Things (IoT) has the ability to connect various objects to exchange information and work together to reach a decision. In the implementation of IoT, good data security must be maintained even though it has limited device resources. To overcome these problems, various encryption algorithms that are effective in IoT applications are proposed. This final project discusses and analyzes the performance of stream cipher and block cipher algorithms, namely SNOW 3G and Advanced Encryption Standard (AES).

The SNOW 3G algorithm is designed and used as the basic algorithm in confidentiality and integrity for 3GPP technology. Also, the AES algorithm is set to be one of the best algorithms for secret data storage and implementation on software and hardware. Each algorithm is then tested for randomness and uncertainty of encryption data through a simulation. Then, compare the two results to determine the best and safest algorithm if it will be implemented on IoT technology.

After the test, this final project research obtained the results of randomness and data uncertainty in the form of the avalanche effect and entropy values of each algorithm. The AES algorithm produces higher avalanche effect and entropy values, which are 50.695% and 3.60603. While the SNOW 3G algorithm produces values of 49.574% and 3.56136.

Keywords: Internet of Things (IoT), Stream Cipher, Block Cipher, SNOW3G algorithm, Advanced Encryption Standard (AES) algorithm.

1. Pendahuluan

Semakin berkembangnya teknologi internet dan keperluan manusia tentang teknologi, maka semakin banyak penelitian yang akan hadir, salah satunya pada IoT. Penerapan IoT dalam berbagai bentuk telah mulai diaplikasikan pada banyak aspek kehidupan manusia, sehingga akan semakin banyak perangkat dan pengguna yang terhubung dan mengirimkan lebih banyak data. Dengan meningkatnya jumlah perangkat IoT yang terhubung ini, teknik untuk menyediakan keamanan informasi merupakan tantangan utama yang harus diatasi selama perancangan perangkat tersebut. Salah satu contoh teknologi IoT, seperti *NarrowBand-Internet of Things* (NB-IoT) yang merupakan teknologi berbasis standar *Low Power Wide Area* (LPWA) dikembangkan untuk memungkinkan berbagai perangkat dan layanan IoT baru [1].

Dalam *Long Term Evolution* (LTE) Rilis 13 [2], NB-IoT diperkenalkan, memberikan peningkatan lebih lanjut seperti pengurangan biaya dan kompleksitas perangkat, masa pakai baterai yang lebih lama, dan *coverage* yang ditingkatkan. Sehingga, algoritma kriptografi yang digunakan untuk mengamankan data harus disesuaikan dengan kebutuhan perangkat dengan sumber daya terbatas. Algoritma yang dapat digunakan untuk kerahasiaan dan perlindungan integritas pengguna sistem LTE diantaranya algoritma AES dan SNOW 3G. Hal ini didefinisikan dalam *Technical Specification System Architecture Evolution* (SAE) dari 3GPP di bawah spesifikasi Arsitektur Keamanan [3].

Penulis mengusulkan bagaimana melakukan pengujian dan analisa simulasi performansi untuk algoritma AES dan SNOW 3G seperti keacakan dan ketidakakuratan data enkripsi berdasarkan masing-masing nilai *avalanche effect* dan *entropy*. Sehingga, nantinya bisa didapatkan kesimpulan algoritma mana yang paling efektif dan paling aman untuk bisa diimplementasikan pada sistem jaringan teknologi IoT.

2. Dasar Teori

2.1 Internet of Things

IoT merupakan teknologi yang memungkinkan objek fisik untuk melihat, mendengar, berpikir, dan melakukan pekerjaan dengan membuat objek fisik tersebut "berbicara" satu sama lain, untuk saling berbagi informasi dan mengoordinasikan keputusan yang tepat [4].

2.2 Kriptografi

Dalam bukunya, menurut J. Katz, Y. Lindell, menjelaskan bahwa *The Concise Oxford Dictionary* (2006) mendefinisikan kriptografi sebagai seni dalam menulis atau memecahkan kode [4]. Dalam kriptografi, terdapat enkripsi yang merupakan proses penyandian informasi. Proses ini mengubah informasi asli, yang dikenal sebagai *plaintext*, menjadi bentuk alternatif yang dikenal sebagai *ciphertext*.

2.3 Cipher

Cipher adalah teknik menyembunyikan pesan dengan mengganti huruf asli menjadi bentuk lain seperti huruf, angka, dan simbol lain. Jenis *cipher* antara lain *Block Cipher* dan *Stream Cipher* [5].

