Sains Malaysiana 52(3)(2023): 1023-1036
http://doi.org/10.17576/jsm-2023-5203-24

Analisis Kerawakan Algoritma Terubah Suai Sifer Blok Ultra-Ringan, SLIM

(Randomness Analysis of the Modified Ultra-Lightweight Block Cipher Algorithm, SLIM)

Isma Norshahila binti Mohammad Shah[1,2,*] & Eddie Shahril bin Ismail[1]

[1]*Department of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia*
[2]*Cryptography Development Department, CyberSecurity Malaysia, Menara Cyber Axis, 63000 Cyberjaya, Malaysia*

Diserahkan: 19 Ogos 2022/Diterima: 12 Februari 2023

ABSTRAK

Ahli kriptografi giat menjalankan penyelidikan dalam bidang kriptografi ringan untuk mengekalkan keselamatan data dalam peranti sumber terhad seperti teg *RFID*, peranti perubatan dan penjagaan kesihatan serta rangkaian sensor. Satu daripada algoritma kriptografi ringan yang telah dibangunkan untuk tujuan tersebut ialah algoritma SLIM. SLIM merupakan algoritma sifer blok ultra-ringan khusus digunakan dalam Internet Kesihatan Benda. SLIM adalah sifer blok bersaiz 32-bit berasaskan struktur Feistel. Algoritma SLIM mempunyai keberkesanan penyulitan yang baik, walau bagaimanapun, algoritma ini tidak mempunyai fungsi kabur dan sebaran yang diperlukan oleh sifer blok sebagai satu daripada aspek keselamatan kriptografi yang harus dipatuhi. Oleh itu, bagi memperbaiki fungsi kabur dan sebaran algoritma ini, pengubahsuaian terhadap algoritma penjanaan kekunci algoritma SLIM telah dilakukan. Analisis kerawakan kemudiannya dilakukan bagi menilai kerawakan algoritma SLIM dan SLIM terubah suai dengan menggunakan Suit Ujian Statistik NIST. Sebanyak sembilan kategori data iaitu *Strict Key Avalanche, Strict Plaintext Avalanche, Plaintext Ciphertext Correlation, Cipher Block Chaining, Random Plaintext Random Key, Low-Density Key, High-Density Key, Low-Density Plaintext* dan *High-Density Plaintext* telah digunakan untuk menjana 100 jujukan input bagi setiap sampel dalam setiap kategori data. Algoritma SLIM dan SLIM terubah suai menjana blok teks sifer yang kemudiannya digabungkan untuk membentuk jujukan dedua. Berdasarkan hasil kajian perbandingan, keputusan analisis kerawakan algoritma SLIM terubah suai adalah lebih baik daripada algoritma asal berdasarkan aras keertian 1%.

Kata kunci: Algoritma SLIM; analisis kerawakan; kriptografi; sifer blok ringan

ABSTRACT

Academics and cryptography professionals are actively conducting research in the field of lightweight cryptography to maintain data security in limited resource devices such as RFID tags, medical and healthcare devices as well as sensor networks. One of the lightweight algorithms that have been developed is the SLIM algorithm. SLIM is an ultra-lightweight block cipher algorithm intended for use on the Internet of Health Things. SLIM is a 32-bit block cipher based on the Feistel structure. The SLIM algorithm does have good encryption efficacy, but the algorithm lacks the diffusion and confusion properties that a block cipher should provide as one of its cryptographic security aspects. Therefore, in order to improve the diffusion and confusion properties of the algorithm, a modification to the key scheduling algorithm for the SLIM algorithm has been done. Randomness analysis was then performed to assess the randomness of the algorithms using the NIST Statistical Test Suite. A total of nine data categories namely Strict Key Avalanche, Strict Plaintext Avalanche, Plaintext Ciphertext Correlation, Cipher Block Chaining, Random Plaintext Random Key, Low-Density Key, High-Density Key, Low-Density Plaintext, and High-Density Plaintext was used to generate 100 input sequences for each sample in each data category. The algorithms generate ciphertext blocks, which are then combined to form a binary sequence. According to the results of the comparison study, the proposed algorithms' randomness analysis results are better than the original algorithm based on the 1% significance level.

Keywords: Cryptography; lightweight block cipher; randomness analysis; SLIM algorithm

Pendahuluan

Bidang kriptografi ringan telah mendapat banyak perhatian sejak beberapa tahun kebelakangan ini disebabkan peralihan paradigma ke arah bidang Internet Benda (*Internet of Things*). Internet Benda, atau IB, merujuk kepada berbilion-bilion alat fizikal yang

kini disambungkan ke internet dan berupaya untuk mengumpul serta bertukar-tukar data di seluruh dunia. Istilah 'Internet Benda' merujuk kepada gajet yang boleh berkomunikasi dengan internet tanpa memerlukan campur tangan manusia. Teg *RFID*, peranti perubatan dan penjagaan kesihatan serta rangkaian sensor adalah antara aplikasi IB.

Sistem IB menggunakan data dalam dunia nyata. Oleh itu, pengumpulan data daripada peranti IB boleh menjadi sasaran serangan siber. Disebabkan ini, tindak balas berdasarkan proses penyulitan menggunakan sistem kriptografi kini semakin penting dan perlu sentiasa dibangunkan dan ditambahbaik dari aspek keselamatan dan kecekapan.

Kriptografi ringan merupakan kaedah penyulitan yang menggunakan tenaga yang kecil serta kerumitan pengiraan yang rendah (Fan et al. 2015). Ia bertujuan untuk memperluaskan penggunaan kriptografi kepada peranti yang mempunyai sumber terhad. Kriptografi ringan secara amnya dikategorikan kepada empat jenis iaitu sifer blok ringan, fungsi cincang ringan, kod pengesahan mesej ringan dan sifer alir ringan (McKay et al. 2017).

Sebilangan besar algoritma yang telah dibangunkan dalam bidang sifer blok ringan dalam beberapa tahun kebelakangan ini adalah seperti PRESENT (Bogdanov et al. 2007), HIGHT (Hong et al. 2006), CLEFIA (Shirai et al. 2007), SIMON/SPECK (Beaulieu et al. 2015) dan SLIM (Aboushosha et al. 2020). Dalam bahagian seterusnya, algoritma tersebut diterangkan secara ringkas.

PRESENT merupakan satu sifer blok ringan yang beroperasi dalam saiz blok 64-bit. PRESENT mempunyai dua saiz kekunci iaitu kekunci 80 bit, disebut PRESENT-80 dan kekunci 128-bit disebut PRESENT-128. PRESENT (Bogdanov et al. 2007) menggunakan struktur rangkaian permutasi-penggantian dengan 31 pusingan dan satu kekunci terakhir menggunakan operasi eksklusif-atau, $\oplus$ pada pusingan terakhirnya. PRESENT disenaraikan sebagai algoritma sifer blok ringan yang disyorkan di dalam dokumen *ISO/IEC 29192-2:2019 Information security — Lightweight cryptography — Part 2: Block ciphers* (ISO/IEC 2012).

