JIKO (JURNAL INFORMATIKA DAN KOMPUTER)
Februari 2024, Volume: **8**, No. **1** | Pages 253–267
doi: 10.26798/jiko.v8i1.1331
e-ISSN : 2477-3964 – p-ISSN : 2477-4413

ARTICLE

DESAIN LFSR SKEMA A5/1 DENGAN SEMBILAN FUNGSI UNTUK PENGAMANAN SERTIFIKAT TANAH DIGITAL

Samuel Danny Nugroho,[*,1] Eko Sediyono,[2] dan Irwan Sembiring[2]

[1]Magister Sisitem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga
[2]Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga
*Penulis Korespondensi: 972020703@student.uksw.edu,samueldanny89@gmail.com

(Disubmit 24-06-04; Diterima 24-06-14; Dipublikasikan online pada 24-09-05)

Abstrak
Penelitian ini merancang Linear Feedback Shift Register (LFSR) skema A5/1 menggunakan sembilan fungsi umpan balik, dan mengimplementasikan dalam sistem pengamanan sertifikat tanah digital menggunakan *hybrid* kriptografi dengan menggubungkan algoritma RSA dan Stream Cipher Rabbit. Hasil pengujian diperoleh, rancangan algoritma dapat menghasilkan luaran bit yang lebih acak dan konsisten dibandingkan dengan penggunan blok fungsi yang lebih kecil. Proses enkripsi dan dekripsi menunjukan rancangan Hybrid RSA-Rabbit merupakan algoritma yang optimum, karena memiliki kompleksitas waktu dan memori yang minimum. Pengujian korelasi menunjukkan plainteks dan cipherteks tidak berhubungan secara statistik, bahkan dalam kriteria Guilford berada dalam kategori "sedikit". Sehingga rancangan algoritma dapat menyembunyikan informasi penting pada sertifikat. Hasil ini menunjukkan bahwa rancangan Hybrid RSA-Rabbit dan dapat digunakan dalam mengamankan sertifikat tanah digital dan dapat diimplementasikan sebagai algoritma sertifikat tanah digital yang berjalan secara *real-time*.

Kata kunci: Linear Feedback Shift Register Skema A5/1, Hybrid RSA-Rabbit, Sertifikat Tanah Digital.

Abstract
This study designed an Linear Feedback Shift Register (LFSR) scheme A5/1 using nine feedback functions and implemented it in a digital land title security system using hybrid cryptography, combining the RSA and Stream Cipher Rabbit algorithms. The results of the testing showed that the designed algorithm produced more random and consistent bit outputs than the use of smaller block functions. The encryption and decryption processes demonstrated that the hybrid RSA-Rabbit algorithm is optimal in terms of time and memory complexity. The correlation testing indicated that the plaintext and ciphertext were not statistically correlated, even within the Guilford criteria, which was classified as "slight." This indicates that the algorithm can effectively conceal critical information in digital certificates. The results demonstrate that the Hybrid RSA-Rabbit design can be employed to safeguard digital land certificates and implemented as a real-time digital land certificate algorithm.

KeyWords: Linear Feedback Shift Register A5/1 Scheme, Hybrid RSA-Rabbit, Digital Land Certificate.

1. Pendahuluan

Kerahasiaan kunci dalam sistem kriptografi menjadi hal yang wajib untuk tidak diketahui oleh orang lain yang tidak memiliki otoritas dalam sistem tersebut, dengan demikian data dalam sistem tersebut dapat terjaga. Selain itu, pembangkitan kunci juga menjadi proses yang penting, sehingga dengan berbagai variasi input kunci yang digunakan dapat menghasilkan kunci yang acak. Salah satu algoritma pembangkit kunci yang baik adalah LFSR dengan skema A5/1, dimana dapat menghasilkan urutan bit yang acak dengan pro-

How to Cite: S. D. Nugroho *et al.*, "DESAIN LFSR SKEMA A5/1 DENGAN SEMBILAN FUNGSI UNTUK PENGAMANAN SERTIFIKAT TANAH DIGITAL", *JIKO (JURNAL INFORMATIKA DAN KOMPUTER)*, Volume: **8**, No.**1**, Pages 253–267, Februari 2024, doi: 10.26798/jiko.v8i1.1331.

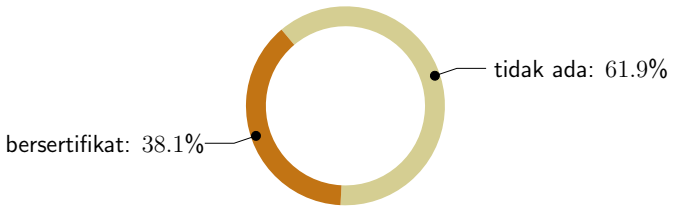
ses yang cepat. Beberapa penelitian sebelumnya juga telah mengembangkan berbagai fungsi XOR dalam setiap blok untuk mendapatkan urutan kunci yang baik. Penelitian [1] menggunakan tiga blok fungsi XOR, dan membandingkan dengan penelitian [2] dengan empat blok, [3] menggunakan lima blok, [4] dengan enam blok, selanjutnya Penelitian [5] tujuh blok. Hasil dari Penelitian [1] dengan pengujian berbagai variasi input diperoleh, algoritma yang menggunakan lebih banyak blok mempunyai rata-rata nilai *p-value* yang lebih tinggi untuk pengujian statistika. Sehingga dengan meningkatkan banyak blok fungsi umpan balik dapat meningkatkan variasi keacakan dari luaran bit yang dihasilkan.

Peningkatan jumlah blok dengan variasi fungsi umpan balik dari algoritma LFSR A5/1 tentunya akan menghasilakn kunci yang baik dalam kriptografi. Dengan demikian, kunci tersebut bila digunakan dalam sistem pengamanan informasi apat meninggkan jaminan keamanan pada sistem tersebut. Banyak kasus yang terjadi di Indonesia yang membutuhkan sisitem kriptografi untuk mengamankan data dan menjamin keaslian data tersebut. Salah satunya adalah masalah sertifikat tanah. Perkembangan teknologi yang begitu maju dengan signifikan, berimplikasi juga pada tindakan kejahatan dalam pemalsuan sertifikat tanah di Indonesia. Banyak kasus yang terjadi, misalnya tindakan percetakan sertifikat palsu yang sama dengan aslinya, penjualan sertifikat palsu, proses manipulasi data, penggadaan sertifikat, perubahan status tanah dan juga yang lainnya [6]-[9].

Tabel 1. Kasus Sertifikat Tanah [10]

No	Provinsi	Presentase Kasus Sertifikat Tanah
1	Bali	79%
2	Papua	77%
3	Jawa Timur	81%
4	Jakarta	61%
5	Papua Barat	76%

The Global Economy menyatakan bahwa industri lahan dan pertanian memberikan kontribusi lebih besar terhadap perekonomian Indonesia dibandingkan sektor lainnya, dan juga Agriculture Development Index menyatakan hampir 50% masyarakat di Indonesia berhubungan dengan sektor lahan pertanian [10]. Setiap masyarakat akan membutuhkan lahan yang cukup untuk meningkatkan perekonomian, dan akhirnya masalah kepemilikan tanah mejadi hal yang penting. Kondisi ini tergambar pada beberapa propinsi di Indonesia, dengan banyak kasus sertifikat tanah palsu yang diajukan ke pengadilan, seperti yang diberikan pada Tabel 1. Tentunya kejadian seperti ini akan meresahkan dan sangat merugikan masyarakat. Dalam hal ini, pemerintah atau instansi terkait perlu menerapkan sistem manajemen dan layanan yang baik kepada masyrakat [11], khususnya sistem pengelolaan kepemilikan tanah [12]. Aspek hukum juga menjadi salah satu masalah yang harus diperhatikan dengan serius [13], terutama kepastian kepemilikan yang sah yang dapat dibuktikan secara hukum [14], [16], [17].