1. Block Cipher

Block Cipher merupakan metode enkripsi dan dekripsi yang dilakukan dengan membagi plaintext menjadi blok-blok, dan masing-masing blok dienkripsi menggunakan kunci yang sama [5].

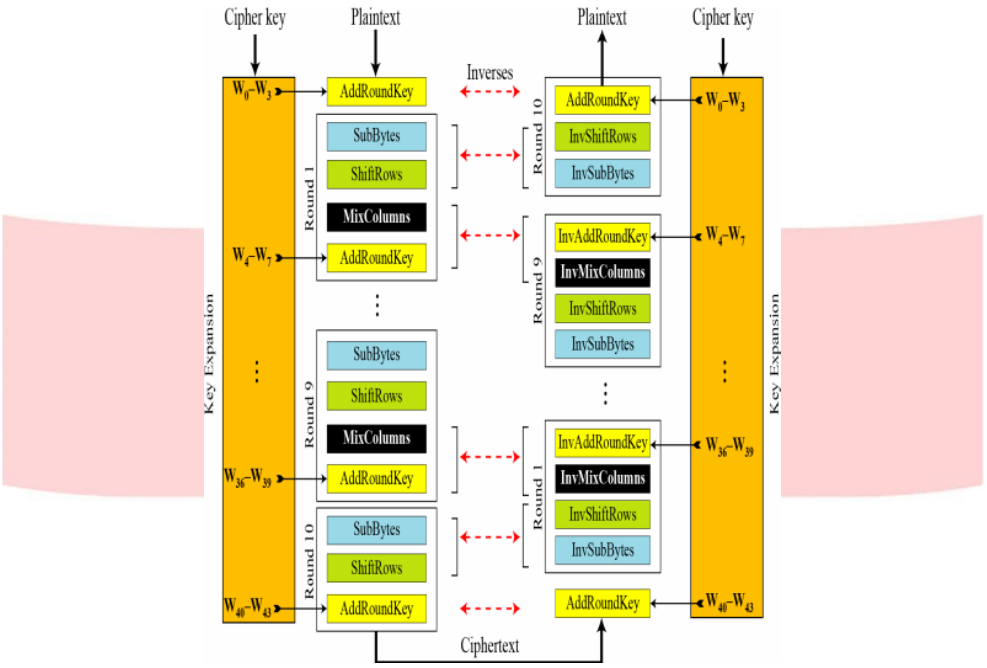
2. Stream Cipher

Stream Cipher merupakan metode enkripsi kunci simetris dimana *plaintext* digabungkan dengan *pseudorandom cipher digit stream* (*keystream*). Nilai *keystream* sendiri didapatkan dari hasil proses *internal state* antara *Key* dan *Initial Vector* (*IV*).

2.4 Algoritma *Advanced Encryption Standard* (AES)

AES adalah *block cipher* simetris, di mana pengirim dan penerima menggunakan satu kunci untuk enkripsi dan juga untuk dekripsi. Panjang kunci yang digunakan bisa 128, 192, atau 256 bit.

Algoritma AES juga merupakan algoritma iteratif. Setiap iterasi dapat disebut *round* atau putaran dan terdiri dari N putaran, di mana jumlah putaran tergantung pada panjang kunci: 10 putaran untuk 128 bit, 12 putaran untuk 192 bit dan 14 putaran untuk 256 bit. Putaran N-1 pertama terdiri dari empat fungsi transformasi yang berbeda, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Putaran terakhir hanya berisi tiga transformasi, dan ada transformasi tunggal awal (AddRoundKey) sebelum putaran pertama, yang dapat dianggap sebagai Putaran 0. AES beroperasi pada *byte array* 4 × 4 *column-major*, yang disebut *state*.



Gambar 2.1 Proses enkripsi dan dekripsi algoritma AES [6].

A. SubBytes

SubBytes merupakan tahap pertama tranformasi *byte* dimana setiap *byte* pada *state* dipetakan dengan meggunakan tabel subsitusi yang disebut S-Box. Tujuan utama dari langkah substitusi adalah untuk mengurangi korelasi antara bit*input* dan bit *output* pada tingkat *byte*.

B. ShiftRows

Transformasi ShiftRows adalah proses pergeseran *byte* dimana *byte* paling kiri akan dipindahkan ke *byte* paling kanan.

C. MixColumns

Transformasi MixColumns menggantikan setiap *byte* kolom dengan fungsi semua *byte* dalam kolom yang sama. Lebih tepatnya, setiap *byte* dalam kolom diganti dengan dua kali *byte* itu, ditambah tiga kali byte berikutnya, ditambah *byte* yang datang berikutnya, dan seterusnya.