HIGHT (Hong et al. 2006) ialah sifer blok yang dibangunkan dengan penglibatan Agensi Internet dan Keselamatan Korea (Korea Internet & Security Agency, KISA). Ia telah dicadangkan sempena *Cryptographic Hardware and Embedded Systems (CHES) 2006, 8th International Workshop* di Yokohama, Jepun untuk kegunaan dalam aplikasi ringan seperti rangkaian sensor dan teg RFID. HIGHT beroperasi pada saiz blok 64-bit dan menggunakan kekunci 128-bit. Sifer ini menggunakan struktur rangkaian Feistel Umum yang berulang pada 32 pusingan. HIGHT telah diterima pakai dalam standard ISO di Korea bermula tahun 2010 (ISO/IEC, December 2010). Penilaian keselamatan HIGHT yang dianalisis dalam Hong et al. (2006) menunjukkan bahawa sifer ini mempunyai keselamatan yang mencukupi untuk bertahan daripada semua serangan kriptografi sifer blok.

CLEFIA (Shirai et al. 2007) ialah algoritma sifer blok ringan yang telah dibangunkan bersama oleh Sony, Universiti Nagoya dan Shirai et al. pada tahun 2007. Saiz blok bagi CLEFIA ialah 128-bit dan mengguna pakai tiga saiz kekunci iaitu 128-bit, 192-bit atau 256-bit. CLEFIA dibangunkan bertujuan untuk digunakan dalam sistem pengurusan hak digital (DRM) (Murph 2022). DRM ialah penggunaan teknologi untuk mengawal dan mengurus akses kepada bahan yang mempunyai hak cipta. CLEFIA adalah antara teknik kriptografi yang disyorkan untuk kegunaan kerajaan Jepun dalam Projek CRYPTREC pada tahun 2013. Pada masa ini, CLEFIA termasuk dalam piawaian *ISO/IEC 29192-2:2019 Information security — Lightweight cryptography — Part 2: Block ciphers* (ISO/IEC 2012). CLEFIA menggunakan struktur rangkaian Feistel Umum Jenis 2, 4-cabang dan 8-cabang. Jumlah pusingan CLEFIA adalah bergantung pada panjang kekunci yang digunakan iaitu 18 (128-bit), 22 (192-bit) dan 26 (256-bit) pusingan dalam proses penyulitan satu blok data.

SIMON dan SPECK (Beaulieu et al. 2015) ialah keluarga sifer blok ringan yang dibangunkan oleh Agensi Keselamatan Negara (NSA), Amerika Syarikat pada 2013. SIMON dan SPECK masing-masing datang dengan sepuluh sifer blok yang berbeza yang mempunyai saiz blok dari 32-bit hingga 128-bit dan saiz kekunci dari 64-bit hingga 256-bit. Keluarga sifer blok ini direka bentuk untuk beroperasi dengan baik pada sesuatu platform tertentu berdasarkan tahap keselamatan dan prestasi penyulitan yang dikehendaki di dalam peranti tersebut. SIMON telah dioptimumkan untuk mempunyai prestasi yang baik dalam pelaksanaan perkakasan, manakala algoritma, SPECK, telah dioptimumkan untuk mempunyai prestasi yang baik dalam pelaksanaan perisian.

SLIM (Aboushosha et al. 2020) ialah sifer blok ringan yang mengguna pakai struktur rangkaian Feistel. SLIM disasarkan untuk kegunaan dalam sistem RFID bagi teknologi Internet Kesihatan Benda (*Internet of Health Things*). Sifer ini menggunakan panjang kunci 80-bit dan beroperasi pada saiz blok 32-bit yang berulang sebanyak 32 pusingan. Berdasarkan kajian Aboushosha

et al. (2020), sifer ini tahan terhadap analisis kriptografi pembezaan dan linear serta memberikan margin keselamatan yang baik.

Kapasiti untuk beroperasi sebagai penjana nombor rawak adalah satu daripada keperluan utama apabila membina algoritma kriptografi. Ini merupakah satu daripada aspek keselamatan kriptografi yang harus dipatuhi. Semakin baik kerawakan sesuatu algoritma itu, semakin tinggi sifat kabur dan sebaran yang terdapat dalam output yang dijana algoritma tersebut.

Sepanjang pengetahuan kami, analisis kerawakan tidak pernah dilakukan pada algoritma SLIM dalam menilai keselamatan sifer blok ringan SLIM. Ujian bagi kerawakan perlu dijalankan terhadap algoritma kriptografi kerana ia dapat menentukan sama ada output daripada algoritma tersebut boleh diramal atau tidak. Oleh itu, penyelidikan ini akan menangani isu ini dalam kajian ini.

Selain itu, pengubahsuaian terhadap algoritma SLIM juga dilakukan. Ini bagi menghasilkan reka bentuk algoritma yang lebih selamat dari segi kerawakan berbanding algoritma asal. Pengubahsuaian ini dilakukan terhadap algoritma penjanaan kekunci algoritma tersebut.

Makalah ini disusun berdasarkan susunan yang berikut. Bahagian kedua membentangkan beberapa kerja terdahulu yang berkaitan dengan analisis kerawakan yang dilakukan pada algoritma kriptografi terdahulu. Bahagian ketiga memberikan penerangan ringkas tentang algoritma SLIM. Seterusnya dalam bahagian keempat, penerangan ringkas pengubahsuaian algoritma SLIM diberikan. Metodologi yang digunakan untuk melakukan analisis kerawakan terhadap kedua-dua algoritma dijelaskan dalam bahagian kelima. Keputusan dan perbincangan dibentangkan dalam bahagian keenam. Akhir sekali, penyelidikan semasa disimpulkan dalam bahagian ketujuh.

PENYELIDIKAN LEPAS

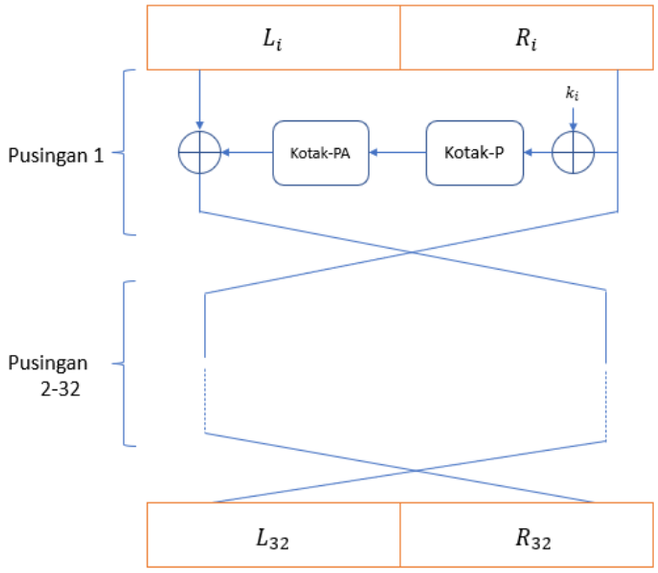
Kerawakan memainkan peranan penting dalam bidang kriptografi. Pelaksanaan operasi kriptografi adalah berdasarkan nombor rawak dengan ciri khas. Satu daripada kriteria penting untuk membangunkan algoritma penyulitan adalah keupayaannya sebagai penjana nombor rawak. Set ujian statistik Penjana Nombor Rawak (*Pseudorandom Number Generator* (PRNG)) boleh digunakan untuk menilai kerawakan output algoritma dengan menggunakan satu siri ujian statistik pada output. Selepas menilai beberapa suit ujian rawak yang tersedia iaitu Diehard (Alani 2010), TestUI (L'Ecuyer & Simard 2007) dan Suit Ujian Statistik NIST (Bassham et al. 2010), didapati bahawa Suit Ujian Statistik NIST adalah paling sesuai untuk melaksanakan ujian ini. Suit Ujian Statistik NIST dibangunkan oleh National Institute of Standards and Technology (NIST), Amerika Syarikat. Terdahulu, Suit Ujian Statistik NIST telah digunakan untuk menguji kerawakan calon dalam Pertandingan Advanced Encryption Standard (AES) (Soto 1999) anjuran NIST dan Projek Penyenaraian Algoritma Kebangsaan iaitu AKSA MySEAL (Kumpulan Fokus MySEAL 2018) yang diterajui oleh CyberSecurity Malaysia. Selain itu, Suit Ujian Statistik NIST telah digunakan untuk menilai kerawakan beberapa algoritma sifer blok ringan sedia ada.