Gambar 1. Tanah Bersertifikat di Indonesia

Sejak 1945, 72 tahun kemerdekaan, Indonesia mempunyai total 126 juta bidang tanah, tapi yang bersertifikat hanya 46 juta bidang tanah [18]. Jika divisualisasikan dalam diagram lingkaran pada Gambar 1, hampir 70% tanah di Indonesia yang tidak bersertifikat, sudah tentu akan menjadi sumber masalah. Berbagai permasalahan sertifikat tanah yang terjadi, tentunya berbading lurus dengan banyak kasus yang ada, oleh karena itu diperlukan pengelolaan sistem sertifikat tanah yang dapat menjamin keasliannya, mencegah terjadinya penipuan dan juga manipulasi data. Disisi lain Undang-Undang ITE nomor 11 Tahun 2008,

Peraturan Menteri Negara Agraria / Kepala Badan Pertanahan Nasional nomor 3 Tahun 1997, dan seterusnya., mengenai pemanfaatan data elektronik, prosedur transaksi elektronik, keamanan legalitas data melalui tanda tangan elektronik pengelolaan data digital, akses informasi pertanahan kepada publik, dan pembatasan informasi pertanahan kepada publik yang bersifat pribadi.

Badan Pertanahan Nasional (BPN) telah mengumumkan penggunaan sertifikat tanah digital, dan diatur dalam Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional No.1/2021 pada tanggal 21 Januari 2021. Masalahnya BPN tidak secara eksplisit menyatakan algoritma kriptografi yang digunakan untuk mengamankan data sertifikat tanah, sehingga kritik dan saran tidak dapat diberikan secara maksimal. Prinsip Kerckhoffs tentang sistem pengamanan informasi menyatakan, algortima harus publik dan hanya kunci yang rahasia. Untuk kasus ini, BPN tidak mengikuti prinsip tersebut. Terlepas dari tidak ada informasi penggunaan algoritma, dalam menentukan algoritma yang digunakan menjadi sebuah masalah tersendiri. Terutama spesifikasi algoritma dengan kebutuhan dalam perancangan aplikasi, tentunya kesalahan memilih algoritma akan membebani proses dari aplikasi yang dirancang.

Terkait dengan pemilihan algoritma, penelitian [19] menyatakan bahwa algoritma yang rekomendasi National Institute of Standards and Technology (NIST) yaitu Data Encryption Standard (DES) dan Advaced Encryption Standard (AES) masih menjadi pilihan terbanyak bagi para kriptografer untuk menggunakannya sebagai pengamanan informasi [20]-[41]. Disisi lain, beberapa penelitian juga menyatakan telah memecahkan algoritma DES maupun penggantinya yaitu AES [42]-[47]. Pada kriptografi, kompleksitas waktu dan memori selalu berbanding terbalik dengan tingkat kemanan dari algoritma, hal ini membuat kriptografer berlomba-lomba untuk menciptakan dan atau menggunakan algoritma yang optimum, dimana kompleksitas rendah tetapi jaminan keamanan tinggi.

Salah satu yang dilakukan saat ini adalah menggunakan kriptografi *hybrid*, dimana distribusi data menggunakan algoritma simetris dan pembangkitan kunci dengan algoritma simetris [48]-[50]. Sehingga kompleksitas waktu dan memori dan juga faktor keamanan dapat terjamin. Masalah pengamanan data pada sertifikat tanah digital menjadi hal yang sangat penting, apalagi dikaitkan dengan penggunaan algoritma kriptografi. BPN yang mempunyai otoritas untuk menentukan keaslian sertifikat digital, dan secara paralel juga pemilik tanah mempunyai hak kepemilikan tanah harus mempunyai akses yang sah untuk menyatakan bahwa tidak ada kepemilikan ganda pada tanah yang dimilikinya.

Tabel 2. Penelitian Hybrid Kriptografi

No	Algoritma Asimetris	Algoritma Simetris	Referensi
1	RSA	AES	[51], [52], [61], [63], [65], [66], [68], [69], [70]
2	RSA	Blowfish	[53], [68]
3	RSA	Playfair	[55], [64]
4	RSA	DES	[67]
5	RSA	Twofish	[70]
6	RSA	Rabbit	[71]
7	ECC	AES	[54], [56], [58]
8	ECC	Blowfish	[57]
9	ECC	Twofish	[60]
10	ECC	Hill Cipher	[59]
11	ECC	DES	[62]

Tabel 2 merupakan penelitian terkait dengan kriptografi hybrid, dimana penggunaan kriptgafi AES merupakan presentase terbesar yaitu sebanyak 39%, seperti yang dijelaskan sebelumnya, bahwa AES masih menjadi pilihan dalam pemelihan algoritma. Penelitian ini merancang sistem pengamanan sertifikat tanah digital menggunakan kriptografi *hybrid* dengan Stream Cipher Rabbit sebagai algoritma untuk distribusi data dan RSA sebagai pengamanan kunci. Kombinasi RSA dan Rabbit dalam hybrid kriptografi memberikan keunggulan yang komplementer. RSA digunakan untuk mengamankan pertukaran kunci dan memverifikasi keaslian sertifikat tanah, sementara Rabbit digunakan untuk mengamankan data yang dikirim atau

disimpan setelah proses pertukaran kunci.

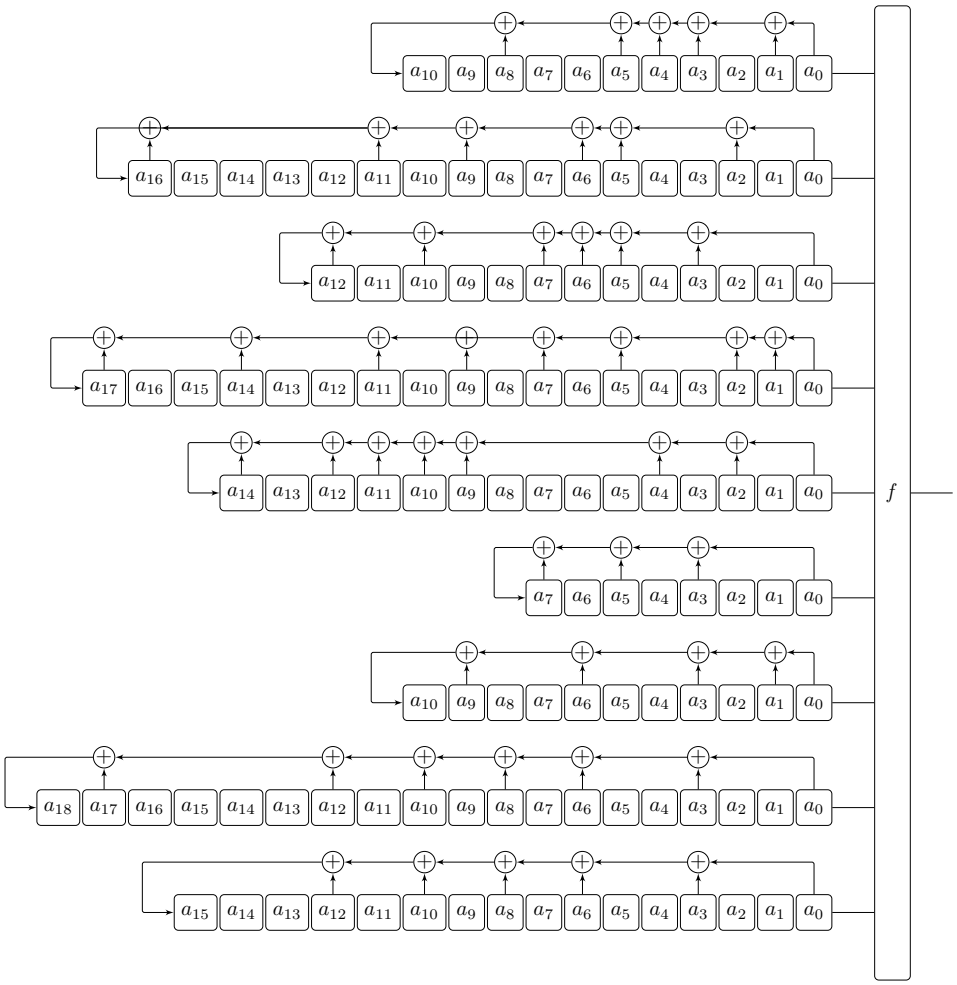
Boesgaard & Scavenius [72] [73], [74] mengatakan Rabbit menjadi stream chiper yang mempunyai performa yang baik, terutama dalam masalah kompleksitas waktu dan memori. Algoritma Rabbit dipilih dan bukan block cipher sebagai algoritma distribusi data, karena secara keseluruhan sertifikat tanah digital mempunyai ukuran yang hampir sama, yang membedakan hanya identitas pemilik dan peta lokasi tanah. Stream cipher menjadi pilihan yang tepat, karena proses enkripsi langsung dilakukan sesuai dengan ukuran file sertifikat. Sebaliknya, apabila dipilih *block cipher* tentunya akan membebani waktu komputasi, karena secara otomatis akan ada proses partisi data yang sesuai dengan panjang blok kunci, baru kemudiaan dilakukan proses enkripsi, sehingga dari kompleksitas waktu dan ruang tentunya akan kurang optimum. Selain itu penelitian ini mendesain pembangkit kunci berbasis *Linear-Feedback Shift Register* (LFSR) yang digunakan sebagai inisialisasi pada kriptografi Rabbit, hal ini dilakukan untuk meningkatkan keamanan informasi secara berlapis.

