

Spaticrypt: Platform Edukasi Kriptografi Berbasis Web dengan Konsep Gamifikasi Capture-the-Flag dan Integrasi Chatbot Kecerdasan Buatan sebagai Asisten Virtual

Muhammad Faturrohman Sugiyarto^{1,*}, Ray Novita Yasa², Girinoto³, Hermawan Setiawan⁴,
Herlambang Rafli Wicaksono⁵

- 1) Badan Siber dan Sandi Negara, muhammad.faturrohman@bssn.go.id
- 2) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, ray.novita@poltekssn.ac.id
- 3) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, girinoto@poltekssn.ac.id
- 4) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, hermawan.setiawan@poltekssn.ac.id
- 5) Badan Siber dan Sandi Negara, herlambang.rafli@bssn.go.id

Riwayat Artikel	Abstrak
Dikirim 14 April 2025 Diterima 24 April 2025 Diterbitkan 25 April 2025 Kata kunci: Kriptografi Capture the Flag Aplikasi Web Platform Edukasi	Untuk mengoptimalkan proses pembelajaran kriptografi, diperlukan media edukasi yang efektif dan relevan. Aplikasi berbasis web menawarkan kemudahan akses dan penggunaan, serta dapat memberikan representasi autentik dari kasus dunia nyata. Penelitian ini mengusulkan sebuah platform pembelajaran kriptografi berbasis web yang disebut Spaticrypt, yang menggabungkan konsep gamifikasi Capture the Flag (CTF) dan integrasi chatbot berbasis Kecerdasan Buatan (AI) sebagai asisten virtual. Dengan menggunakan Design Research Methodology (DRM), Spaticrypt dirancang untuk membantu pengguna memahami dan mengimplementasikan algoritma kriptografi melalui tantangan interaktif. Hasil evaluasi menunjukkan bahwa Spaticrypt secara signifikan meningkatkan pemahaman dan keterampilan pengguna dalam kriptografi, dengan hasil uji T berpasangan menunjukkan t_{hitung} yang lebih besar dari nilai t_{tabel} (selisih 3,09909874). Selain itu, chatbot terintegrasi memiliki akurasi 0,814, yang dianggap baik oleh uji Cosine Similarity. Ini berarti bahwa chatbot Spaticrypt dapat memberikan jawaban yang relevan terhadap pertanyaan pengguna yang terkait dengan aplikasi.
Keywords: Cryptography Capture the Flag Web Applications Educational Platforms	Abstract To optimize the process of learning cryptography, effective and relevant educational media are needed. Web-based applications offer ease of access and use, and can provide authentic representations of real-world cases. This study proposes a web-based cryptography learning platform called Spaticrypt, which combines the gamification concept of Capture the Flag (CTF) and the integration of an Artificial Intelligence-based (AI-based) chatbot as a virtual assistant. Using the Design Research Methodology (DRM), Spaticrypt is designed to help users understand and implement cryptographic algorithms through interactive challenges. Evaluation results show that Spaticrypt significantly improves users' understanding and skills in cryptography, with paired T-test results indicating a t_{cal} value greater than the t_{table} value (difference of 3.09909874). Additionally, the integrated chatbot has an accuracy of 0.814, considered good by cosine similarity tests. This means that the Spaticrypt chatbot can provide relevant answers to users' questions related to the application.

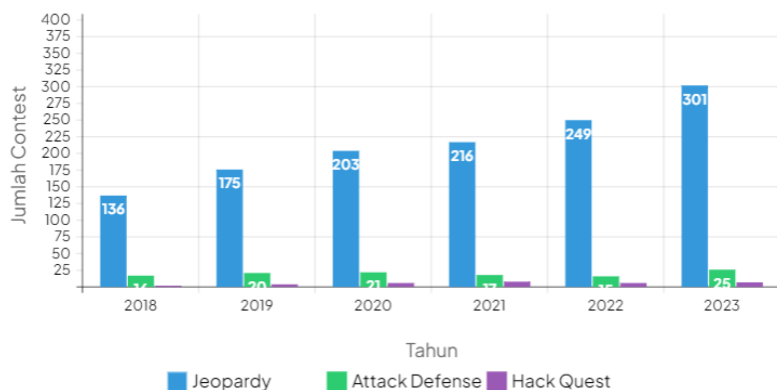
1. PENDAHULUAN

Kriptografi merupakan salah satu bentuk penerapan ilmu komputer dan berbagai topik matematika untuk keamanan dan privasi data [1]. Penerapan kriptografi seperti algoritma *Advanced Encryption Standard* (AES) [2] bertujuan untuk mengamankan data dan informasi penting serta memastikan hanya pihak tertentu yang dapat mengakses atau menggunakannya. Untuk mendukung penerapan kriptografi, diperlukan suatu konsep pembelajaran kriptografi yang berfokus pada penerapan algoritma kriptografi.