D. AddRoundKey

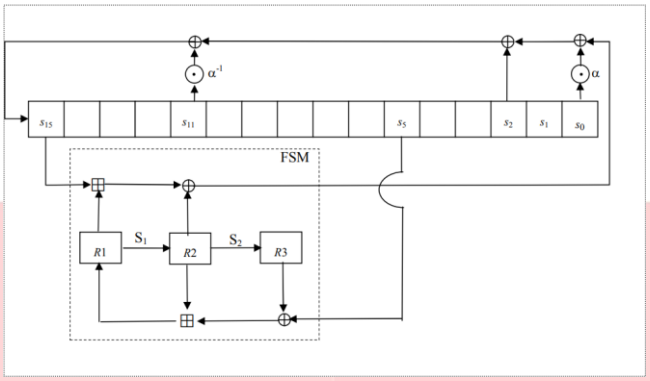
Pada langkah AddRoundKey, *sub key* digabungkan dengan *state*. Setiap putaran, *sub key* diturunkan dari kunci utama. *Sub key* ditambahkan dengan menggabungkan setiap *state* berisi *byte* dengan *byte* yang sesuai dari *sub key* menggunakan *bitwise* XOR.

2.5 Algoritma SNOW 3G

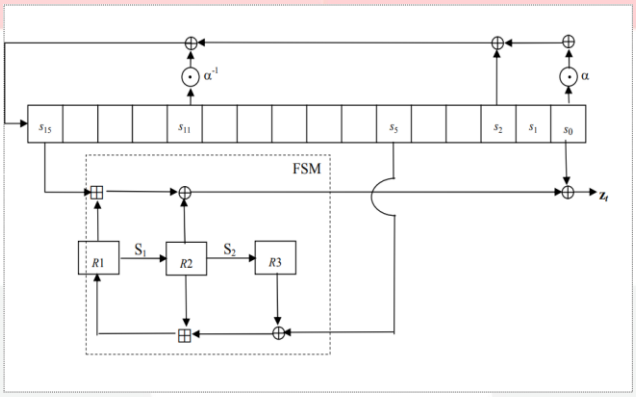
SNOW 3G adalah algoritma *stream cipher* yang menghasilkan 32 bit *word keystream* di bawah kendali 128-bit *Ciphering Key* (CK) dan 128-bit *Initialization Vector* (IV). SNOW 3G terdiri dari dua modul yang saling berinteraksi, *Linear Feedback Shift Register* (LFSR) dan *Finite State Machine* (FSM) [7]. LFSR dibangun dari 16 tingkat dan masing-masing memiliki 32 bit. Sedangkan, FSM didasarkan pada tiga register 32 bit R1, R2, dan R3 dan menggunakan duaensembel kotak subsitusi (S-box) S1 dan S2.

Tahap pertama, inisialisasi kunci dilakukan, yaitu *cipher* di-*clock* tanpa menghasilkan *output*, kemudian dengan setiap *clock* akan menghasilkan *output* 32 bit.SNOW 3G diinisialisasi dengan kunci 128 bit yang terdiri dari empat kata 32 bit k_0, k_1, k_2, k_3 dan variabel inisialisasi yang terdiri dari empat kata 32 bit IV_0, IV_1, IV_2, IV_3. FSM diinisialisasi dengan R1 = R2 = R3 = 0. Kemudian *cipher* berjalan dalam mode khusus tanpa menghasilkan *output*:

Gambar 2.2 dan Gambar 2.3 menunjukkan inisialisasi kunci dan *keystream generation* dari SNOW 3G.



Gambar 2.2 Inialisasi kunci algoritma SNOW 3G [7].



Gambar 2.3 *Keystream Generation* algoritma SNOW 3G [7].

2.6 Avalanche Effect

Avalanche effect merupakan parameter yang menyatakan jika *input* suatu algoritma enkripsi sedikit berubah (seperti membalik satu bit tunggal), maka *output* akan berubah secara signifikan dan perubahan *output* bisa mencapai setengahnya [8]. *Avalanche effect* memiliki persamaan sebagai berikut.

$$avalanche\ effect\ (\%) = \frac{jumlah\ bit\ berubah}{jumlah\ seluruh\ bit} \times 100\% \quad (2.1)$$

Nilai *avalanche effect* dikatakan baik ketika terjadi perubahan satu bit *input*, maka akan menghasilkan *output* lain dengan perbedaan mencapai lebih dari 50%.