2. Rancangan Algoritma

Bagian ini membahas rancangan algoritma LFSR A5/1 dengan sembilan fungsi umpan balik, yang kemudian digunakan dalam sistem pengamanan sertifikat digital.

2.1 Rancangan LFSR A5/1

Rancangan LFSR yang ditunjukkan pada Gambar 2, digunakan sembilan fungsi umpan balik dan input yang digunakan adalah 128-bit. Setiap kelompok bit, (K_i), dimana $i = 1, 2, \cdots, 9$, terbagi dalam ukuran bit yang berbeda. Kelompok pertama $K_1 = \{a_0, a_1, a_2, \cdots, a_{10}\}$, sedangkan kedua $K_2 = \{a_0, a_1, a_2, \cdots, a_{16}\}$, dan $K_3 = \{a_0, a_1, a_1, \cdots, a_{12}\}$, sampai dengan kesembilan $K_9 = \{a_0, a_1, a_2, \cdots, a_{15}\}$.



Gambar 2. Rancangan LFSR skema A5/1 dengan 9 Fungsi Umpan Balik

Setiap K_i digunakan sebagai input pada proses fungsi XOR, dinamakan sebagai fungsi umpan balik. Setiap fungsi umpan balik dinotasikan sebagai A_i, untuk $i = 1, 2, \cdots, 9$. Persamaan 1 adalah proses fungsi XOR secara lengkap untuk setiap kelompok bit. Secara keseluruhan, untuk memperoleh luaran dari LFSR dilakukan operasi XOR untuk sembilan fungsi umpan balik yang telah diperoleh. Model secara umum diberikan pada Persamaan 1.

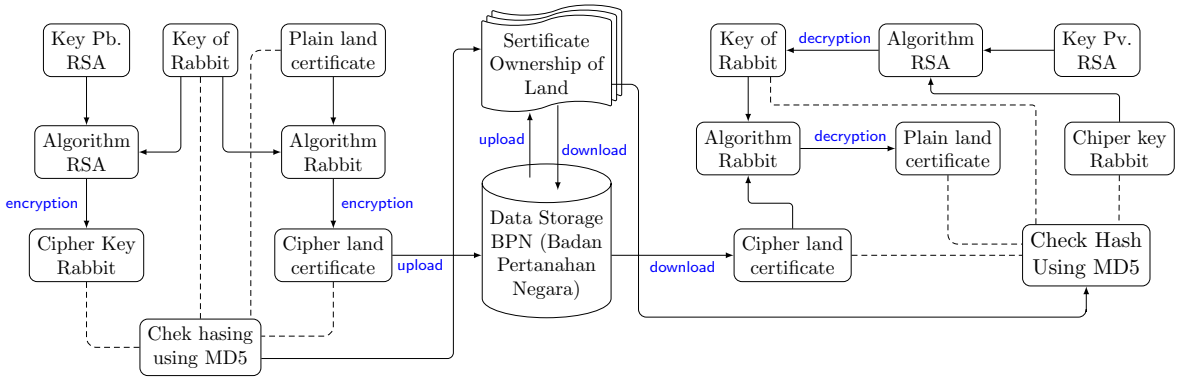
$$f = A_1 \oplus A_2 \oplus A_3 \oplus A_4 \oplus A_5 \oplus A_6 \oplus A_7 \oplus A_8 \oplus A_9 \tag{1}$$

Setiap $a_j \in A_i$ digunakan secara khusus untuk penentuan fungsi umpan balik. Misalkan untuk blok pertama (A_1), dimana $j = 1, 2, \cdots, 10$, fungsi XOR yang digunakan adalah $a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_8$. Penggabungan setiap a_j pada masing-masing fungsi umpan balik A_i merupakan sebuah salah satu algoritma terbaik dalam menghasilkan bilangan acak dengan *p-value* tertinggi. Fungsi umpan balik dari blok yang lain secara lengkap diberikan pada Persamaan 2.

$$\begin{aligned}
A_1 &= a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_8 \\
A_2 &= a_0 \oplus a_2 \oplus a_5 \oplus a_6 \oplus a_9 \oplus a_{11} \oplus a_{16} \\
A_3 &= a_0 \oplus a_3 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus a_{12} \\
A_4 &= a_0 \oplus a_1 \oplus a_2 \oplus a_5 \oplus a_7 \oplus a_9 \oplus a_{11} \oplus a_{14} \oplus a_{17} \\
A_5 &= a_0 \oplus a_2 \oplus a_4 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{14} \\
A_6 &= a_0 \oplus a_3 \oplus a_5 \oplus a_7 \\
A_7 &= a_0 \oplus a_1 \oplus a_3 \oplus a_6 \oplus a_9 \\
A_8 &= a_0 \oplus a_3 \oplus a_6 \oplus a_8 \oplus a_{10} \oplus a_{12} \oplus a_{17} \\
A_9 &= a_0 \oplus a_3 \oplus a_6 \oplus a_8 \oplus a_{10} \oplus a_{12} \oplus a_{15}
\end{aligned} \tag{2}$$

2.2 Rancangan Kriptografi Hybrit

Rancangan algoritma kriptografi hybrit dengan RSA dan Rabbit, untuk pengamanan sertifikat tanah digital diberikan pada Gambar 3. Selanjutnya, proses enkripsi dan dekripsi secara umum secara berturut-turut diberikan dalam Algoritma 1 dan Algoritma 2.



Gambar 3. Hybrid algorithm flowchart

Algorithm 1 Proses Enkripsi

```
Start
Input Key_Pb_RSA
Input Plain_Land_Certificate
Key_Rabbit = Generate_Key_Rabbit()
Cipher_Land_Certificate = Rabbit_Encrypt(Plain_Land_Certificate, Key_Rabbit)
Cipher_Key_Rabbit = RSA_Encrypt(Key_Rabbit, Key_Pb_RSA)
Hash_Cipher_Land_Certificate = MD5_Hash(Cipher_Land_Certificate)
Upload_To_BPN(Cipher_Key_Rabbit, Cipher_Land_Certificate, Hash_Cipher_Land_Certificate)
Print "Data terenkripsi dan disimpan di BPN"
End
```

Algorithm 2 Proses Dekripsi

```
Start
Input Key_Pv_RSA
(Cipher_Key_Rabbit, Cipher_Land_Certificate, Hash_Cipher_Land_Certificate) = Download_From_BPN()
Key_Rabbit = RSA_Decrypt(Cipher_Key_Rabbit, Key_Pv_RSA)
Plain_Land_Certificate = Rabbit_Decrypt(Cipher_Land_Certificate, Key_Rabbit)
Hash_Verified = MD5_Hash(Plain_Land_Certificate)
if Hash_Verified == Hash_Cipher_Land_Certificate then
    Print "Hash verifikasi cocok. Data sertifikat tanah asli."
    Print Plain_Land_Certificate
else
    Print "Hash verifikasi tidak cocok. Data sertifikat tanah mungkin telah diubah."
end if
End
```

3. Hasil dan Pembahasan

3.1 Proses Pembangkitan Kunci

Penggunaan kriptografi stream cipher tentunya akan memerlukan panjang kunci sama dengan panjang plainteks. Pembuatan sertifikat dimulai dengan input kunci, hanya saja setiap user tidak akan punya kemampuan untuk dapat mengingat kunci yang sangat panjang. Oleh karena itu dirancang sebuah skema yang dapat menggunakan kunci yang diinput user, kemudian dilakukan proses pembangkitan kunci sehingga dapat memenuhi kebutuhan pada algoritma Rabbit.