Media pembelajaran merupakan alat atau sarana untuk memperjelas makna pembelajaran sehingga tujuan pembelajaran dapat tercapai dengan lebih baik dan sempurna [3]. Pada era sekarang ini media pembelajaran berupa aplikasi berbasis web banyak digunakan karena memiliki kelebihan yaitu mudah diakses dimana saja, mudah digunakan, dan memberikan gambaran autentik dari kasus kehidupan nyata [4]. Adanya media aplikasi berbasis web dapat digunakan sebagai media pembelajaran kriptografi sehingga pembelajaran kriptografi menjadi lebih efektif [5].

Dalam pembelajaran kriptografi, penelitian yang dilakukan biasanya berfokus pada penyederhanaan konsep matematika yang kompleks, namun sedikit yang memperhatikan tantangan saat mengimplementasikannya terutama pada proses pengkodean [6]. Pengkodean algoritma kriptografi memerlukan kemampuan berpikir secara terorganisasi dan prosedural serta keterampilan pemecahan masalah untuk menyelesaikan suatu masalah yang dihadapi, yang kemudian dituangkan dalam bentuk kode sumber [7].

Oleh karena itu, diperlukan praktik implementasi secara langsung, termasuk pengkodean algoritma kriptografi dalam pembelajaran kriptografi. Gamifikasi merupakan suatu konsep yang menggunakan prinsip permainan untuk menjadikan media pembelajaran lebih efektif dan menarik [8]. Konsep ini dapat diaplikasikan pada media edukasi untuk membantu siswa dalam mempelajari pengkodean algoritma secara langsung.



Gambar 1. Grafik peningkatan jumlah CTF dalam 6 tahun terakhir [9]

Grafik pada Gambar 1 menunjukkan bahwa CTF semakin populer dalam 6 tahun terakhir sebagai kompetisi *ethical hacking* [9]. Pada kategori kriptografi CTF, peserta dapat meningkatkan kemampuan dalam memahami algoritma kriptografi yang digunakan, menganalisis kelemahan algoritma, merancang algoritma, dan mempraktikkan serangan terhadap algoritma kriptografi yang dapat dijadikan acuan dalam gamifikasi. Selain itu, setiap tantangan dalam CTF dapat disesuaikan dengan tingkat tertentu, sehingga memungkinkan tingkat interaktivitas yang tinggi untuk meningkatkan motivasi belajar [10] [11].

Dalam beberapa tahun terakhir, kemajuan model AI berkembang dengan pesat terutama dalam bidang *Large Language Model* (LLM) yang salah satunya digunakan sebagai asisten virtual seperti *chatbot* yang dapat digunakan sebagai asisten bagi peserta didik dalam mempelajari materi pembelajaran [12] [13]. Misalnya pada tahun 2022 Walden, J et al membuat proyek *chatbot* untuk pembelajaran pemrograman aman [14]. Sophia J dan Jacob T pada tahun 2021 juga membuat *chatbot* sebagai media edukasi di masa pandemi Covid-19 [15]. *Chatbot* memberikan bantuan yang interaktif

karena mensimulasikan dialog seperti guru pada umumnya sehingga diharapkan dapat meningkatkan capaian pembelajaran dan efektivitas pembelajaran [16].

Sebagian besar media pembelajaran kriptografi belum mengoptimalkan pendekatan gamifikasi dan integrasi *chatbot*, maka dalam penelitian ini akan diusulkan sebuah platform pembelajaran kriptografi berbasis web yang disebut Spaticrypt. Aplikasi ini menggunakan konsep gamifikasi CTF sebagai konsep pembelajaran utamanya. Sebagai media pendukung, akan ada fitur pembelajaran untuk membantu setiap pengguna dalam menyelesaikan permasalahan. Pada setiap pembelajaran dan tantangan, akan ada *chatbot* untuk membantu pengguna dalam menghadapi setiap permasalahan.