Analisis kerawakan bagi algoritma sifer blok ringan menggunakan Suit Ujian Statistik NIST telah dijalankan secara meluas pada algoritma KTANTAN (Nik Abdullah et al. 2011), KATAN (Lot et al. 2011), LBlock (Nik Abdullah et al. 2014), SPECK (Nizam Chew et al. 2015), SIMON (Mohammad Shah et al. 2015 & 2019), Modified Version of LBlock Block Cipher (Nik Abdullah et al. 2015), RECTANGLE (Zakaria et al. 2020) dan PRESENT (Mohammad Shah & Ismail 2020).

ALGORITMA SLIM

Bahagian ini menerangkan tentang struktur algoritma. SLIM yang merupakan algoritma penyulitan simetri iaitu kedua-dua proses penyulitan dan penyahsulitan menggunakan kekunci yang sama. Satu perbezaan antara dua proses ini ialah sub-kekunci penyahsulitan digunakan dalam susunan terbalik.

Sifer blok SLIM beroperasi dengan blok teks biasa dan teks sifer 32-bit dan dikawal oleh kekunci 80-bit. Ciri asas dalam reka bentuk algoritma ini ialah ia mempunyai kawasan pemprosesan yang kecil dan sesuai untuk aplikasi teg *RFID*. Struktur sistem kripto ini telah direka untuk dilaksanakan dengan cekap dalam kedua-dua jenis platform iaitu perisian dan perkakasan. SLIM beroperasi dalam 32 pusingan menggunakan 32 sub-kekunci yang setiap sub-kekunci adalah bersaiz 16-bit yang dijana daripada kekunci 80-bit. Seni bina asas algoritma penyulitan SLIM ditunjukkan dalam Rajah 1. Seperti yang dapat dilihat dalam rajah ini, seni bina SLIM adalah berdasarkan struktur Feistel. Input dibahagikan kepada bahagian kanan dan kiri yang melalui 32 pusingan bersama-sama dengan sub-kekunci yang dihasilkan.



RAJAH 1. Proses penyulitan algoritma SLIM

PEMPROSESAN SATU PUSINGAN SLIM

Seni bina SLIM yang lebih terperinci boleh diperoleh dengan mengkaji struktur dalaman satu pusingan. Langkah pertama ialah input 32-bit dibahagikan kepada dua bahagian 16-bit yang sama, dikenali sebagai separuh kiri, L_i dan separuh kanan, R_i yang $0 \leq i \leq 32$. Pemprosesan keseluruhan pada setiap pusingan boleh diringkaskan sebagai Persamaan (1) dan (2) iaitu separuh kanan input R_i, separuh kiri, L_i dan sub-kekunci k_i dimanipulasi menggunakan operasi eksklusif-atau, $\oplus$. Output operasi eksklusif-atau, $\oplus$ dimajukan ke kotak penggantian (Kotak-P) dan output kotak-P dimajukan ke proses pilih atur (Kotak-PA). Akhir sekali, output menjalankan operasi eksklusif-atau, $\oplus$ dengan separuh kiri untuk menjadi input separuh kanan pusingan seterusnya. Separuh kanan input R_i menjadi input separuh kiri pusingan seterusnya. Perhatikan persamaan berikut.

$$L_i = R_{i-1} \tag{1}$$

$$R_i = L_{i-1} \oplus P(S(k_i \oplus R_{i-1})) \tag{2}$$

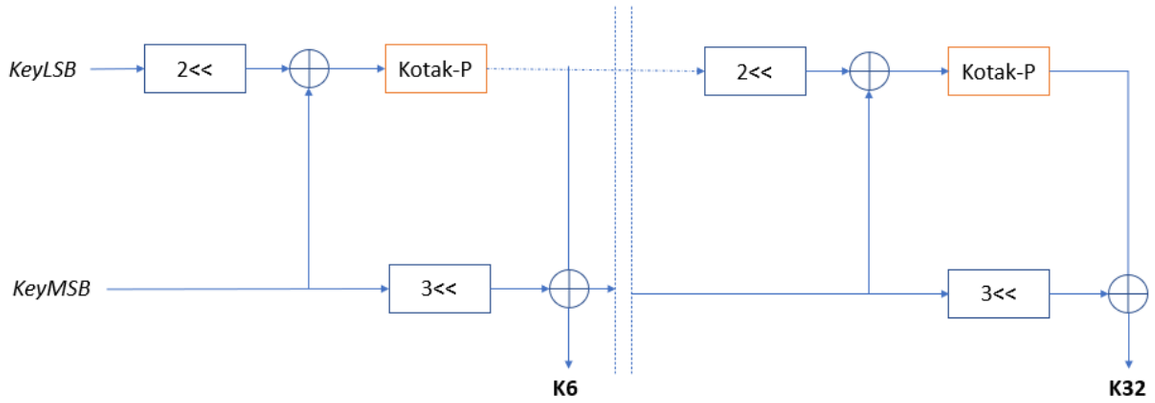
SLIM menggunakan Kotak-P seperti dalam Jadual 1. Kotak-P dalam SLIM digunakan sebanyak empat kali secara selari. Pilih atur ialah fasa terakhir fungsi SLIM. Kotak-PA menerima 16-bit dan mengubah suai inputnya menggunakan peraturan tertentu yang menghasilkan output 16-bit seperti yang ditunjukkan dalam Jadual 2.

Untuk 32 pusingan dan blok teks biasa 32-bit, 32 sub-kekunci bersaiz 16-bit diperlukan. Nilai sub-kekunci ini dijana daripada kekunci penyulitan 80-bit algoritma SLIM seperti yang ditunjukkan dalam Rajah 2. Proses penjanaan kekunci bagi setiap pusingan adalah diterangkan seperti berikut:

Lima sub-kekunci pertama, dilabelkan sebagai k_1, k_2, k_3, k_4 dan k_5 diambil terus daripada kekunci asal. Sub-kekunci k_1 adalah sama dengan 16-bit yang pertama (paling kanan), k_2 adalah sepadan dengan 16-bit berikutnya dan seterusnya bagi sub-kekunci k_3, k_4 dan k_5. Kemudian, kekunci asal 80-bit akan dibahagi kepada dua bahagian sama panjang dan menghasilkan dua kuantiti 40-bit kekunci, berlabel *KeyMSB* dan *KeyLSB*. Kekunci *KeyMSB* dan *KeyLSB* akan melalui proses yang berasingan untuk menjana sub-kekunci seterusnya.

Nilai kekunci daripada *KeyMSB* akan melalui proses anjakan pusing ke kiri sebanyak 3-bit dan di ekslusif-atau dengan *KeyLSB* yang telah dimanipulasikan untuk menghasilkan sub-kekunci pusingan yang seterusnya.