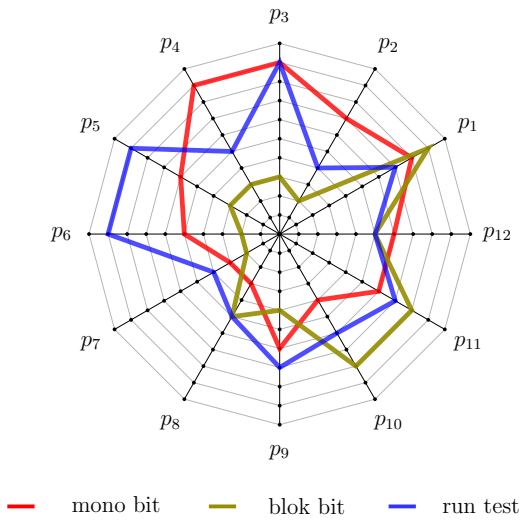
Algorithm 3 Pembangkitan Kunci Rabbit

```
Start
Input key
if length(key) ≤ 6 then
    key = key + padding
end if
generated_key = LFSR(key)
encrypted_data = rabbit_algorithm(generated_key)
Print encrypted_data
End
```

Algoritma 3 adalah proses pembangkitan kunci pada algoritma Rabbit, setiap kunci yang diinput user $K = \{x_1, x_2, \cdots, x_n\}$, dengan syarat $n = 6$, apabila $n \neq 6$ maka proses *padding* dengan karakter spasi (setara dengan 32 dalam ASCII) sehingga akan memenuhi 6 karakter ASCII. Penetapan 6 karekter sebagai kunci dengan memperhatikan kemampuan user dalam mengingat kunci, dan disisi lain masyaratkat Indonesia sudah terbiasa dengan mengingat dan mempunyai kemampuan untuk mengingat PIN ATM. Setelah setiap input kunci yang telah memenuhi 6 karakter ASCII, tahap selanjutnya adalah proses pembangkitan kunci dengan meregenerasi 48 bit menjadi 128 bit. Kunci 128-bit menjadi input untuk LFSR yang diberikan pada Gambar 2 sebelumnya, dan luaran dari LFSR kemudian akan menjadi input pada kriptografi stream cipher Rabbit, yang dimana sudah dibahas pada Algoritma 1 dan Algoritma 2.

3.2 Pengujian Keacakan

Pengujian statistik yang digunakan adalah monobit, blok bit, dan uns test, digunakan derajat kebebasan $\alpha = 1\%$, setiap $p\text{-}value > \alpha$ maka urutan bit berada dalam kategori acak, sebaliknya $p\text{-}value \leq \alpha$ maka urutan bit yang dihasilkan tidak acak. Pengujian ini akan memastikan apakah setiap kunci yang dibangkitkan benar merupakan urutan bit yang acak sehingga dapat digunakan sebagai kunci. Digunakan dua belas input (p_i) untuk $i = 1, 2, \cdots, 12$. Dua belas input diberikan pada Tabel 3 adalah variasi input yang sering digunakan sebagai input kunci. Secara umum menggunakan tiga model kombinasi huruf, pertama adalah kata/teks biasa, kedua kombinasi huruf, angka, dan simbol, dan ketiga adalah teks yang sama.



Gambar 4. Visualisasi Pengujian Keacakan

Hasil pengujian dengan rancangan algoritma LFSR ditunjukkan secara visual menggunakan diagram radar pada Gambar 4. Digunakan 12 rusuk (p_i), dimana setip rusuk terdiri dari 10 untuk nilai dari *p-value*, yaitu $(0.0, 0.1, 0.2, \cdots, 1.0)$. Hasil yang diperoleh untuk setiap pengujian diperoleh *p-value* dengan berbeda, dan juga lebih besar dari $\alpha = 1\%$. Nampak semua pengujian menghasilkan hasil yang bervariasi, tetapi berdasarkan hasil tersebut nampak bahwa rancangan algoritma berhasil menghasilkan luaran urutan bit yang acak. Hasil ini menunjukkan bahwa rancangan LFSR berhasil sebagai pembangkit kunci pada kriptografi stream cipher.

3.3 Analisa Kekuatan Kunci LFSR

Secara teoritis bahawa pembangkitan kunci dengan LFSR mempunyai sifat periodik, dan akan menghasilkan pola bit yang sama pada urutan $2^n - 1$ dengan n adalah banyak input bit. Rancangan algoritma menggunakan input kunci sebanyak 6 karakter dengan padding, sehingga dalam LFSR diperoleh input bit $n = 128$, sehingga periodiknya adalah $2^{128} - 1$.

$$\text{banyak kelipatan bit} = \frac{2^{128} - 1}{128} = 265845599156983000000000000000000000000$$

Disisi lain, kunci untuk algoritma rabbit dalam sekali proses enkripsi maupun dekripsi hanya memerlukan 128 bit, sehingga rancangan LFSR dapat menyediakan $265845599156983 \times 10^{22}$ kelompok bit yang dapat digunakan. Hasil ini menunjukkan bahwa kebutuhan bit sebagai kunci pada algoritma Rabbit lebih kecil dari bit yang dihasilkan oleh proses pembangkitan kunci LFSR. Sehingga dapat menambah kekuatan dari algoritma hybrid, terutama dalam proses pemecahan kunci dengan penebakan secara langsung akan lebih sulit

3.4 Perbandingan dengan Algoritma Lain

Kemampuan algoritma dalam menghasilkan bilangan acak adalah tujuan dari pembangkitan LFSR. Bagian ini membandingkan dengan penelitian yang telah dilakukan sebelumnya. Tabel 3 menujukkan hasil pengujian secara lengkap, dengan tiga indikator pengujian statistik yaitu run test (RT), mono bit (MB) dan blok bit (BB).

Tabel 3. Perbandingan dengan LFSR Lainnya

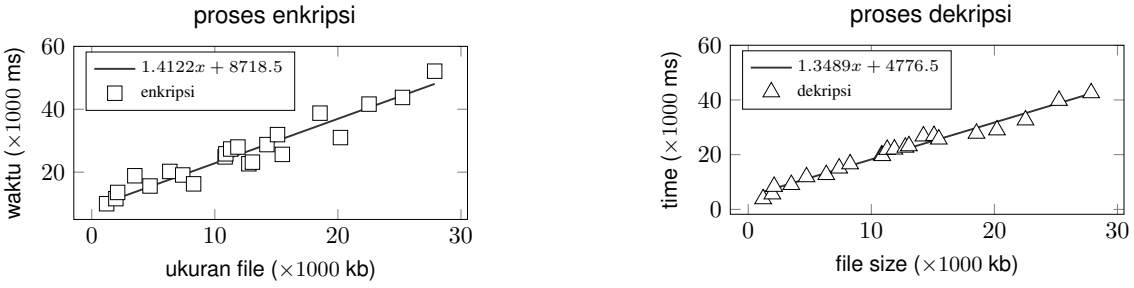
No	Input	RT	MB	BB	RT [2]	MB [2]	BB [2]	RT [1]	MB [1]	BB [1]
1	fti	0.841	1.000	0.781	0.688	0.841	0.259	0.895	0.424	0.629
2	ftj	0.741	0.230	0.476	0.869	0.072	0.668	0.906	0.549	0.928
3	$aL4t19A	0.960	0.317	0.986	0.977	0.230	0.629	0.725	0.317	0.140
4	$aL4t19B	0.565	0.230	0.551	0.960	0.317	0.373	0.385	0.009	0.140
5	xxxy	0.651	0.317	0.928	0.461	0.110	0.706	0.271	1.000	0.192
6	xxxx	0.565	0.230	0.976	0.790	0.072	0.815	0.748	0.016	0.125
7	uksw	0.278	0.028	0.213	0.688	0.841	0.213	0.611	0.689	0.976
8	uksv	0.321	0.689	0.100	0.818	0.230	0.706	0.816	0.424	0.947
9	25i+g1	0.665	0.424	0.781	0.489	0.689	0.781	0.622	0.689	0.551
10	25i+g2	0.483	0.841	0.668	0.453	0.072	0.070	0.741	0.230	0.629
11	baaaa	0.618	0.841	0.668	0.665	0.424	0.706	0.580	0.317	0.877
12	aaaaa	0.604	0.549	0.590	0.888	0.072	0.373	0.545	0.016	0.551
	Rataan	0.608	0.475	0.643	0.729	0.331	0.525	0.654	0.390	0.557