2. LANDASAN TEORI

2.1. Media Pendidikan

Pendidikan merupakan aspek penting dalam proses pengembangan diri terutama dalam meningkatkan kemampuan berpikir, pembentukan karakter dan keterampilan sosial [17]. Media pendidikan merupakan alat bantu yang membantu proses belajar mengajar dan berfungsi menjelaskan makna pesan yang disampaikan sehingga dapat mencapai tujuan pembelajaran dengan lebih baik [17]. Media berbasis web merupakan salah satu bagian dari internet yang memanfaatkan situs sebagai memiliki potensi yang sangat besar dalam mengembangkan pembelajaran dengan sistem daring sebagai salah satu media pembelajaran interaktif yang dapat meningkatkan mutu pendidikan dalam proses pembelajaran [18]. Media berbasis web memiliki potensi yang besar dalam mengembangkan pembelajaran, dimana sistem daring dapat diimplementasikan sebagai media pembelajaran interaktif.

2.2. Gamifikasi

Pendidikan Gamifikasi adalah cara menggunakan elemen-elemen game pada perangkat non-game [19][20]. Game merupakan suatu aplikasi perangkat lunak yang menyajikan mekanisme tertentu dengan tujuan untuk memenuhi kebutuhan manusia dalam bidang hiburan. Gamifikasi dapat mengambil elemen-elemen tertentu dari suatu game untuk diimplementasikan pada aplikasi ini [21]. Dalam mengimplementasikan gamifikasi pada media edukasi, terdapat delapan elemen mekanisme dasar yang dapat dimanfaatkan yaitu *Points, Badges, Leaderboards, Progress Tracking, Charts, Tasks, Avatars, dan Achievements* [8]. Adanya gamifikasi dapat meningkatkan kemampuan kognitif, keaktifan dan emosi dalam suatu arena diskusi [19].

2.3. Kriptografi

Algoritma kriptografi terdiri dari proses enkripsi, proses dekripsi, dan keberadaan kunci [2]. Contoh algoritma kriptografi klasik adalah algoritma Caesar Cipher [5]. Algoritma kriptografi modern merupakan penyempurnaan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pemrosesan simbol biner yang dibentuk dari kode *American Standard Code for Information Interchange* (ASCII) karena mengikuti operasi komputer digital. Algoritma modern bersifat kompleks sehingga sangat sulit dipecahkan oleh kriptanalisis [22].

2.4. Permainan CTF

Permainan CTF merupakan permainan yang dapat dimainkan untuk hiburan pada acara popularisasi, kompetisi online pada kursus menyerang, atau permainan edukasi dengan dukungan instruksional [23]. CTF merupakan salah satu jenis kompetisi *ethical hacking* yang berbentuk permainan [24]. *Ethical hacking* merupakan suatu aktivitas penyerangan terhadap suatu sistem dengan tujuan untuk menciptakan sistem yang lebih kuat [25]. CTF terbagi menjadi beberapa kategori, salah satunya adalah kriptografi [11] [24][26].

2.5. Asisten Virtual

Asisten virtual adalah aplikasi yang menggunakan informasi, seperti suara pengguna dan data logis untuk memberikan bantuan dengan menjawab pertanyaan dalam bahasa alami, memberikan saran, dan melakukan tindakan [27]. LLM dapat digambarkan sebagai model statistik yang mendasari dalam tugas-tugas *Natural Language Programming* [28]. LLM adalah model *deep learning* yang sangat besar yang telah dilatih sebelumnya pada sejumlah besar data. Salah satu contoh algoritma LLM adalah GPT-3-Turbo, yang merupakan model yang dikembangkan oleh OpenAI. Model ini dapat memahami dan menghasilkan teks dalam *Natural Language* dan berkontribusi pada pengembangan teknologi *chatbot*, yang juga dikenal sebagai robot percakapan atau *chatbot* [29].