Pada setiap pusingan *KeyLSB*, nilai kekunci akan melalui proses anjakan pusing ke kiri sebanyak 2-bit dan kemudian output yang terhasil di eksklusif-atau, $\oplus$ dengan *KeyMSB*. Output operasi eksklusif-atau, $\oplus$ ini seterusnya dimajukan ke lapisan penggantian yang mengguna pakai Kotak-P. Output daripada proses ini seterusnya akan di eksklusif-atau, $\oplus$ dengan *KeyMSB* yang telah melalui proses anjakan pusing ke kiri terdahulu.



RAJAH 2. Proses penjanaan sub-kekunci algoritma SLIM

JADUAL 1. Kotak penggantian algoritma SLIM

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

*P(x) merupakan output daripada kotak penggantian

JADUAL 2. Kotak pilih atur algoritma SLIM

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$PA(x)$	7	13	1	8	11	14	2	5	4	10	15	0	3	6	9	12

*PA(x) merupakan output daripada kotak pilih atur

ALGORITMA SLIM TERUBAH SUAI

Algoritma penjanaan kekunci adalah faktor penting yang mempunyai kesan besar terhadap keselamatan algoritma kriptografi. Algoritma penjanaan kekunci yang kuat boleh menjana kekunci pusingan dengan sifat bebas, rawak dan tidak berkaitan antara satu sama lain. Ini dapat disahkan dengan melakukan analisis kerawakan terhadap algoritma tersebut (Rana et al. 2020).

Pengubahsuaian terhadap algoritma SLIM dilakukan terhadap algoritma penjanaan kekuncinya. Algoritma penjanaan kekunci dalam algoritma SLIM terubah suai mengguna pakai algoritma penjanaan kekunci bagi algoritma PRESENT-80. Proses penjanaan kekunci algoritma SLIM terubah suai adalah seperti yang berikut.

Kekunci rahsia 80-bit disimpan dalam daftar kekunci K dan dibentangkan sebagai $k_{79}\ldots k_0$. Nilai K_i iaitu kekunci pusingan ke i terdiri daripada 64-bit paling kiri bagi keadaan semasa daftar kekunci K. Oleh itu, $K_i = k_{63}\ldots k_0 = k_{79}\ldots k_{16}$. Selepas kekunci pusingan K_i telah diekstrak, daftar kekunci dikemaskini menggunakan tiga langkah berikut:

i. $[k_{79}k_{78} \ldots k_1k_0] = [k_{18}k_{17} \ldots k_{20}k_{19}]$

ii. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$

iii. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus kaunterpusingan$

Ini bermakna, pertama sekali daftar kekunci akan terputarkan dengan 61 kedudukan ke kiri. Dengan itu, empat bit paling kiri akan diproses oleh Kotak-P. Kotak-P adalah sama dengan Kotak-P yang digunakan dalam rutin penyulitan. Akhir sekali, bit k_{19} k_{18} k_{17} k_{16} k_{15} bagi *K*, akan diekslusif-atau dengan bit yang kurang bererti bagi *kaunterpusingan*.

KAEDAH KAJIAN

Kaedah bagi menjalankan analisis kerawakan ini terdiri daripada beberapa langkah, iaitu, penyediaan sampel, melakukan analisis kerawakan dan menilai keputusan ujian. Untuk menyediakan sampel untuk analisis kerawakan, sembilan set data dianalisis. Setiap set data dipilih berdasarkan fungsi khususnya yang diterangkan dalam bahagian seterusnya. Selepas menyediakan sampel, algoritma diuji menggunakan Suit Ujian Statistik NIST untuk menilai kerawakan algoritma. Akhirnya, keputusan ujian statistik dinilai.

KATEGORI DATA

Analisis kerawakan dilakukan untuk pusingan lengkap algoritma SLIM dan SLIM terubah suai berdasarkan tahap keertian 1%. Sembilan kategori data digunakan untuk membina input data dalam bentuk teks biasa atau kekunci, seperti ditunjukkan dalam Jadual 3. Kategori data berkaitan analisis ini ialah *Strict Key Avalanche, Strict Plaintext Avalanche, Plaintext Ciphertext Correlation, Cipher Block Chaining, Random Plaintext Random Key, Low-Density Key, High-Density Key, Low-Density Plaintext* dan *High-Density Plaintext*. Sebanyak 100 sampel dihasilkan menggunakan setiap kategori data. Jadual 4 meringkaskan panjang jujukan output yang dijana untuk setiap sampel dalam setiap kategori data.

Strict Plaintext Avalanche

Kategori data *Strict Plaintext Avalanche* digunakan untuk memeriksa kesensitifan sifer blok terhadap perubahan dalam teks biasa 32−bit. Bagi kekunci yang tetap, kesan *avalanche* dicapai apabila mana-mana bit teks biasa dilengkapkan dan setiap bit blok teks sifer berubah dengan kebarangkalian satu perdua.

Setiap sampel bagi kategori data ini menggunakan kekunci yang ditetapkan kepada semua sifar dan 977 blok 32−bit teks biasa asas yang rawak. Setiap teks biasa asas terlebih dahulu disulitkan menggunakan kekunci yang kesemuanya sifar. Kemudian, setiap teks biasa asas dibalikkan pada bit ke-*i*, yang $1 \leq i \leq 32$ bagi menghasilkan jumlah teks biasa yang diubah sebanyak 31,264 kali. Kemudian, setiap teks biasa yang diubah akan disulitkan menggunakan kekunci yang kesemuanya sifar. Semua teks sifer yang terhasil daripada teks biasa yang diubah akan melalui operasi eksklusif-atau, $\oplus$ menggunakan teks sifer yang terhasil daripada penyulitan teks biasa asas yang sepadan. Produk output daripada operasi eksklusif-atau, $\oplus$ itu disebut blok terbitan dan akan dirangkaikan untuk membina jujukan bit yang besar.

Plaintext/Ciphertext Correlation

Kategori data *Plaintext/Ciphertext Correlation* digunakan untuk memeriksa hubung kait antara pasangan teks biasa/ teks sifer dan menggunakan mod operasi *Electronic Code Book* (ECB).

Setiap sampel bagi kategori data ini menggunakan 31,250 blok 32−bit teks biasa dan satu 80−bit kekunci yang rawak. Setiap blok teks biasa disulitkan menggunakan 80−bit kekunci yang rawak. Kemudian, teks sifer yang terhasil akan melalui operasi eksklusif-atau, $\oplus$ menggunakan teks biasa yang sepadan. Produk output daripada operasi eksklusif-atau,$\oplus$ itu disebut blok terbitan dan akan dirangkaikan untuk membina jujukan bit yang besar.

Cipher Block Chaining

Kategori data *Ciphertext Block Chaining* menggunakan mod operasi *Cipher Block Chaining* (CBC). Dalam kategori data ini, setiap blok teks biasa akan melalui operasi ekslusif-atau, $\oplus$ menggunakan blok teks sifer yang terdahulu sebelum disulitkan, manakala blok pertama akan melalui operasi ekslusif-atau, $\oplus$ menggunakan vektor pemulaan. Perubahan satu-bit dalam mana-mana teks biasa atau vektor pemulaan akan memberi kesan terhadap semua blok teks sifer yang berikutnya.