2.7 Entropy

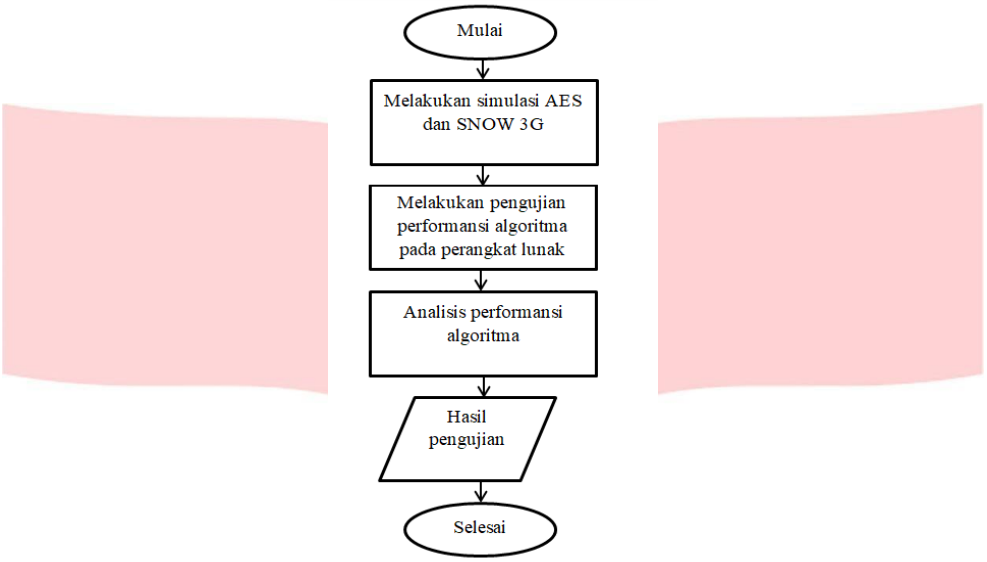
Entropy di dalam teori informasi, merupakan parameter yang menyatakan kandungan informasi rata-rata persimbol pada suatu *codeword*. *Entropy* sangat erat kaitannya dengan karya Shannon yang terkait dengan ketidakpastian suatu data [9]. Shannon merumuskan persamaan seperti berikut.

$$H(X) = -\sum_x \quad \mathrm{P[x]}\ log_2(\mathrm{P[x]}) \quad (2.2)$$

Dimana (X) adalah nilai *entropy* rata-rata suatu variabel *random* X dan $[x]$ adalah peluang munculnya simbol x dalam variabel *random* X. Sehingga jika nilai *entropy* suatu *codeword* tinggi, maka probabilitas yang dimiliki juga semakin tinggi [9]. Artinya simbol x dalam variabel *random* X semakin tidak pasti muncul.

3. Pembahasan

3.1 Desain Sistem



Gambar 3.1 Diagram alir skema perancangan sistem.

Skema perancangan ini dimulai dengan simulasi algoritma AES dan SNOW 3G. Dilanjutkan dengan melakukan pengujian performansi masing-masing algoritma pada perangkat lunak tertentu. Sehingga, kemudian dapat dilakukan pengujian terhadap kedua algoritma dan dianalisis dengan parameter yang sudah ditentukan. Hasil keluaran pengujan merupakan hasil data performansi dari masing-masing algoritma yang dibandingkan, berdasarkan nilai keacakan dan ketidakpastian yang paling baik.

3.2 Simulasi dan Pengujian Algoritma

Pada tahap ini dilakukan simulasi dan analisis terhadap algoritma AES dan SNOW 3G. Metode yang digunakan yaitu dengan melakukan pengukuran nilai *entropy* dan nilai *avalanche effect* terhadap masing-masing algoritma.

3.2.1 Pengujian Program Algoritma

Skenario pengujian algoritma AES dan SNOW 3G yang akan dianalisis, diaplikasikan pada variabel uji seperti berikut.

Tabel 3.1 Variabel pengujian pada program algoritma AES.

Input		***Output*** **(Variabel Uji)**	**Jumlah Data**	**Jenis Data**
Key	***Plaintext***			
Key-a1	Plaintext-a1	Ciphertext1	20	Hexa
Key-a2	Plaintext-a1	Ciphertext2	20	Hexa
Key-a1	Plaintext-a2	Ciphertext3	20	Hexa

Tabel 3.2 Variabel pengujian pada program algoritma SNOW 3G.