Berdasarkan input yang diberikan, nampak rancangan algoritma lebih unggul secara rata-rata untuk pengujian mono bit dan blok bit, tetapi run test masih lebih kecil dari Penelitian [2]. Secara keseluruhan, rancangan algoritma lebih konsisten dan dapat menghasilkan luaran yang acak, karena pada penelitian [2] pada input ke-2, ke-10 dan ke-12 menghasilkan *p-value* yang kecil, bahkan hampir diketegorikan tidak acak. Penelitian [1] untuk input ke-4 untuk pengujian mono bit berada dalam kondisi tidak acak. Sehingga secara keseluruhan, rancangan algoritma LFSR dengan sembilang fungsi pembangkit lebih baik dalam menghasilkan bilangan acak bila dibandingkan dengan penelitian sebelumnya.

3.5 Kompleksitas Waktu dan Memori Pengujian Sistem Kriptografi

Bagian ini melihat kompleksitas waktu dan memori, sehingga dapat mengetahui seberapa optimum algoritma dalam melakukan proses enkripsi dan dekripsi. Pengujian dilakukan dengan membuat digitalisasi sertifikat tanah yang telah dicetak sebagai data sampel, kemudian pembangkitan kunci dan proses enkripsi dilakukan seperti yang ditunjukkan pada Gambar 1. Dipilih 22 data sebagai sampel dan digunakan metode pecocokan kurva untuk memperoleh model dan mengetahui kemampuan algoritma berdasarkan karakteristik data hasil pengukuran.

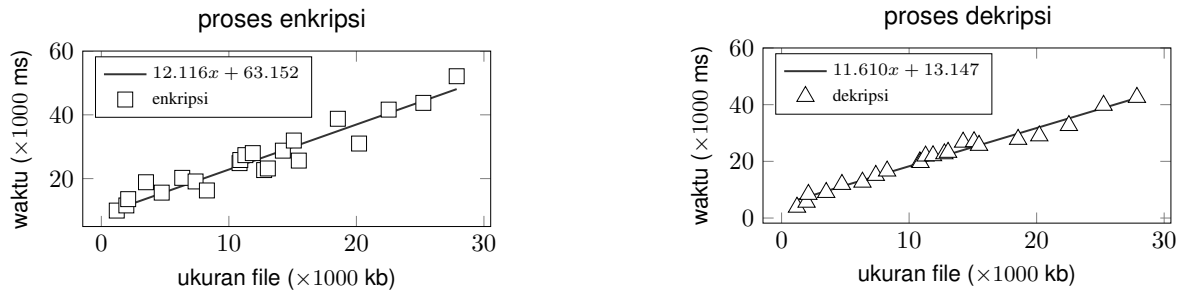
Hasil pengujian kebutuhan waktu dalam melakukan proses enkripsi maupun dekrispsi diberikan pada Gambar 5. Diperoleh model untuk enkripsi adalah $y = 1.4122 + 8718.5$ dengan $R^2 = 0.9174$ dan model untuk dekripsi adalah $y = 1.3489 + 4776.5$, $R^2 = 0.9773$. Nilai koefisen determinasi (R^2) dari proses enkripsi dan dekripsi mendekati 1, hasil ini menunjukkan bahwa model linier yang dipakai sangat mendekati dengan pola atau karakter data. Model linier yang diperoleh menginformasikan bahwa rancangan algoritma dalam melakukan enkripsi dan dekripsi memiliki kebutuhan waktu yang berbading lurus dengan besar ukuran sertifikat.



Gambar 5. Pengujian Kompleksitas Waktu

Secara umum jika ukuran file diperbesar, maka kebutuhan waktu juga akan meningkat, begitu juga sebaliknya kebutuhan waktu juga akan berkurang apabila size sertifikat yang kecil. Hal penting dalam model

enkripsi dengan model linier adalah kemiringan garis atau gradien yang menentukan seberapa cepat fungsi tersebut naik (*increasing*) atau turun (*decreasing*), sehingga dapat menilai krakteristik dari algoritma dalam kompleksitas waktu. Rancangan algoritma hybrid memperoleh gradien untuk enkripsi m_e = 1.4122 dan dekripsi m_d = 15.3, hasil ini memberikan informasi bahwa perbadingan waktu terhadap ukuran data tidak naik secara signifikan atau tidak memiliki sifat eksponensial. Secara kompleksitas waktu rancangan algoritma sangat baik dalam melakukan proses enkripsi maupun dekripsi, sehingga akan baik bila diimplementasikan sebagai pengamanan data pada sertifikat digital.



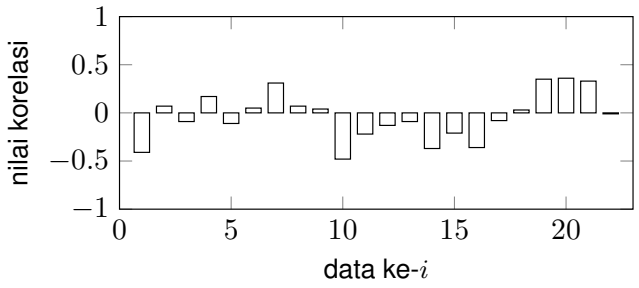
Gambar 6. Pengujian Kompleksitas Memori

Pengujian kompleksitas memori juga menggunakan metode pencocokan kurva, dan diperoleh model linier yang terbaik. Gambar 6 adalah model kebutuhan memori untuk proses enkripsi y = 12.116 + 63.152 dan model untuk proses deskripsi diperoleh y = 11.610x + 13.147. Nilai koefisien determinasi dari model enkripsi dan dekripsi secara berturut-turut adalah R^2 = 0.891 dan R^2 = 0.9228, keduanya mempunyai nilai yang mendekati satu, dengan demikian model yang diperoleh dapat menggambarkan karakteristik algoritma, dan dapat mewakilkan prilaku algoritma dalam proses enkrispsi-dekripsi.

Nilai gradien dari model eknkripsi m_e = 12.116, dan dekripsi adalah m_d = 1.3489, keduanya menunjukkan kemiringan yang tidak naik secara signifikan, sehingga rancangan algoritma tidak membutuhkan memori yang banyak dalam melakukan enkripsi dan dekripsi. Hasil ini tentu akan baik bila diimplementasikan sebagai algoritma sertifikat digital, karena dalam penggunaannya akan berjalan secara *real-time*.