Setiap sampel bagi kategori data ini menggunakan teks biasa yang ditetapkan kepada semua sifar (*TB*), 80−bit kekunci yang rawak (*K*) dan vektor pemulaan yang kesemuanya sifar (*IV*). Proses penyulitan dilakukan sebanyak 31,250 kali. Blok terbitan bagi kategori data ini ialah blok teks sifer dalam mod operasi CBC. Blok teks sifer yang pertama, TS_1 ditakrifkan sebagai $TS_1 = E_K\ (V \oplus TB_1)$, dan blok teks sifer yang berikutnya ditakrifkan sebagai $TS_i = E_K\ (TS_{i-1} \oplus B_i)$ bagi $2 \leq i \leq 31, 250$.

Random Plaintext/Random Key

Kategori data *Random Plaintext/Random Key* digunakan untuk memeriksa kerawakan teks sifer berdasarkan teks biasa rawak dan kekunci rawak. Setiap sampel bagi kategori data ini menggunakan 31,250 blok 32−bit teks biasa yang rawak dan satu 80-bit kekunci yang rawak.

JADUAL 3. Penyediaan satu sampel bagi setiap kategori data

Kategori data	Blok kekunci	Blok teks biasa	Blok terbitan
Strict Key Avalanche	391 blok rawak	Semua '0'	391
Strict Plaintext Avalanche	Semua '0'	977 blok rawak	977
Plaintext Ciphertext Correlation	Satu blok rawak	31,250 blok rawak	31,250
Cipher Block Chaining	Satu blok rawak	Semua '0'	31,250
Random Plaintext Random Key	Satu blok rawak	31,250 blok rawak	31,250
Low-Density Key	3,241 blok khusus	Satu blok rawak	3,241
High-Density Key	3,241 blok khusus	Satu blok rawak	3,241
Low-Density Plaintext	Satu blok rawak	529 blok khusus	529
High-Density Plaintext	Satu blok rawak	529 blok khusus	529

JADUAL 4. Panjang jujukan output yang dijana untuk satu sampel dalam setiap kategori data

Kategori data	Panjang (bit) jujukan output
Strict Key Avalanche	1,000,960
Strict Plaintext Avalanche	1,000,448
Plaintext Ciphertext Correlation	1,000,000
Cipher Block Chaining	1,000,000
Random Plaintext Random Key	1,000,000
Low-Density Key	103,712
High-Density Key	103,712
Low-Density Plaintext	16,928
High-Density Plaintext	16,928

Setiap blok teks biasa disulitkan menggunakan 80−bit kekunci yang rawak. Blok terbitan bagi kategori data ini ialah blok teks sifer dalam mod operasi ECB yang akan dirangkaikan untuk membina jujukan bit yang besar.

Low-Density Key

Kategori data *Low-Density Key* dibentuk berdasarkan 80−bit kekunci yang berkepadatan rendah. Setiap sampel bagi kategori data ini menggunakan 1 blok 32-bit teks biasa yang rawak dan 3,241 blok kekunci 80−bit yang khusus. Blok teks biasa pada awalnya disulitkan menggunakan 80−bit kekunci yang kesemuanya sifar. Kemudian, blok teks biasa yang sama akan disulitkan menggunakan 80-bit kekunci dengan hanya satu bit '1' dalam setiap kedudukan 80-bit kekunci dan semua bit kekunci yang lain ditetapkan kepada bit '0'. Ini akan

menghasilkan 81 blok teks sifer. Kemudian, blok teks biasa akan disulitkan menggunakan 80-bit kekunci dengan dua bit '1' dalam setiap gabungan kedudukan dua bit kekunci dan semua bit kekunci yang lain ditetapkan kepada bit '0'. Ini akan menghasilkan 3,160 blok teks sifer. Secara keseluruhannya, blok terbitan bagi kategori data ini ialah 3,241 blok teks sifer dalam mod operasi ECB dan akan dirangkaikan untuk membina jujukan bit yang besar.

High Density Key

Kategori data *High Density Key* dibentuk berdasarkan 80−bit kekunci berkepadatan tinggi. Setiap sampel bagi kategori data ini menggunakan 1 blok 32−bit teks biasa yang rawak dan 3,241 blok kekunci 80−bit yang khusus. Blok teks biasa pada awalnya disulitkan menggunakan 80−bit kekunci yang kesemuanya satu. Kemudian, blok teks biasa akan disulitkan menggunakan 80−bit kekunci dengan hanya satu bit '0' dalam setiap kedudukan kekunci 80−bit dan semua bit kekunci yang lain ditetapkan kepada bit '1'. Ini akan menghasilkan 81 blok teks sifer. Kemudian, blok teks biasa akan disulitkan menggunakan 80−bit kekunci dengan dua bit '0' dalam setiap gabungan kedudukan dua bit kekunci dan semua bit kekunci yang lain ditetapkan kepada bit '1'. Ini akan menghasilkan 3,160 blok teks sifer. Secara keseluruhannya, blok terbitan bagi kategori data ini ialah 3,241 blok teks sifer dalam mod operasi ECB dan akan dirangkaikan untuk membina jujukan bit yang besar.

Low-Density Plaintext

Kategori data *Low-Density Plaintext* dibentuk berdasarkan 32−bit blok teks biasa berkepadatan rendah. Setiap sampel bagi kategori data ini menggunakan 1 blok 80−bit kekunci yang rawak dan 529 blok 32−bit blok teks biasa yang khusus. 32−bit blok teks biasa yang kesemuanya sifar akan disulitkan menggunakan 80−bit kekunci rawak. Kemudian, blok teks biasa dengan hanya satu bit '1' dalam setiap kedudukan 32-bit teks biasa dan semua bit teks biasa lain yang ditetapkan kepada bit '0', akan disulitkan menggunakan 80−bit kekunci rawak yang sama. Ini akan menghasilkan 33 blok teks sifer. Kemudian, blok teks biasa dengan dua bit '1' dalam setiap gabungan kedudukan dua bit teks biasa dan semua bit teks biasa lain yang ditetapkan kepada bit '0', akan disulitkan menggunakan 80−bit kekunci rawak yang lain. Ini akan menghasilkan 496 blok teks sifer. Secara keseluruhannya, blok terbitan bagi kategori data ini ialah 529 blok teks sifer dalam mod operasi ECB dan akan dirangkaikan untuk membina jujukan bit yang besar.

High-Density Plaintext

Kategori data *High-Density Plaintext* dibentuk berdasarkan 32−bit blok teks biasa berkepadatan tinggi. Setiap sampel bagi kategori data ini menggunakan 1 blok 32−bit kekunci yang rawak dan 529 blok 32−bit blok teks biasa yang khusus. 32−bit blok teks biasa yang kesemuanya sifar akan disulitkan menggunakan 80−bit kekunci rawak. Kemudian, blok teks biasa dengan hanya satu bit '0' dalam setiap kedudukan 32−bit teks biasa dan semua bit teks biasa lain yang ditetapkan kepada bit '1', akan disulitkan menggunakan 80−bit kekunci rawak yang sama. Ini akan menghasilkan 33 blok teks sifer. Kemudian, blok teks biasa dengan dua bit '0' dalam setiap gabungan kedudukan dua bit teks biasa dan semua bit teks biasa lain yang ditetapkan kepada bit '1', akan disulitkan menggunakan 80−bit kekunci rawak yang lain. Ini akan menghasilkan 496 blok teks sifer. Secara keseluruhannya, blok terbitan bagi kategori data ini ialah 529 blok teks sifer dalam mod operasi ECB dan akan dirangkaikan untuk membina jujukan bit yang besar.