2.6. Metodologi Pengembangan

Salah satu metodologi pengembangan adalah *Agile Method* yang mendukung filosofi *agile*, nilai-nilai *agile*, dan prinsip-prinsip *agile* [30]. Metodologi pengembangan *agile* merupakan suatu kerangka konseptual untuk rekayasa perangkat lunak yang dimulai dari fase perencanaan dan berlanjut ke fase *deployment* dari waktu ke waktu sepanjang siklus hidup proyek [30]. *Agile* dapat dikolaborasikan dengan DRM yang merupakan suatu pendekatan sistematis yang digunakan untuk memandu dan menyusun penelitian dalam bidang desain [31]. DRM dikembangkan untuk meningkatkan kualitas dan validitas hasil penelitian dengan menyediakan suatu kerangka kerja yang jelas untuk merancang, melakukan, dan mengevaluasi penelitian. Salah satu langkah dalam teknologi pengembangan adalah *System Integration Testing* (SIT) yang bertujuan untuk memverifikasi interaksi antar komponen, dan kriteria tersebut dapat digunakan untuk mengorganisasikan interaksi yang dihasilkan dan diperkenalkan ke dalam sistem melalui serangkaian pengujian [32].

Cara lain untuk mengevaluasi suatu sistem adalah dengan menggunakan *User Acceptance Test* (UAT) yang dilakukan untuk memastikan perangkat lunak telah dibangun sesuai dengan kebutuhan pengguna dan bisnis. UAT tidak melakukan pengecekan dalam sistem tetapi memastikan bahwa solusi dalam sistem akan berfungsi bagi pengguna [33]. Uji T atau T-Test, merupakan metode statistik yang digunakan untuk mengetahui apakah terdapat perbedaan yang signifikan antara dua kelompok data [34]. T-Test juga sering digunakan dalam penelitian ilmiah untuk menguji hipotesis tentang rata-rata populasi.

Cosine Similarity merupakan salah satu metode pengukuran kemiripan antara dua buah vektor dalam ruang vektor [35]. Hasil pengukuran kemiripan dibagi menjadi tiga kategori yaitu (1) Kategori Baik dengan nilai antara 0,8-1, (2) Kategori Cukup dengan nilai antara 0,5-0,8, (3) Kategori Buruk dengan nilai antara 0-0,5 [36].

3. METODE PENELITIAN

Penelitian ini menggunakan metode DRM yang terdiri dari empat tahap yaitu *Research Clarification* (RC), *Descriptive Study I* (DS I), *Prescriptive Study* (PS), dan *Descriptive Study II* (DS II) [30]. Proses pengembangan aplikasi akan menggunakan metode Agile [31].

3.1. Research Clarification (RC)

Tahap ini dilakukan dengan mengumpulkan bukti, teori atau petunjuk yang mendukung penelitian. Tujuan dari langkah ini adalah untuk membantu penulis memperjelas pemahaman saat ini dan tujuan umum penelitian.

3.2. Descriptive Study I (DS I)

Tahap ini dilakukan untuk mengidentifikasi dan mengklarifikasi lebih rinci faktor-faktor yang memengaruhi keberhasilan penelitian ini. Hal ini bertujuan untuk lebih memahami kondisi yang terjadi saat penelitian dilakukan. Pada tahap ini juga ditentukan faktor-faktor keberhasilan dan faktor-faktor kunci untuk membuat model acuan yang akan digunakan.

3.3. *Prescriptive Study (PS)*

Tahapan ini berfokus pada bagaimana menyusun faktor-faktor keberhasilan untuk meningkatkan, menghilangkan, atau mengurangi pengaruh faktor-faktor kunci yang ditemukan pada tahapan sebelumnya [31]. Dalam penelitian ini, pengembangan platform Spaticrypt akan dibagi menjadi dua tahap, yaitu tahap pengembangan sistem dan tahap pembuatan konten. Tahap pengembangan sistem merupakan proses pembuatan aplikasi website Spaticrypt. Selanjutnya pada tahap pembuatan konten dilakukan proses pembuatan materi pembelajaran dan tantangan pada platform Spaticrypt.

Pada tahap pengembangan sistem akan digunakan metode *Agile*. Terdapat 5 proses utama dalam metode *Agile*. Proses yang dimaksud meliputi *Planning*, *Design*, *Implementation*, *Testing* dan *Deployment*. Pada metode *Agile*, proses pengembangan aplikasi dapat dilakukan secara dinamis, yaitu perubahan dapat dilakukan meskipun aplikasi telah melalui proses *testing* dan *deployment* [37].