3.6 Pengujian Enkripsi

Pengujian korelasi digunakan untuk melihat seberapa baik rancangan algoritma dalam mengubah plainteks menjadi cipheteks. Diketahui daerah hasil (*range*) dari nilai korelasi (r) berada dalam interval $-1 \leq r \leq 1$, dan secara statistik apabila nilai korelasi mendekati atau sama dengan 0, maka kedua variabel yang diukur mempunyai korelasi lemah atau tidak berkorelasi. Dalam kriptografi, algoritma berfungsi untuk menyamarkan informasi pada plainteks, akibatnya algoritma yang baik dapat menyembunyikan hubungan antara plainteks dan cipherteks. Pengujian korelasi dapat digunakan untuk mengukur seberapa baik algoritma bekerja, harapannya setiap algoritma mempunyai nilai korelasi yang mendekati nilai nol. Sehingga algoritma tersebut berhasil dalam menyembunyikan informasi penting dari plainteks.



Gambar 7. Hasil Pengujian Korelasi

Digunakan 22 data sertifikat untuk menguji kemampuan rancangan algoritma dalam menyamarkan in-

formasi. Hasil pengujian secara lengkap diberikan pada Gambar 7, dimana nilai korelasi yang diperoleh sangat bervariasi ada bernilai positif dan ada juga negatif. Walaupun bervariasi, hasil pengujian berada pada interval $-0.48 \leq x \leq 0.31$, dimana nilai korelasi yang memiliki jarak terjauh dengan nol ada pada data ke-sepuluh yaitu -0.48, sedangkan nilai terdekat adalah 0.04 pada data ke-sembilan. Interval daerah-hasil (*range*) dari nilai korelasi yang selalu lebih kecil dari 0.5 atau -0.5 menunjukkan bahwa rancangan algoritma secara konsisiten membuat plainteks tidak berhubungan dengan cipherteks. Selain itu, bila dilihat secara keseluruhan rata-rata mutlak dari nilai korelasi adalah 0.2, dan berdasarkan kriteria Guilford, berada dalam kategori "sedikit" atau bahkan "tidak mempunyai korelasi". Hasil ini menunjukkan bahwa rancangan algoritma sangat baik dalam menyembunyikan informasi penting pada sertifikat tanah. Sehingga algoritma hybrid menggunakan RSA-Rabbit dapat digunakan dalam mengamankan sertifikat tanah digital.

4. Conclusion

Rancangan algoritma LFSR A5/1 dengan sembilan fungsi umpan balik berhasil menghasilkan luaran bit yang acak walaupun digunakan input yang bervariasi. Selain itu rancangan algoritma secara rata-rata pada pengujian mono bit dan blok bit lebih baik bila dibandingkan dengan penelitian yang menggunakan blok fungsi umpan balik yang lebih sedikit. Rancangan algoritma juga mempunyai luaran bit acak yang lebih konsisten, sehingga dapat diimplementasikan pada sistem pengamanan sertifikat digital.

Pengujian korelasi menunjukkan kemampuan algoritma dalam melakukan enkripsi-dkekripsi sangat baik karena dapat membuat plainteks dan cipherteks tidak berhubungan secara statistik, bahkan dalam kriteria Guilford berada dalam kategori "sedikit". Sehingga menunjukkan bahwa rancangan algoritma menggunakan RSA-Rabbit dapat menyembunyikan informasi penting pada sertifikat tanah dan dapat digunakan dalam mengamankan sertifikat tanah digital.

Hasil pengujian sistem pengamanan sertifikat tanah digital mempunyai kebutuhan waktu dalam melakukan proses enkripsi diperoleh model $y = 1.4122x + 8718.5$ dan dekripsi $y = 1.3489x + 4776.5$. Pengujian kebutuhan memori juga diperoleh model linier, model enkripsi $y = 12.116 + 264.51$ dan dekripsi $y = 11.610x + 13.147$ Dengan diperoleh model linier memberikan informasi bahwa perbadingan waktu dan memori terhadap ukuran data tidak naik secara signifikan. Sehingga Hybrid RSA-Rabbit dapat menjadi algoritma yang optimum dalam melakukan enkripsi-dekripsi, kerena memiliki kebutuhan waktu dan memori yang minimum. Hasil ini tentu akan baik bila diimplementasikan sebagai algoritma sertifikat digital, karena dalam penggunaannya akan berjalan secara *real-time*.

Pustaka

[1] Ramadhani, A. & Wowor, A.D., *"Implemintasi Variasi Fungsi XOR dalam pembangkitan kunci LFSR pada skema A5/1 dengan tiga blok"*, Jurnal Informatika dan Komputer (JIKO), 8 (1), 161-173, 2024.

[2] Nahading, T. S., & Wowor, A. D., *"Desain Pembangkit Kunci LFSR dengan Skema A5/1 Menggunakan empat Blok Bit Fungsi XOR"*., Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen), 4(2), 409-419, 2023.

[3] Manullang, R. V., *"Desain Lima Fungsi Umpan Balik LFSR dengan Skema A5/1 sebagai Pembangkit Kunci Kriptografi Stream Cipher"*, Skripsi S-1 Prodi Teknik Informatika UKSW Salatiga, 2022.

[4] Nafurbenan, R. Maria, *"Perancangan Enam Bagan Fungsi XOR sebagai Umpan Balik sebagai Pembangkit Bilangan Acak LFSR dengan Skema A5/1"*. Skripsi S-1 Prodi Teknik Informatika UKSW Salatiga, 2022.

[5] A.J., Herman, *"Desain Pembangkit Kunci LFSR dengan Skema A5/1 Menggunakan 7 Blok Bit Fungsi XOR"*., Skripsi S-1 Prodi Teknik Informatika UKSW Salatiga, 2022.

[6] A. Tehupeiory, "Land mafia case handling through the optimalization of land mafia task force role," *SASI*, vol. 29, Issue 2, pp. 214-226, June. 2023, doi: 10.47268/sasi.v29i2.1185.

[7] A. Tehupeiory, "Factors influencing land mafia cases," *International Journal Of Artificial Intelegence Research*, vol. 6, no. 1, pp. 459-465, June. 2022, doi: https://doi.org/10.29099/ijair.v6i1.2.737.

[8] A. Tehupeiory, "Role model of eradicating the land mafia in Indonesia," *Baltic Journal of Law & Politics*, vol. 16, no. 3, pp 459-465, 2023, doi: 10.2478/bjlp-2023-0000040.

[9] Supriyono, "Study of dual certificate law in ownership of land rights," in *Proceedings of the 2nd International Conference on Law, Social Science, Economics, and Education (ICLSSEE)*, April. 2022, doi: 10.4108/eai.16-4-2022.2320069.

[10] A. Noor, "Legal status of electronic land certificates in the land case proof system in Indonesia," *International Journal of Cyber Criminology*, vol. 15, Issue 1, pp. 172-187, June. 2021, doi: 10.5281/zenodo.4766541.

[11] A.N. Wahidah, D.N. Martono, and Supriatna, "Land use sustainability to mitigate potential land slide in Ciletuh watershed, Sukabumi, Indonesia," in *IOP Conference Series: Earth and Environmental Science: 2nd International Seminar on Natural Resources and Environmental Management (2nd ISeNREM 2021) 4th-5th*, vol. 950, no. 1, August. 2022. doi: 10.1088/1755-1315/950/1/012006.

[12] B. Shantiko, N. Liswanti, R. Bourgeois, and Y. Laumonier, "Land-use decisions in complex commons: engaging multiple stakeholders through foresight and scenario building in Indonesia," *Environmental Management*, vol. 68, pp. 642-664, April. 2021. doi: https://doi.org/10.1007/s00267-021-01470-1.

[13] S. D. Suryani BR M and J. N. Saly, "Application of electronic land certificates in the Indonesian land system," *Injuruty: Interdiciplinary Journal and Humanity*, vol. 3, no. 1, pp. 172-187, January. 2024, doi: https://doi.org/10.58631/injurity.v3i1.157.

[14] I. Yuliawan, "Electronic land certificates in the perspective IUS constitutum and IUS constitutum in Semarang regency," in *The 1st Virtual International Conference on Economics, Law and Humanities*, vol. 1, no. 1, pp. 119-129, 2022.

[15] I.E. Sihombing, E. Pandamdari, D. Setyorini, and I. P. Probondaru, "Strengthening legal security of land security of legal security of land ownership based on Girik and village head land certificate," *International Journal of Social Health*, vol. 1, no. 1, pp. 119-129, June. 2022, doi: 10.58860/ijsh.v2i6.61.