SUIT UJIAN STATISTIK NIST

Suit Ujian Statistik NIST digunakan untuk melakukan analisis kerawakan ke atas algoritma SLIM. Suit Ujian Statistik NIST ialah kit ujian kerawakan untuk jujukan binari yang dijana berdasarkan perkakasan atau perisian, sama ada melalui kriptografi rawak atau nombor penjanaan pseudo-rawak. Suit ujian ini mengandungi 15 ujian yang dibahagikan kepada dua kategori, iaitu Ujian Berparameter dan Ujian Tidak Berparameter. Ujian statistik untuk Ujian Berparameter termasuk *Block Frequency, Non-Overlapping Templates, Overlapping Template, Maurer's Universal, Linear Complexity, Serial* dan *Approximate Entropy*. Ujian statistik untuk Ujian Tidak Berparameter pula terdiri daripada *Frequency, Runs, Longest Runs of Ones, Binary Matrix Rank, Spectral, Cumulative Sums (Forward and Reverse), Random Excursion* dan *Random Excursion Variant*.

Setiap sampel dalam setiap ujian memerlukan bilangan minimum panjang bit yang nilainya dijadualkan dalam Jadual 5.

Kesemua ujian statistik kecuali *Cumulative Sums (Forward and Reverse), Serial, Non-Overlapping Templates, Random Excursion* dan *Random Excursion Variant* akan menghasilkan satu nilai-*p* untuk setiap sampel. Ujian *Cumulative Sums (Forward and Reverse)* dan Ujian *Serial* menghasilkan dua nilai-*p* untuk setiap ujian. Ujian *Non-Overlapping Templates* menghasilkan 148 nilai-p untuk setiap sampel. Jadual

JADUAL 5. Panjang bit minimum yang diperlukan bagi setiap ujian statistik

Kategori data	Panjang (bit) minimum
Block Frequency	100
Non-Overlapping Templates	100
Overlapping Template	1,000,000
Maurer's Universal	387,840
Linear Complexity	1,000,000
Serial	100
Approximate Entropy	100
Frequency	100
Runs	100
Longest Runs of Ones	128
Binary Matrix Rank	38,912
Spectral	1,000
Cumulative Sums (*Forward and Reverse*)	100
Random Excursion	1,000,000
Random Excursion Variant	1,000,000

6 menunjukkan nilai-*p* yang disediakan oleh setiap sampel bagi setiap ujian statistik.

Dalam Ujian Berparameter, nilai parameter bagi setiap ujian statistik mesti ditentukan. Jadual 7 menunjukkan nilai parameter yang digunakan dalam ujian kerawakan ini. Untuk menerangkan parameter yang digunakan dalam ujian tersebut, singkatan berikut digunakan: panjang blok (M *atau* L), panjang jujukan (*n*), blok *non-overlapping* (*N* = *nM*), panjang templat (*m*), dan bilangan blok dalam jujukan permulaan (*Q*).

HASIL DAN PERBINCANGAN

Dalam analisis ini, julat perkadaran yang boleh diterima untuk jujukan dedua ditentukan menggunakan selang keyakinan:

$$[p'_a, p'_b] = p' \pm 3\sqrt{\frac{p'(1-p')}{s}}$$

iaitu $p' = 1 - \alpha$, yang α ialah tahap keertian ($\alpha = 0.01$) dan *s* merupakan saiz sampel yang sama dengan 100 teks sifer bagi kesemua ujian statistik kecuali *Random Excursion* dan *Random Excursion Variant*. Jika nilai perkadaran berada di luar julat $[p'_a, p'_b]$, maka sampel adalah dianggap sebagai tidak rawak.

Ujian seperti *Overlapping Template*, *Linear Complexity, Random Excursion* dan *Random Excursion Variant* memerlukan bilangan bit tertentu bagi mendapatkan keputusan kerawakan manakala ujian statistik *Maurer's Universal* memerlukan sekurang-kurangnya 387,840 bit jujukan binari. Oleh itu, analisis jujukan output yang dijana daripada kategori data *Low-Density Key*, *High-Density Key*, *Low-Density Plaintext* dan *High-Density Plaintext* tidak boleh dilakukan dalam ujian-ujian ini.

Dalam analisis kerawakan yang dijalankan ke atas algoritma SLIM dan SLIM terubah suai, terdapat sejumlah 188 nilai-*p* yang diperoleh daripada kategori

JADUAL 6. Perincian nilai-*p* yang diperoleh dalam setiap ujian statistik

Kategori Data	Nilai-*p*
Block Frequency	1
Non-Overlapping Templates	148
Overlapping Template	1
Maurer's Universal	1
Linear Complexity	1
Serial	2
Approximate Entropy	1
Frequency	1
Runs	1
Longest Runs of Ones	1
Binary Matrix Rank	1
Spectral	1
Cumulative Sums (*Forward and Reverse*)	2
Random Excursion	8
Random Excursion Variant	18

JADUAL 7. Nilai parameter yang digunakan dalam Ujian Berparameter

Ujian statistik	Nilai parameter	Justifikasi pemilihan nilai parameter
Block Frequency	$M = 20{,}000$	Pastikan $n \geq MN$, $M > 20$, $M \geq 0.01n$ dan $N < 100$
Non-Overlapping Templates	$m = 9$	Saranan oleh NIST (Bassham et al. 2010)
Overlapping Template	$m = 9$	Saranan oleh NIST (Bassham et al. 2010)
Maurer's Universal	L = 7,Q	Saranan oleh NIST (Bassham et al. 2010)
Linear Complexity	$M = 500$	M mesti berada dalam lingkungan $500 \leq M \leq 5000$ dan $N \geq 200$ dandan dan
Serial	$m = 2$	Pastikan $m < \log_2 n-2$
Approximately Entropy	$m = 2$	Pastikan $m < \log_2 n-5$

data *Strict Key Avalanche, Strict Plaintext Avalanche, Plaintext Ciphertext Correlation, Cipher Block Chaining* dan *Random Plaintext Random Key* dan 159 nilai-*p* diperoleh daripada kategori data *Low-Density Key, High-Density Key, Low-Density Plaintext* dan *High-Density Plaintext*.

Memandangkan analisis ini menggunakan seratus sampel dan tahap keertian ditetapkan pada 0.01, julat perkadaran penerimaan sampel sesuai untuk semua ujian kecuali ujian *Random Excursion* dan *Random Excursion Variant* berada dalam lingkungan [0, 4]. Ujian *Random Excursion* dan *Random Excursion Variant* tidak memerlukan kesemua 100 jujukan dedua, kerana beberapa jujukan dedua tidak mempunyai kitaran yang mencukupi untuk menjalankan ujian. Hanya sampel yang mempunyai lebih daripada 500 kitaran dalam ujian tersebut adalah dinilai. Sampel dengan bilangan kitaran yang tidak mencukupi tidak dipertimbangkan. Oleh itu, julat perkadaran yang boleh diterima bagi kedua-dua ujian ini adalah berbeza-beza (Jadual 8) bergantung pada sampel yang memenuhi keperluan. Bagi kategori data *Low-Density Key, High-Density Key, Low-Density Plaintext,* dan *High-Density Plaintext* bilangan bit sampel adalah tidak mencukupi bagi ujian statistik *Random Excursion* dan *Random Excursion Variant*.