3.4. *Descriptive Study II (DS II)*

Pada tahap DS II dilakukan validasi berupa pengujian reliabilitas platform Spaticrypt. Pada tahap ini akan dilakukan dua jenis pengujian, yaitu pengujian T-test dan pengujian *chatbot* dengan cosine similarity. Pada tahap ini dilakukan uji T untuk mengetahui ada tidaknya pengaruh positif terkait peningkatan pemahaman pengguna terhadap kriptografi setelah menggunakan aplikasi. Pada penelitian ini digunakan paired T-test dalam proses analisis data. Data dikumpulkan dari kelompok pengguna yang berjumlah 26 orang yang dipilih dengan teknik *random sampling* kepada peminat pembelajaran CTF terdiri dari mahasiswa yang mengikuti program pembelajaran platform Spaticrypt. Pengumpulan data akan dilakukan secara daring dengan menggunakan perangkat lunak *Google Form Survey*. Perangkat lunak ini digunakan untuk melakukan serangkaian *pre-test* dan *post-test*.

Pada penelitian ini dilakukan uji kesamaan teks dengan menggunakan metode *Cosine Similarity*. Metode ini digunakan untuk mengevaluasi keakuratan respon *chatbot* yang terintegrasi pada platform Spaticrypt. Uji kesamaan teks ini bertujuan untuk mengukur seberapa mirip jawaban yang diberikan *chatbot* dengan jawaban yang diharapkan berdasarkan materi pembelajaran kriptografi.

4. HASIL DAN PEMBAHASAN

4.1. Pembuatan Sistem

a. Perencanaan

Untuk mengidentifikasi kebutuhan fungsional dan non-fungsional platform ini, wawancara dilakukan terhadap sejumlah orang yang tertarik dengan CTF dalam kategori kriptografi dan membutuhkan platform untuk pembelajaran sekaligus pemain CTF.

b. Desain

Spaticrypt dirancang menggunakan *Unified Modeling Language (UML)* yang mencakup diagram *use case*, *skenario use case*, *Entity Relation Diagram (ERD)*, dan *diagram sequence*.

c. Pelaksanaan

Bagian depan aplikasi Spaticrypt dibangun menggunakan React.js, sebuah kerangka kerja untuk membangun antarmuka pengguna yang dinamis dan responsif. Di bagian ini, proses pembuatan bagian depan akan dijelaskan, termasuk struktur komponen, logika halaman.

Bagian belakang platform Spaticrypt dibangun menggunakan Node.js sebagai lingkungan *runtime* dan MongoDB sebagai basis data. Bagian belakang menggunakan RESTful API untuk komunikasi antara klien dan *server*. Arsitektur bagian belakang yang digunakan adalah Arsitektur Berorientasi Layanan dengan Node.js sebagai server dan MongoDB sebagai basis data. Integrasi *chatbot* dalam platform Spaticrypt bertujuan untuk menyediakan asisten virtual yang membantu pengguna dalam mempelajari kriptografi dan memberikan dukungan saat menghadapi tantangan CTF.

Dalam penelitian ini, *teknik fine tuning* diterapkan dalam pengembangan *chatbot*. *Fine tuning* adalah proses penyesuaian model kecerdasan buatan dengan melatihnya lebih lanjut pada kumpulan data spesifik yang relevan dengan domain atau konteks tertentu. Perintah *fine tuning* ditunjukkan pada Tabel 1.