Key	***Initial Vector*** **(IV)**	***Input***		***Output*** **(Variabel Uji)**	**Jumlah Data**	**Jenis Data**
		Keystream	***Plaintext***			
Key-s1	Iv-s1	Keystream1	Plaintext1	Ciphertext1	20	Hexa
Key-s2	Iv-s1	Keystream2	Plaintext1	Ciphertext2	20	Hexa
Key-s1	Iv-s2	Keystream3	Plaintext1	Ciphertext3	20	Hexa

Berdasarakan Tabel 3.1 dan Tabel 3.2, algoritma AES dan SNOW 3G memiliki input enkripsi yang berbeda. Hal itu dikarenakan kedua algoritma memiliki metode enkripsi yang berbeda. Algoritma AES merupakan algoritma yang termasuk ke dalam kelompok *block cipher*, sehingga dalam proses enkripsinya hanya memerlukan *key* dan *plaintext* sebagai *input* untuk langsung menghasilkan *ciphertext*.

Sedangkan algoritma SNOW 3G termasuk ke dalam kelompok *stream cipher*, sehingga dalam proses enkripsinya memerlukan *key* dan IV sebagai inisialisasi awal untuk menghasilkan *keystream*. Simulasi pengujian masing-masing algoritma akan dilakukan sebanyak 20 kali dengan variasi konfigurasi *key* dan *plaintext* untuk algoritma AES, dan konfigurasi *key* dan IV untuk algoritma SNOW 3G.

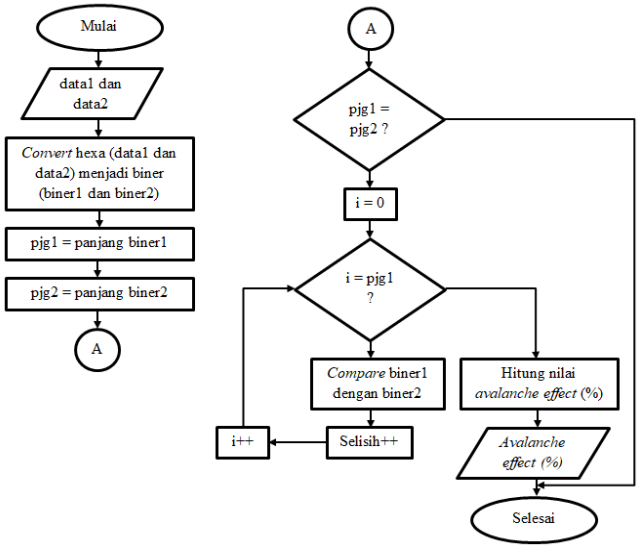
3.2.1.1 Pengujian *Avalanche Effect*

Analisis terhadap pengujian *avalanche effect* dilakukan dengan membandingkan dua buah data dari kedua program algoritma. Seperti data skenario pengujian yang ditunjukkan pada Tabel 3.3, data1 merupakan data awal yang belum ada perubahan pada bitnya. Kemudian, akan dibandingkan dengan data2 yang merupakan data setelah adanya perubahan pada salah satu bitnya.

Tabel 3.3 Skenario pengujian *avalanche effect.*

Algoritma	Pengujian	data1	data2
SNOW 3G	Avalanche1	Ciphertext1	Ciphertext2
	Avalanche2	Ciphertext1	Ciphertext3
AES	Avalanche1	Ciphertext1	Ciphertext2
	Avalanche2	Ciphertext1	Ciphertext3

Berikut ini merupakan diagram alir dalam melakukan pengukuran nilai *avalanche effect*.

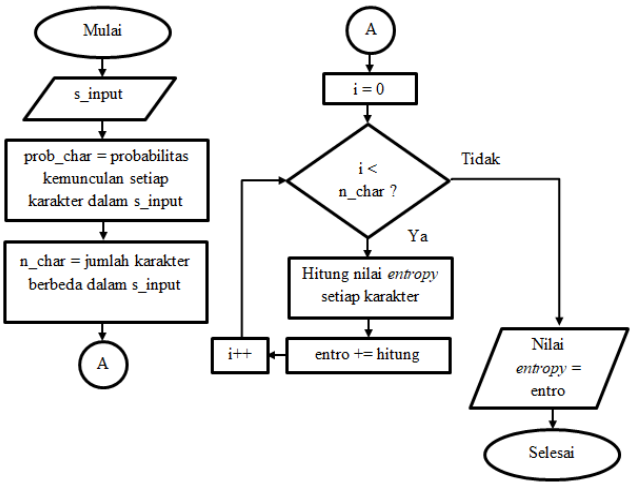


Gambar 3.2 Diagram alir pengukuran nilai *avalanche effect.*

Berdasarkan Gambar 3.3, data yang akan dianalisis yaitu data1 dan data2 sebagai variabel pengujian. Kemudian, program akan melakukan konversi terhadap masing-masing input data hexadesimal menjadi data biner. Proses selanjutnya menghitung panjang kedua input data dan membandingkannya, jika panjangnya tidak sama maka program akan berakhir. Sedangkan, jika panjang kedua data sama maka selanjutnya program akan menghitung selisih kedua data biner tersebut. Terakhir dilanjutkan dengan program melakukan perhitungan nilai *avalanche effect*.