NIST mencadangkan bahawa data adalah dianggap sebagai rawak jika dan hanya jika jujukan itu melepasi semua prosedur ujian. Jika jujukan yang diuji gagal satu atau lebih prosedur ujian rawak, terdapat bukti yang jelas bahawa data adalah tidak rawak. Keputusan analisis SLIM diringkaskan dalam Jadual 9. Keputusan analisis SLIM terubah suai diringkaskan dalam Jadual 10. Jika jujukan yang ditolak berada dalam julat perkadaran yang boleh diterima, hasilnya adalah lulus (L). Jika tidak, hasilnya gagal (G). Untuk kategori data yang mempunyai jujukan yang gagal, bilangan jujukan yang gagal ditunjukkan dalam kurungan '()'.

JADUAL 8. Julat perkadaran penerimaan ujian kerawakan bagi ujian statistik *Random Excursion* dan *Random Excursion Variant*

Kategori data	Jumlah sampel yang dianalisis	Julat perkadaran penerimaan
Strict Key Avalanche	63	[0, 3]
Strict Plaintext Avalanche	68	[0, 4]
Plaintext Ciphertext Correlation	36	[0, 3]
Cipher Block Chaining	51	[0, 3]
Random Plaintext Random Key	33	[0, 3]

Seperti yang ditunjukkan dalam Jadual 9, jumlah bilangan jujukan teks sifer yang gagal daripada algoritma SLIM ialah 8 kategori data. Kesemua kategori data tersebut ialah *Strict Key Avalanche, Strict Plaintext Avalanche, Cipher Block Chaining, Random Plaintext Random Key, Low-Density Key, High-Density Key, Low-Density Plaintext* dan *High-Density Plaintext*. Algoritma SLIM hanya lulus kesemua ujian statistik dalam kategori data *Plaintext Ciphertext Correlation*.

Jadual 10 pula menunjukkan jumlah bilangan jujukan teks sifer yang gagal daripada algoritma SLIM terubah suai ialah 6 kategori data iaitu *Strict Key Avalanche, Strict Plaintext Avalanche, Random Plaintext Random Key, Low-Density Key, Low-Density Plaintext* dan *High-Density Plaintext.* Algoritma SLIM terubah suai lulus kesemua ujian statistik dalam tiga kategori data iaitu *Plaintext Ciphertext Correlation, Cipher Block Chaining* dan *High-Density Key*.

Oleh itu, adalah jelas bahawa jujukan output yang dijana daripada SLIM pada asasnya adalah tidak rawak. Walau bagaimanapun, setelah pengubahsuaian dilakukan terhadap algoritma SLIM, kerawakan output daripada algoritma SLIM terubah suai menunjukkan peningkatan sebanyak 22.22% kadar kerawakan.

JADUAL 9. Keputusan ujian kerawakan bagi pusingan penuh algoritma SLIM

Kategori Data	1	2	3	4	5	6	7	8	9
Block Frequency	L	L	L	L	L	L	L	L	L
Non-Overlapping Templates	G(7)	G(15)	L	G(1)	G(1)	G(2)	G(1)	G(3)	G(1)
Overlapping Template	L	L	L	L	L	L	L	L	L
Maurer's Universal	L	L	L	L	L	L	L	L	L
Linear Complexity	L	L	L	L	L	L	L	L	L
Serial	G(1)	G(1)	L	L	L	L	L	L	L
Approximate Entropy	L	L	L	L	L	L	L	L	G(1)
Frequency	L	L	L	L	L	L	L	L	L
Runs	L	L	L	L	L	L	L	L	L
Longest Runs of Ones	L	L	L	L	L	L	L	L	L
Binary Matrix Rank	L	L	L	L	L	L	L	L	L
Spectral	L	L	L	L	L	L	L	L	L
Cumulative Sums (*Forward and Reverse*)	L	L	L	L	L	L	L	L	L
Random Excursion	L	L	L	L	L	L	L	L	L
Random Excursion Variant	L	L	L	L	L	L	L	L	L

1 = Strict Key Avalanche, 2 = Strict Plaintext Avalanche, 3 = Plaintext Ciphertext Correlation, 4 = Cipher Block Chaining,
5 = Random Plaintext Random Key, 6 = Low-Density Key, 7 = High-Density Key, 8 = Low-Density Plaintext, 9 = High-Density Plaintext

JADUAL 10. Keputusan ujian kerawakan bagi pusingan penuh algoritma SLIM terubah suai

Kategori data	1	2	3	4	5	6	7	8	9
Block Frequency	L	G(1)	L	L	L	L	L	L	L
Non-Overlapping Templates	G(5)	G(9)	L	L	G(1)	G(1)	L	G(2)	G(2)
Overlapping Template	L	L	L	L	L	L	L	L	L
Maurer's Universal	L	L	L	L	L	L	L	L	L
Linear Complexity	L	L	L	L	L	L	L	L	L
Serial	L	L	L	L	L	L	L	L	L
Approximate Entropy	L	L	L	L	L	L	L	L	L
Frequency	G(1)	L	L	L	L	L	L	L	L
Runs	G(1)	L	L	L	L	L	L	L	L
Longest Runs of Ones	L	L	L	L	L	L	L	L	L
Binary Matrix Rank	L	L	L	L	L	L	L	L	L
Spectral	L	L	L	L	L	L	L	L	L
Cumulative Sums (*Forward and Reverse*)	G(2)	L	L	L	L	L	L	L	L
Random Excursion	L	L	L	L	L	L	L	L	L
Random Excursion Variant	L	L	L	L	L	L	L	L	L

1 = Strict Key Avalanche, 2 = Strict Plaintext Avalanche, 3 = Plaintext Ciphertext Correlation, 4 = Cipher Block Chaining,
5 = Random Plaintext Random Key, 6 = Low-Density Key, 7 = High-Density Key, 8 = Low-Density Plaintext, 9 = High-Density Plaintext

KESIMPULAN

Dengan menggunakan Suit Ujian Statistik NIST, analisis kerawakan berdasarkan tahap keertian 1% telah dilakukan pada algoritma SLIM. Analisis ini telah dijalankan ke atas 100 sampel yang berada di bawah sembilan kategori data, iaitu *Strict Key Avalanche, Strict Plaintext Avalanche, Plaintext Ciphertext Correlation, Cipher Block Chaining, Random Plaintext Random Key, Low-Density Key, High-Density Key, Low-Density Plaintext* dan *High-Density Plaintext*. Tahap keertian telah ditetapkan kepada 0.01 untuk menentukan sama ada jujukan output yang dihasilkan daripada algoritma adalah rawak ataupun tidak. Hasilnya menunjukkan bahawa jujukan output yang dijana daripada SLIM pada asasnya adalah tidak rawak berdasarkan tahap keertian 1%.

Mengambil kira kepentingan jujukan output yang baik, pengubahsuaian telah dilakukan terhadap algoritma SLIM. Algoritma penjanaan kekunci telah diubah suai mengguna pakai algoritma penjanaan kekunci daripada algoritma PRESENT. Berdasarkan analisis kerawakan yang telah dilakukan didapati kerawakan jujukan output daripada algoritma SLIM terubah suai menunjukkan peningkatan sebanyak 22.22% kadar kerawakan berbanding algoritma asalnya. Pengubahsuaian yang dibuat kepada algoritma asal meningkatkan keputusan analisis kerawakan mengguna pakai sampel yang sama. Secara umumnya, ini membuktikan bahawa algoritma yang diubah suai dapat mengurangkan sifat tidak rawak bagi teks sifer berbanding algoritma asal. Kerawakan output daripada sesuatu algoritma kriptografi adalah sangat penting. Algoritma yang melepasi semua ujian statistik tidak menjamin keselamatannya. Walau bagaimanapun, algoritma selamat harus lulus semua ujian (Zakaria et al. 2020).