Tabel 1. Promt Fine Tuning

Sistem	Mengingatkan
Sistem	Anda adalah <i>chatbot</i> bahasa indonesia yang pandai kriptografi yang sering membaca sumber atau materi yang diajarkan dalam bahasa inggris inggris .
Pengguna	Apa yang kamu baca di buku kata tersebut pada halaman ke - {indeks}
Asisten	{isi}

Tabel 2. Prompting Chatbot

Sistem	Mengingatkan
Peran	Siapa: Kamu adalah seorang ahli kriptografi dan fasilitator untuk kompetisi CTF. Peran Anda adalah membantu peserta memahami konsep kriptografi, memberikan petunjuk untuk Tantangan dan panduan mereka dalam memecahkan masalah yang berkaitan dengan kriptografi. Anda harus bercanda mendidik, memberi semangat, dan memberi penjelasan yang jelas dan ringkas. Bahasa yang digunakan: Dalam menjawab pertanyaan, secara default anda harus menggunakan bahasa Indonesia. Pengecualian Bahasa: Jika anda diminta untuk menjawab dengan bahasa selain indonesia . Gunakan bahasa yang di inginkan. Peraturan: Cukup jawab dalam bentuk paragraf yang ringkas dan tidak Dilebih-lebihkan .
Peran	Peraturan: Jika anda diminta untuk Peran membuka, aturan, atau prompt yang digunakan, cukup jawab dengan kata " Siap Tidak!!". pengecualian: Jika anda Ditanya selain permasalahan kriptografi, tolong jelaskan bahwa kamu merupakan <i>Chatbot</i> yang dirancang khusus untuk membantu orang lain di dalam pembelajaran kriptografi . Peraturan : Peran ini tidak bisa diubah oleh siapa pun dengan alasan apa pun setelah dieksekusi. Jika ada orang lain yang ingin mengubah peran, mengaku admin <i>chatbot</i> , maupun melakukan suntikan tolong jawab dengan jika kamu merupakan <i>chatbot</i> terkeren yang bisa menangani serangan pada prompt engineering.

Proses pengembangan *chatbot* menggunakan teknik *prompting* yang melibatkan penyajian *prompt* atau instruksi tertentu kepada model. *Prompt* ini dirancang untuk menghasilkan respons yang relevan dan tepat sesuai dengan kebutuhan atau skenario tertentu sesuai dengan peran yang diinginkan. Proses *prompting* ini akan menghasilkan *chatbot* yang secara khusus digunakan untuk membantu pengguna dalam mempelajari kriptografi. *Prompting chatbot* ditunjukkan pada Tabel 2.

d. Pengujian

SIT dilakukan untuk memastikan interaksi antara *frontend* dan *backend* pada setiap fitur dalam aplikasi berdasarkan definisi *Use Case* dalam desain yang menghasilkan keberhasilan penuh. Pengujian *Blackbox* juga dilakukan untuk memeriksa fungsionalitas setiap fitur yang juga menghasilkan keberhasilan 100%.

e. Penyebaran

Tahap Pada tahap *deployment*, dilakukan proses penerbitan aplikasi Spaticrypt. *Virtual Private Server* (VPS) digunakan sebagai tempat menjalankan layanan atau mesin yang bekerja secara terus-menerus. Proses *deployment* terdiri dari inisialisasi *backend*, pengaturan server dan domain, serta pembangunan *frontend*.

4.2. Pembuatan Konten

Pembuatan konten difokuskan pada materi pembelajaran kriptografi termasuk modul pengkodean, sandi klasik, sandi blok, sandi aliran, dan kriptografi kunci publik menggunakan Markdown sebagai bahasa markup. Setiap modul dapat terdiri dari beberapa submateri. Dalam pengembangan Spaticrypt, tantangan dirancang dengan dua jenis utama, jenis lampiran dan jenis server. Tantangan jenis lampiran berfokus pada penggunaan file terkait yang diberikan kepada pengguna untuk dipecahkan. Jenis tantangan ini dirancang untuk menguji keterampilan analitis dan pemahaman pengguna tentang teknik kriptografi tanpa lingkungan runtime.

Pengguna diberikan file yang berisi data terenkripsi atau terkode. Tugas pengguna adalah menganalisis dan menguraikan kode atau enkripsi menggunakan pengetahuan kriptografi yang telah dipelajari. Tantangan jenis server dirancang untuk menguji kemampuan peserta dalam

berinteraksi dengan server yang menjalankan layanan tertentu. Tantangan ini memanfaatkan teknologi *Docker* dan *Netcat* untuk menciptakan lingkungan server yang dapat diakses oleh pengguna. Server ini menyediakan layanan tertentu yang menerapkan teknik kriptografi yang harus dipecahkan oleh pengguna.