3.2.1.2 Pengujian *Entropy*

Entropy memiliki diagram alir dalam melakukan pengukuran nilainya seperti berikut.



Gambar 3.3 Diagram alir pengukuran nilai *entropy*.

Berdasarkan Gambar 3.3, s_input merupakan variabel pengujian yang akan dianalisis. Selanjutnya, program akan mengitung probabilitas kemunculan setiap karakter serta jumlah karakter berbeda yang ada pada s_input. Terakhir, program akan menghitung nilai *entropy* setiap karakter dan menjumlahkan nilai tersebut sebagai hasil akhir pengukuran nilai *entropy* suatu data.

3.3 Analisis dan Pembahasan Hasil Simulasi

Tugas Akhir ini melakukan pengujian performansi pada masing-masing simulasi enkripsi algoritma SNOW 3G dan AES. Hasil dari pengujian akan menghasilkan nilai tingkat keacakan dan ketidakakuratan data melalui perhitungan *avalance effect* dan *entropy* kedua algoritma. Lalu, hasil pengujian data yang dihasilkan tersebut dapat menentukan algoritma mana yang lebih baik dan aman untuk bisa diimplementasi pada sistem IoT.

3.3.1 Hasil Pengujian Simulasi

Pada hasil pengujian ini, akan dijelaskan hasil data enkripsi dari simulasi pengujian pada algoritma AES dan SNOW 3G yang dijalankan pada *software* CrypTool. Berikut adalah salah satu hasil data enkripsi dari 20 kali pengujian yang telah dilakukan pada algoritma AES.

Tabel 4.1 Hasil data enkripsi algoritma AES.

Pengujian	Fungsi	Variabel	Data	Panjang Karakter
Uji 1	*Input* Enkripsi	Key-a1	**00000000 cccccccc 00000000 cccccccc**	32
		Plaintext-a1	**64fbac3d ff50932c 6d8231ae 888eda7b**	32
	Output Enkripsi	Ciphertext1	**d5546322 41b4bd1a c8db6ce3 8280ed6c**	32
Uji 2	*Input* Enkripsi	Key-a2	**10000000 cccccccc 00000000 cccccccc**	32
		Plaintext-a1	**64fbac3d ff50932c 6d8231ae 888eda7b**	32
	Output Enkripsi	Ciphertext2	**f178579c 1a856244 121c7025 3d81df19**	32
Uji 3	*Input* Enkripsi	Key-a1	**00000000 cccccccc 00000000 cccccccc**	32
		Plaintext-a2	**74fbac3d ff50932c 6d8231ae 888eda7b**	32
	Output Enkripsi	Ciphertext3	**72899a8e d8573c92 f0be5ce5 5ac8d3e4**	32

Pada Tabel 4.1, menujukkan variabel Key-a1 dan Plaintext-a1 merupakan *key* dan *plaintext* sebagai input sebelum adanya perubahan bit. Sedangkan, variabel Key-a2 dan Plaintext-a2 merupakan variabel setelah adanya perubahan pada masing-masing bit pertamanya. Variasi bit yang dilakukan terhadap *key* maupun *plaintext* ditunjukkan dengan huruf awal yang memiliki warna berbeda yaitu warna merah.

Pengujian data pada algoritma AES ini memiliki data *input key* maupun *plaintext* dengan panjang 32 karakter. Karena algoritma AES yang diterapkan pada Tugas Akhir merupakan AES-128, sehingga *key* yang digunakan adalah 128 bit sebagai *input* enkripsi. Proses enkripsi terjadi ketika *plaintext* langsung dienkripsi dengan *key* yang sudah ditentukan, sehingga dapat menghasilkan *ciphertext*. Sedangkan, salah satu hasil pengujian dari algoritma SNOW 3G, dapat dirincikan sebagai berikut.

Tabel 4.2 Hasil data enkripsi algoritma SNOW 3G.