Seperti yang telah dibincangkan, keputusan ujian kerawakan bagi algoritma asal SLIM bagi kategori data *Strict Key Avalanche, Strict Plaintext Avalanche, Cipher Block Chaining, Random Plaintext Random Key, Low-Density Key, High-Density Key, Low-Density Plaintext* dan *High-Density Plaintext* adalah gagal. Oleh itu, adalah dinasihatkan kepada pengguna untuk berhati-hati dalam menggunakan input teks biasa dan input kekunci apabila menggunakan algoritma SLIM. Selain itu, pengguna boleh memilih untuk menggunakan algoritma SLIM terubah suai yang telah dicadangkan bagi mendapatkan jujukan output yang mempunyai kerawakan yang lebih baik.

PENGHARGAAN

Kajian ini telah dibiayai oleh Kementerian Pengajian Tinggi (KPT) Malaysia di bawah projek Fundamental Research Grant (FRGS) no. FRGS/1/2020/STG06/UKM/02/2. Penulis ingin mengucapkan terima kasih kepada Presiden Kanan CyberSecurity Malaysia, Dr Maslina Daud dan Jabatan Pembangunan Kriptografi, CyberSecurity Malaysia atas saranan dan cadangan menambahbaikan makalah yang diberikan. Penulis juga ingin mengucapkan terima kasih kepada editor dan semua pengulas tanpa nama atas komen berharga mereka.

RUJUKAN

Aboushosha, B., Ramadan, R.A., Dwivedi, A.D., El-Sayed, A. & Dessouky, M.M. 2020. SLIM: A lightweight block cipher for internet of health things. *IEEE Access* 8: 203747-203757. doi:10.1109/ACCESS.2020.3036589

Alani, M.M. 2010. Testing randomness in ciphertext of block-ciphers using DieHard tests. *Int. J. Comput. Sci. Netw. Secur*. 10(4): 53-57.

Bassham, L.E., Rukhin, A.L., Soto, J., Nechvatal, J.R., Smid, M.E., Leigh, S.D., Levenson, M., Vangel, M., Heckert, N.A. & Banks, D.L. 2010. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *Nist Special Publication 800-22 Rev. 1a*.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. & Wingers, L. 2015. The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference.* pp. 1-6.

Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y. & Vikkelsoe, C. 2007. PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2007. Lecture Notes in Computer Science,* vol 4727, edited by Paillier, P. & Verbauwhede, I. Springer, Berlin, Heidelberg. pp. 450-466.

Fan, X., Mandal, K. & Gong, G. 2013. A lightweight stream cipher for resource-constrained smart devices. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks. 9th International Conference, QShine 2013,* Greader Noida, India, January 11-12. Revised Selected Papers.

Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B.S., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J. & Chee, S. 2006. HIGHT: A new block cipher suitable for low-resource device. In *Cryptographic Hardware and Embedded Systems - CHES 2006. Lecture Notes in Computer Science,* vol 4249, edited by Goubin, L. & Matsui, M. Springer, Berlin, Heidelberg.

ISO/IEC 29192.2: 2012. I. (2012). Information technology - Security techniques–lightweight cryptography–part 2: block ciphers.

ISO/IEC 18033-3: 2010. I. (2010). Information technology - Security techniques - Encryption - Part 3: Block ciphers.

Kumpulan Fokus MySEAL. 2018. Projek MySEAL: Kriteria Penyerahan dan Penilaian. Malaysia. https://myseal.cybersecurity.my/en/files/CD-5-RPT-0218-Kriteria_MySEAL_Versi_2.0-V1a.pdf

L'ecuyer, P. & Simard, R. 2007. TestU01: AC library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS)* 33(4): 1-40.

Lot, N.H., Abdullah, N.A.N. & Rani, H.A. 2011. Statistical analysis on KATAN block cipher. In *2011 International Conference on Research and Innovation in Information Systems IEEE*. pp. 1-6.

McKay, K.A., Bassham, L., Turan, M.S. & Mouha, N. 2017. *NISTIR 8114 Report on Lightweight Cryptography*. National Institute of Standards and Technology (NIST). Gaithersburg.

Shah, I.N.M., Rani, H.A., Ahmad, M.M. & Ismail, E.S. 2019. Cryptographic randomness analysis on Simon32/64. *International Journal of Cryptology Research* 9(1): 1-18.

Mohammad Shah, I.N., Nizam Chew, L.C., Mohd Yusof, N.A., Nik Abdullah, N.A., Lot @ Ahmad Zawawi, N.H. & Abdul Rani, H. 2015. Statistical analysis on lightweight block cipher, SIMON. *International Journal of Cryptology Research* 5(2): 28-43.

Mohammad Shah, I.N. & Ismail, E.S. 2020. Randomness analysis on lightweight block cipher, PRESENT. *Journal of Computer Science* 16(11): 1639-1647.

Murph, D. 2022. Engadget. https://www.engadget.com/2007-03-25-sony-develops-new-clefia-drm.html

Nik Abdullah, N.A., Lot Ahmad Zawawi, N.H. & Abdul Rani, H. 2011. Analysis on lightweight block cipher, KTANTAN. *7th International Conference on Information Assurance and Security (IAS),* Malacca, Malaysia. pp. 46-51.

Nik Abdullah, N.A., Nizam Chew, L.C., Zakaria, A.A., Seman, K. & Md Norwawi, N. 2015. The comparative study of randomness analysis between modified version of lblock block cipher and its original design. *International Journal of Computer and Information Technology* 4(6): 867-875.

Nik Abdullah, N.A., Seman, K. & Md Norwawi, N. 2014. Statistical analysis on lblock block cipher. *International Conference on Mathematical Sciences and Statistics 2013.* Singapore: Springer. pp. 233-245.

Nizam Chew, L.C., Mohammad Shah, I.N., Nik Abdullah, N.A., Ahmad Zawawi, N.H., Abdul Rani, H. & Zakaria, A.A. 2015. Randomness analysis on speck family of lightweight block cipher. *International Journal of Cryptology Research* 5(1): 44-60.

Rana, M., Mamun, Q. & Islam, R. 2020. *Current Lightweight Cryptography Protocols in Smart City IoT Networks: A Survey*. arXiv preprint arXiv:2010.00852.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S. & Iwata, T. 2007. The 128-bit blockcipher CLEFIA (Extended Abstract). In *Fast Software Encryption*. FSE 2007. Lecture Notes in Computer Science, vol 4593. Berlin, Heidelberg: Springer. pp. 181-195.

Soto, J. 1999. *NISTIR 6390: Randomness Testing of the Advanced Encryption Standard Candidate Algorithms.*

Zakaria, A.A., Azni, A.H., Ridzuan, F., Zakaria, N.H. & Daud, M. 2020. Randomness tests on nine data categories of RECTANGLE using NIST statistical test suite. *International Journal of Cryptology Research* 10(2): 1-22.

*Pengarang untuk surat-menyurat; email: p111700@siswa.ukm.edu.my