[16] W. Brontowiyono, A. A. Asmara,R. Jana, A. Yulianto, and S. Rahmawati, "Land-Use Impact on Water Quality of the Opak Sub-Watershed, Yogyakarta, Indonesia," *Sustainability*, vol. 14, Issue 7, no. 4366, pp. 1-21, April. 2022, doi: 10.3390/su14074346.

[17] R. A. A. Jayanti, A. Asikin, and R. R. Cahyowati, "Legal Protection Model For Land Management Right Permit Holders For Investment In Indonesia," *PONTE: Multidisciplinary Journal of Sciences and Research*, vol. 75, no. 2, pp. 65-71, 2019. doi: 10.21506/j.ponte.2019.09.19

[18] H. Purwnato, "President distributes 2,550 land certificates in Central Java," *Antara Website*, June. 2017 https://en.antaranews.com/news/111410/president-distributes-2550-land-certificates-in-central-java

[19] M. A. I. Pakereng and A. D. Wowor, "Square transposition: an approach to the transposition process in block cipher," *Bulletin of Electrical Engineering and Informatics*, vol. 10, No. 6, pp. 3385-3392, December. 2021, doi: https://doi.org/10.11591/eei.v10i6.3129.

[20] T. Manojkumar, P. Karthigaikumar, and V. Ramachandran, "An optimized s-box circuit for high speed AES design with enhanced PPRM architecture to secure mammographic images," *Journal of Medical Systems*, vol. 43, no. 31, January. 2019. doi: https://doi.org/10.1007/s10916-018-1145-9.

[21] C. A. Sari, G. Ardiansyah, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman Coding on Image Steganography," *TELKOMNIKA*, vol. 17, no.5, pp. 2400-2409, October 2019. doi: http://doi.org/10.12928/telkomnika.v17i5.9570.

[22] A. A. Thinn and M. M. S. Thwin,"Modification of AES algorithm by using second key and modified subbytes operation for text encryption," *Computational Science and Technology part of Lecture Notes in Electrical Engineering*, vol. 481, pp. 435-444, August. 2018, doi: https://doi.org/10.1007/978-981-13-2622-6_42.

[23] M. Yang, B. Xiao, and Q. Meng, "New AES Dual Ciphers Based on Rotation of Columns," *Wuhan University Journal of Natural Sciences*, vol. 24, pp. 93-97, March. 2019, doi: https://doi.org/10.1007/s11859-019-1373-y.

[24] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES Algorithm," *The Journal of Supercomputing* , vol. 75, pp. 6663-6682, May. 2019, doi: https://doi.org/10.1007/s11227-019-02878-7.

[25] C. R. Dongarsane, D. Maheshkumar, and S. V. Sankpal, "Performance Analysis of AES Implementation on a Wireless Sensor Network," in *Techno-Societal 2018* , pp. 87-93, November. 2019, doi: https://doi.org/10.1007/978-3-030-16848-3_9

[26] C Ashokkumar, B. Roy, M. B. S. Venkatesh, and B. L. Menezes, "S-box implementation of AES is not side channel resistant," *Journal of Hardware and Systems Security*, vol. 4, issue 2, pp.86-97 December 2019, doi: https://doi.org/10.1007/s41635-019-00082-w.

[27] S. D. Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan, and A. D. Ahmad, "Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3," *TELKOMNIKA*, vol. 17, no.3, pp. 2182-1289, June. 2019, doi: http://doi.org/10.12928/telkomnika.v17i3.9384.

[28] G. C. Prasetyadi, R. Refianti, and A. B. Mutiara, "File encryption and hiding application based on AES and append insertion steganography," *TELKOMNIKA*, vol. 16, no.1, pp. 361-367, February. 2018, doi : http://doi.org/10.12928/telkomnika.v16i1.6409.

[29] C. A. Sari, E. H. Rachmawanto, and C. A. Haryanto, "Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 105-117, November. 2018, doi: https://doi.org/10.15294/sji.v5i2.14844.

[30] J. L. Calpito, P. L. Olanday, and A. C. Gallarde, "Application of advanced encryption standard in the computer or handheld online year-round registration system," *ndonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 2, pp. 922-935, August. 2022, doi: 10.11591/ijeecs.v27.i2.pp922-935.

[31] S. Pavithra, P. Muthukannan, and V. Prabhakaran, "An enhanced cryptographic algorithm using bimodal biometrics," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, issue 11, pp. 2575-2582, September. 2019, doi : 10.35940/ijitee.K1870.0981119.

[32] S.D. Putra, A. S. Ahmad, S. Sutikno, Y. Kurniawan, A. Datumaya and W. Sumari, "Revealing AES encryption device key on 328P microcontrollers with differential power analysis", *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 2, pp. 181-187, December. 2017, doi : http://doi.org/10.11591/ijece.v8i6.pp5144-5152.

[33] E. R. Arboleda, J. L. Balaba, and J. C. L. Espineli, "Chaotic Rivest-Shamir-Adlelman algorithm with Data Encryption Standard scheduling," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 3, pp. 219-227, September. 2017, doi: https://doi.org/10.11591/eei.v6i3.627.

[34] J. M. B. Espalmado, and E. R. Arboleda, "DARE algorithm: a new security protocol by integration of different cryptographic techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 2, pp. 1032–1041, April. 2017, doi: http://doi.org/10.11591/ijece.v7i2.pp1032-1041.

[35] R. Srividya and B. Ramesh, "Implementation of AES using Biometric," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4266-4276, October. 2019, doi: http://doi.org/10.11591/ijece.v9i5.pp4266-4276.

[36] M. Yang, B. Xiao, and Q. Meng, "New AES dual ciphers based on rotation of columns," *Wuhan University Journal of Natural Sciences*, vol. 24, pp. 93-97, March. 2019, doi: https://doi.org/10.1007/s11859-019-1373-y.

[37] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES Algorithm," *The Journal of Supercomputing* , vol. 75, pp. 6663-6682, Mey. 2019, doi: https://doi.org/10.1007/s11227-019-02878-7.

[38] A. A. Thinn and M. M. S. Thwin, "Modification of AES algorithm by using second key and modified subbytes operation for text encryption," *Computational Science and Technology part of Lecture Notes in Electrical Engineering*, vol. 481, pp. 435-444, August. 2019, doi: https://doi.org/10.1007/978-981-13-2622-6_42.

[39] C. R. Dongarsane, D. Maheshkumar, and S. V Sankpal, "Performance analysis of AES implementation on a wireless sensor network," *Techno-Societal* , pp. 87-93, November. 2019, doi: https://doi.org/10.1007/978-3-030-16848-3_9.

[40] C. Ashokkumar, R. M. Bholanath, S. V. Bhargav, and B. L. Menezes, "S-Box implementation of AES Is not side channel resistant," *Journal of Hardware and Systems Security*, vol. 4, pp. 86-97, December. 2019, doi: 10.1007/s41635-019-00082-w

[41] M. Aledhari, A. Marhoon, A.Hamad, and F. Saeed, "A New cryptography algorithm to protect cloud-based healthcare services," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Pages 37-43, August. 2017, doi: 10.1109/CHASE.2017.57.

[42] A. Biryukov and D. Khovratovich, "Related-Key Cryptanalysis of the Full AES-192 and AES-256," *Advances in Cryptology - ASIACRYPT*, vol. 5912, pp 1-18, 2009, doi: https://doi.org/10.1007/978-3-642-10366-7_1.

[43] J. Kim, S. Hong, and B. Preneel, "Related-key rectangle attacks on reduced AES-192 and AES-256," in *Fast Software Encryption 2007*, vol. 4593 of *LNCS*, pp 225–241, 2007, doi: https://doi.org/10.1007/978-3-540-74619-5_15.

[44] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," *IACR Transactions on Symmetric Cryptology*, vol. 2019, issue 2, pp 55-93, 2019, doi: https://doi.org/10.13154/tosc.v2019.i2.55-93.