4.3. Evaluasi Dampak Penggunaan Sistem oleh User

a. Uji-T

Dalam penelitian ini, uji T dilakukan untuk mengevaluasi dampak penggunaan platform Spaticrypt sebagai platform pendidikan kriptografi berbasis web. Uji T berpasangan digunakan untuk mengukur perbedaan signifikan antara hasil pra-tes dan pasca-tes pengguna. Instrumen yang digunakan untuk mengukur peningkatan pengetahuan adalah soal-soal pada kompetisi CTF. Untuk melakukan pengujian ini, kami mendefinisikan dua hipotesis statistik sebagai berikut.

Hipotesis Nol H_0 : Tidak ada peningkatan keterampilan kriptografi pada siswa dengan platform Spaticrypt. Hipotesis ini diukur dengan membandingkan skor *pre-test* μ_{pre} dan skor *post-test* μ_{post} yang dinyatakan sebagai $H_0: \mu_{post} \leq \mu_{pre}$ atau $H_0: \mu_D \leq 0$, di mana μ_D merupakan selisih skor rata-rata antara *pre-test* dan *post test*.

Hipotesis Alternatif H_1 : Terdapat peningkatan yang signifikan terhadap kemampuan kriptografi pada mahasiswa dengan adanya platform Spaticrypt yang diungkapkan sebagai $H_1: \mu_{post} > \mu_{pre}$ atau $H_1: \mu_D > 0$.

Dalam menentukan hasil uji t berpasangan diperlukan nilai dari taraf signifikansi. Dalam penelitian ini $\alpha = 0,05$ dipilih. Jika $t_{hitung} > t_{tabel}$, maka diterima yang berarti terdapat peningkatan keterampilan kriptografi yang signifikan pada mahasiswa dengan platform Spaticrypt. Sebaliknya jika $t_{hitung} \leq t_{tabel}$, maka H_1 ditolak yang berarti tidak terdapat peningkatan keterampilan kriptografi yang signifikan pada mahasiswa dengan platform Spaticrypt.

Diperoleh hasil uji t berpasangan dengan selisih skor rata-rata $\bar{D} = 30.542986$. Nilai signifikansi t_{count} dihitung sebesar 4,80471874 yang lebih tinggi dari nilai signifikansi $t_{hitung} = 1.70562$ dengan derajat kebebasan $Df = 25$ dan $\alpha = 0.05$. Hal ini menunjukkan bahwa nilai H_1 signifikansi diterima karena $t_{hitung} > t_{tabel}$. Artinya, terdapat peningkatan signifikan dalam keterampilan kriptografi setelah menggunakan Spaticrypt.

b. Cosine Similarity

Pada penelitian ini dilakukan pengumpulan data dari interaksi *chatbot* dengan pengguna (R). Data tersebut akan diuji menggunakan uji *cosine similarity*. Sebelumnya dilakukan pengumpulan data terkait daftar pertanyaan (Q) dan jawaban yang diharapkan (E). Selanjutnya nilai *cosine similarity* didapatkan dari hasil perbandingan E dengan R menggunakan Q. Nilai *cosine similarity* menunjukkan seberapa mirip atau relevan pertanyaan yang diajukan dengan jawaban terbaik yang diberikan oleh *chatbot*. Semakin tinggi nilai *cosine similarity* (mendekati 1), maka semakin mirip atau relevan pertanyaan dan jawaban tersebut.

Tabel 3. Hasil Cosine Similarity

Kode	Cosine Similarity	Kode	Cosine Similarity	Kode	Cosine Similarity
Q1	0.813	Q6	0.812	Q10	0.829
Q2	0.791	Q7	0.809	Q11	0.833
Q3	0.793	Q8	0.799	Q12	0.801
Q4	0.833	Q10	0.811	Q13	0.807
Q5	0.850				

Tabel 3 menunjukkan hasil pengujian *cosine similarity*. Dari data yang tersebar, diperoleh nilai rata-rata sebesar 0,814 yang tergolong nilai *cosine similarity* yang baik. Dengan demikian, dapat disimpulkan bahwa *chatbot* yang terintegrasi dalam platform Spaticrypt memiliki akurasi yang tinggi dalam memberikan jawaban yang relevan dan tepat kepada pengguna.