Pengujian	Fungsi	Variabel	Data	Panjang Karakter
Uji 1	*Input* Inisialisasi	Key-s1	**00000000 cccccccc 00000000 cccccccc**	32
		Iv-s1	**64fbac3d ff5093c 6d8231ae 888eda7b**	32
	Output Inisialisasi	Keystream1	**e4fc016d f34c5ea7 e8539b38 058f56bf**	32
	Input Enkripsi	Plaintext1	**bacabaca bacabaca bacabaca bacabaca**	32
	Output Enkripsi	Ciphertext1	**5e36bba7 4986e46d 529921f2 bf45ec75**	32
Uji 2	*Input* Inisialisasi	Key-s2	**10000000 cccccccc 00000000 cccccccc**	32
		Iv-s1	**64fbac3d ff5093c 6d8231ae 888eda7b**	32
	Output Inisialisasi	Keystream2	**dbd5a0dc 4840a27b 7dc17667 61475482**	32
	Input Enkripsi	Plaintext1	**bacabaca bacabaca bacabaca bacabaca**	32
	Output Enkripsi	Ciphertext2	**611f1a16 f28a18b1 c70bccad db8dee48**	32
Uji 3	*Input* Inisialisasi	Key-s1	**00000000 cccccccc 00000000 cccccccc**	32
		Iv-s2	**74fbac3d ff5093c 6d8231ae 888eda7b**	32
	Output Inisialisasi	Keystream3	**0332647c b38a591c 6cd02780 702c5a9a**	32
	Input Enkripsi	Plaintext1	**bacabaca bacabaca bacabaca bacabaca**	32
	Output Enkripsi	Ciphertext3	**b9f8deb6 0940e3d6 d61a9d4a cae6e050**	32

Pada Tabel 4.2, menujukkan variabel Key-s1 dan Iv-s1 merupakan *key* dan IV sebagai input awal sebelum adanya perubahan bit. Sedangkan, variabel Key-s2 dan Iv-s2 merupakan variabel setelah adanya perubahan pada masing-masing bit pertamanya. Variasi bit yang dilakukan terhadap *key* maupun IV ditunjukkan dengan huruf awal yang memiliki warna berbeda yaitu warna merah.

Sama seperti algoritma AES, pengujian algoritma SNOW 3G memiliki data *input key* maupun IV dengan panjang 32 karakter. Karena algoritma ini menggunakan *key* dan IV 128 bit sebagai inisialisasi awal proses enkripsi. Kemudian, proses enkripsi terjadi saat *keystream* di-XOR dengan *plaintext* sehingga dapat menghasilkan *ciphertext*.

Tujuan dilakukannya perubahan bit pada masing-masing variabel dari kedua algoritma, yaitu untuk memenuhi skenario pengujian nilai *avalanche effect*. Sehingga, nilai tersebut dapat dianalisis dan bisa menentukan tingkat keacakan data mana yang paling baik diantara kedua algoritma.

3.3.2 Analisis Pengujian *Avalanche Effect*

Di tahap ini, analisis dilakukan terhadap hasil nilai rata-rata *avalance effect ciphertext* dari kedua algoritma. Perhitungan masing-masing nilai *avalanche effect* dapat menggunakan persamaan (2.1). Berikut hasil data yang diperoleh setelah melakukan pengujian pada algoritma AES dan SNOW 3G.

Tabel 4.3 Hasil pengujian *avalanche effect* pada algoritma AES.

Algoritma	Pengujian	*Ciphertext*	
		Jumlah Data	Nilai Rata-Rata (%)
AES	Avalanche1	20	50,7
	Avalanche2	20	50,69
	Rata-Rata (%)		**50,695**

Tabel 4.4 Hasil pengujian *avalanche effect* pada algoritma SNOW 3G.

Algoritma	Pengujian	*Ciphertext*	
		Jumlah Data	Nilai Rata-Rata (%)
SNOW 3G	Avalanche1	20	49,44
	Avalanche2	20	49,71
	Rata-Rata (%)		**49,575**

Berdasarkan Tabel 4.3, algoritma AES menghasilkan nilai rata-rata *avalanche effect* pada *ciphertext*nya sebesar 50,695%. Sedangkan, Tabel 4.4 menujukkan hasil nilai rata-rata *avalanche effect ciphertext* dari algoritma SNOW 3G sebesar 49,575%, dengan kata lain nilai yang dimiliki algoritma AES lebih tinggi dibandingkan dengan nilai yang dimiliki algoritma SNOW 3G.