[45] D. Gerault, P. Lafourcade, M. Minier, and C. Solnon, "Revisiting AES related-key differential attacks with constraint programming," *Cryptology*, vol. 139, pp. 24-29, November. 2018, doi: 0.1016/j.ipl.2018.07.001.

[46] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation", in *Proceedings The Royal Society London A, Mahtematical Physical and Engineering Sciences*, vol 439, Page: 553–558, December. 1992, doi: https://doi.org/10.1098/rspa.1992.0167.

[47] S. Lucks, "Ciphers secure against related-key attacks," in *Fast Software Encryption*, vol. 3017, pp. 359–370, 2004, doi: https://doi.org/10.1007/978-3-540-25937-4_23.

[48] M. Abe, R. Gennaro, and K. Kurosawa, "Tag-KEM/DEM: A new framework for hybrid encryption," *Journal of Cryptology*, Vol. 21, pp. 97-130, November. 2008, doi: 10.1007/s00145-007-9010-x.

[49] M. Abe, R. Gennaro, K. Kurosawa, and V. Shoup, "Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM," *Advances in Cryptology - EUROCRYPT 2005*, Vol. 3494, pp. 128-146, 2005, doi: https://doi.org/10.1007/11426639_8.

[50] Q. Zhang, "An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption," in *Proceedings of IEEE International Conference on Computing and Data Science (CDS)*, pp. 616-622, 2021, doi: 10.1109/CDS52072.2021.00111.

[51] S. M. Daisy, R. S. Shaiji, and J. P. Jayan, "Asymetric key based data communication under mobile cloud system," *Proceedings of IEEE Global Conference on Communication Technologies*, December. 2015, doi: 10.1109/GCCT.2015.7342724.

[52] C. Liang, N. Ye, R. Malekian, and R. Wang, "The hybrid encryption algorithm of lightweight data in cloud storage," *2nd International Symposium on Agent, Multi-Agent System and Robotics*, pp. 160-166, January. 2017, doi: 10.1109/ISAMSR.2016.7810021.

[53] Timoty, D.P., & Santr, A.K., "A hybrid cryptography algorithm for cloud computing security," in *International conference on Microelectronic Devices, Circuits and System*, pp. 1-5. December. 2017, doi: 10.1109/ICMDCS.2017.8211728.

[54] M. S. Asang, D. Manongga, and I. Sembiring, "Data security on internet of things device using hybrid encryption models," *International Journal of Computer Science and Information Security*, vol. 16, no. 8, pp 93-103, August. 2018.

[55] R. K. Salih and M. S. Yousif, "Hybrid encryption using playfair and RSA cryptosystems," *International Journal Nonlinear Anal. Appl.*, vol. 12, no. 2, pp 2345-2350, July. 2021, doi: 10.22075/ijnaa.2021.5379

[56] Y. Chen, H. Liu, B. Wang, B. Sonompil, Y. Ping, and Z. Zhang, "A threshold hybrid encryption method for integrity audit without trusted center," *Journal of Cloud Computing*, vol. 10, no. 3, January. 2021, doi: https://doi.org/10.1186/s13677-020-00222-6.

[57] P. Chinnasamy, S. Padmavathi, and R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," *Inventive Communication and Computational Technologies*, pp 537-547, September. 2020, doi: https://doi.org/10.1007/978-981-15-7345-3_46.

[58] P. Gayathri, S. Umar, G. Sridevi, N. Bashwanth, and R. Srikanth, "Hybrid cryptography for random-key generation based on ECC algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 3, pp 1293-1298, June. 2017, doi: http://doi.org/10.11591/ijece.v7i3.pp1293-1298.

[59] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp 6461-6471, December. 2020, doi: http://doi.org/10.11591/ijece.v10i6.pp6461-6471.

[60] S. Sankaran P. and Kirubanand V.B., "Hybrid Cryptography security in public cloud using TwoFish and ECC algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 4, pp 2578-2584, August. 2019. doi: http://doi.org/10.11591/ijece.v9i4.pp2578-2584.

[61] C. Puttaswamy and N. P. K. Shivaprasad, "Enhancing wireless sensor network security with optimized cluster head selection and hybrid public-key encryption," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp 2976-2987, June. 2024. doi: http://doi.org/10.11591/ijece.v14i3.pp2976-2987.

[62] M. M. Hoobi, "Efficient Hybrid Cryptography Algorithm," *Journal of Southwest Jiaotong University*, vol. 55, no. 3, May. 2020, doi: https://doi.org/10.35741/issn.0258-2724.55.3.5.

[63] T. Mantoro and A. Zakariya, "Securing e-mail communication using hybrid cryptosystem on android-based mobile devices," *TELKOMNIKA: Indonesian Journal of Electrical Engineering*, vol. 10, no. 4, pp. 807-814, December. 2012. doi: http://doi.org/10.12928/telkomnika.v10i4.870

[64] S. J. Suhael, Z. A. Ahmed, and A. J. Hussain, "Proposed hybrid cryptosystems based on modifications of playfair cipher and RSA cryptosystem," *Baghdad Science Journal*, vol. 21, no. 1, pp. 151-160, January. 2024, doi: https://doi.org/10.21123/bsj.2023.8361.

[65] Hameed, M.E., Ibrahim, M.M., Manap, N.A., & Mohammed, A.A, "An enhanced lossless compression with cryptography hybrid mechanism for ECG biomedical signal monitoring," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3235-3243, June. 2020. doi: http://doi.org/10.11591/ijece.v10i3.pp3235-3243.

[66] S. Ghaly and M. Z. Abdullah, "Design and implementation of a secured SDN system based on hybrid encrypted algorithms," *TELKOMNIKA: Indonesian Journal of Electrical Engineering*, vol. 19, no. 4, pp. 1118-1125, August. 2021, doi: http://doi.org/10.12928/telkomnika.v19i4.18721.

[67] E. R. Arboleda, J. L. Balaba, and J. C. L. Espineli, "Chaotic Rivest-Shamir-Adleman algorithm with Data Encryption Standard scheduling," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 6, no. 3, pp. 219-227, September. 2017, doi: 10.11591/eei.v6i3.627.

[68] H. S. Christnatalis and A. M. Husein, "Digital signs security system using AES-Blowfish-RSA hybrid cryptography approach," *Sinkron*, vol. 4, no. 1, pp. 185-190, October. 2019, doi: 10.33395/sinkron.v4i1.10244.

[69] Y. Liu, W. Gong and W. Fan "Application of AES and RSA hybrid algorithm in e-mail," in *IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, pp. 701-703, June. 2018, doi: 10.1109/ICIS.2018.8466380.

[70] M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, "Novel hybrid encryption algorithm based on AES, RSA, and Twofish for bluetooth encryption," *Journal of Information Security*, vol. 9, no. 2, pp. 168-176, April. 2018. doi: 10.4236/jis.2018.92012.

[71] D. Sarumaha, M. A. Budiman, and M. Zarlis, "Performance analysis of hybrid cryptographic algorithms Rabbit Stream and enhanced dual RSA," *Journal of Computing and Applied Informatics (JoCAI)*, vol. 7, issue 1, pp. 35-43, January.2023. doi: https://doi.org/10.32734/jocai.v7.i1-10483.

[72] Boesgaard, M. V., & Scavenius, O., "Rabbit: A new high-performance stream chiper," in *International Workshop on Fast Software Encryption*, vol. 2887, pp 307-329, 2003, doi: https://doi.org/10.1007/978-3-540-39887-5_23.

[73] Boesgaard, M., Pedersen, T., Vesterager, M., & Zenner, E., "The Rabbit Stream Cipher - Design and Security Analysis," *SASC 2004: State of the Art in Stream Ciphers*, no. 1, pp. 7-29, October. 2004.

[74] M. Boesgaard, M. Vesterager, and E. Zenner, "The Rabbit Stream Cipher" *In: Robshaw, M., Billet, O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science*, vol. 4986, pp. 69-83, 2008. doi: https://doi.org/10.1007/978-3-540-68351-3_7.