Oleh karena itu, algoritma AES dapat menghasilkan *output* dengan tingkat keacakan data yang baik karena menghasilkan nilai *avalanche effect* lebih dari 50%. Sehingga data yang dienkripsi akan lebih aman jika menggunakan algoritma AES dibandingkan menggunakan algoritma SNOW 3G.

3.3.3 Analisis Pengujian *Entropy*

Di tahap ini, analisis dilakukan terhadap hasil nilai rata-rata *entropy ciphertext* dari kedua algoritma. Perhitungan masing-masing nilai *entropy* dapat menggunakan persamaan (2.2). Berikut hasil data yang diperoleh setelah melakukan pengujian pada algoritma AES dan SNOW 3G.

Tabel 4.5 Hasil pengujian *entropy* pada algoritma AES.

Algoritma	Pengujian	*Ciphertext*	
		Jumlah Data	Nilai Rata-Rata
AES	Ciphertext1	20	3,63369
	Ciphertext2	20	3,62322
	Ciphertext3	20	3,56119
	Rata-Rata		**3,60603**

Tabel 4.6 Hasil pengujian *entropy* pada algoritma SNOW 3G.

Algoritma	Pengujian	*Ciphertext*	
		Jumlah Data	Nilai Rata-Rata
SNOW 3G	Ciphertext1	20	3,56971
	Ciphertext2	20	3,53676
	Ciphertext3	20	3,57762
	Rata-Rata (%)		**3,56136**

Berdasarkan Tabel 4.5, algoritma AES menghasilkan nilai rata-rata *entropy* pada *ciphertext*nya sebesar 3,60603. Sedangkan, Tabel 4.6 menujukkan hasil nilai rata-rata *entropy ciphertext* dari algoritma SNOW 3G sebesar 3,56136. Dari hasil pengujian kedua algoritma, nilai *entropy* pada *codeword ciphertext* algoritma AES lebih tinggi dibandingkan dengan nilai SNOW 3G. Sehingga berdasarkan perbandingan nilai tersebut, algoritma AES memiliki probabilitas yang lebih tinggi dalam ketidakpastian munculnya sebuah data.

4. Kesimpulan

Berdasarkan hasil pengujian dan analisa yang telah dilakukan pada program algoritma AES maupun SNOW 3G, kesimpulan yang dapat diambil adalah sebagai berikut:

1. Algoritma AES memiliki nilai *avalanche effect* yang lebih tinggi. Nilai tersebut menunujukkan bahwa keacakan data AES baik, sehingga apabila satu bit *input* diubah, maka dapat menghasilkan lebih dari 50% *ouput* data dari sebelum adanya perubahan bit.
2. Algoritma AES memiliki nilai *entropy* yang lebih baik, sehingga ketidakpastian data yang tinggi dapat menghasilkan *output* yang lebih sulit ditebak.

Referensi:

[1] NarrowBand-Internet of Things, *"GSMA | NarrowBand-Internet of Things (NB-IoT) | Internet of Things"*, Agustus, 2021. [Online]. Available: www. gsma.com/iot/narrow-band-internet-of-things-nb-iot/.

[2] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, J. P. Koskinen, "*Overview of narrowband IoT in LTE Rel-13*", 2016 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 1-7, Oct 2016.

[3] C. Luis, F. Sebastien, L. Liang, *"Design of an Area Efficient Crypto Processor for 3GPP-LTE NB-IoT Devices"*, Microprocessors and Microsystems (2019), pp. 1-8, September 2019.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "*Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications*," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347- 2376, Fourthquarter 2015.

[5] J. Katz, Y. Lindell, "*Introduction to Modern Cryptography: Principles and Protocols*," 1st ed. Florida, United States of America: CRC Press, 2007.

[6] Radhika D.Bajaj, Dr. U.M. Gokhale, *"Design and Simulation of AES Algorithm for Cryptography"* International Journal of Engineering Science and Computing, vol. 6, issues 6, PP. 6340-6344, Juni 2014.

[7] G. Orhanou, S. El Hajji, Y. Bentaleb, *"SNOW 3G Stream Cipher Operation and Complexity Study,"* Contemporary Engineering Sciences, vol. 3, no. 3. Pp. 97 –111. 2010.

[8] Larry B. de Guzman, Ariel M. Sison, and Ruji P. Medina, "*MD5 Secured Cryptographic Hash Value*," In Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence (MLMI2018). Association for Computing Machinery, New York, NY, USA, 54–59. 2018.

[9] Ben-Naim, Arieh, "*Entropy, Shannon's Measure of Information and Boltzmann's H-Theorem.*" Entropy 19, no. 2: 48. 2017.