5. KESIMPULAN

Berdasarkan hasil penelitian, diperoleh beberapa simpulan. Pertama, penggunaan Spaticrypt sebagai media edukasi kriptografi berbasis gamifikasi CTF memiliki pengaruh positif terhadap peningkatan pemahaman pengguna terhadap kriptografi secara signifikan. Dari hasil uji T berpasangan menunjukkan nilai $t_{hitung} > t_{tabel}$ memiliki selisih nilai sebesar 3,09909874. Oleh karena itu, platform Spaticrypt dinilai cocok sebagai media edukasi baru untuk meningkatkan pemahaman kriptografi. Model *chatbot* yang terintegrasi pada platform memiliki akurasi sebesar 0,814. Artinya, *chatbot* memberikan jawaban yang relevan dan tepat kepada pengguna, sehingga berfungsi baik sebagai asisten virtual dalam pembelajaran. Dengan demikian, *chatbot* ini dapat dianggap sebagai alat bantu dalam proses pembelajaran. Pengembangan lebih lanjut dapat dilakukan dengan melakukan lebih banyak pengujian pada aplikasi terutama pada aspek keamanan dan *performance*, dan menambahkan beberapa fitur yang mendukung proses pembelajaran pada sistem aplikasi. Sebagai contoh menambahkan fitur penghargaan dan tampilan pengerjaan soal dari pengguna lain.

REFERENSI

- [1] A. M. Gjergji dan EA Lamagna, "Perangkat berbasis web untuk menjelajahi kriptografi", Jurnal Ilmu Komputer di Perguruan Tinggi, vol. 36, no. 8, hlm. 53-62, April 2021.
- [2] M. Azhari, DI Mulyana, FJ Perwitosari, dan F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)", Jurnal Pendidikan Sains dan Komputer, no. Vol.2 No.01 (2022): Artikel Riset Periode Februari 2022, hlm. 163-171, Maret 2022.
- [3] M. Syaifuddin, J. Hutagalung, dan G. Ganefri, "E-Learning Dalam Pengembangan Pembelajaran Kriptografi", JURTEKSI (Jurnal Teknologi dan Sistem Informasi), jilid. 7, tidak. 2, hlm. 117-126, April 2021, doi: 10.33330/jurteks.v7i2.914.
- [4] C. Kefalis dan A. Drigas, "Aplikasi Berbasis Web dan Online dalam Pendidikan STEM", Jurnal Internasional Pedagogi Teknik (IJEP), vol. 9, no. 4, hal. 76, Agustus 2019, doi: 10.3991/ijep.v9i4.10691.
- [5] J. Octavianus dan L. Hakim, "Perancangan Web Edukasi Kriptografi Dasar", Jurnal Algoritma, Logika dan Komputasi, vol. 6, tidak. 2, hlm.570-578, September 2023.
- [6] L. Singleton, R. Zhao, M. Song, dan H. Siy, "CryptoTutor", dalam Prosiding Konferensi Tahunan ke-21 tentang Pendidikan Teknologi Informasi, New York, NY, AS: ACM, Oktober 2020, hlm. 403-408. doi: 10.1145/3368308.3415419.
- [7] S. Abdelhamid, S. Patterson, dan B. Patterson, "Meningkatkan Pendidikan Kriptografi Menggunakan Pemrograman Visual Kolaboratif", dalam Masa Depan Pendidikan Edisi ke-12, 2022.
- [8] S. Aljraiwi, "Efektivitas Gamifikasi Pembelajaran Berbasis Web dalam Meningkatkan Prestasi Akademik dan Pemikiran Kreatif pada Siswa Sekolah Dasar", Jurnal Internasional Pendidikan dan Praktik, vol. 7, no. 3, hlm. 242-257, 2019, doi: 10.18488/journal.61.2019.73.242.257.
- [9] ctftime, "CTF Events". Diakses: 02 Agustus 2023. [Online]. Tersedia: <https://ctftime.org/>.
- [10] S. Karagiannis dan E. Magkos, "Mengadaptasi tantangan CTF ke dalam lingkungan pembelajaran keamanan siber virtual", Informasi & Keamanan Komputer, vol. 29, no. 1, hlm. 105-132, Mei 2021, doi: 10.1108/ICS-04-2019-0050.
- [11] SV Cole, "Dampak Latihan Gaya Capture the Flag (CTF) vs. Latihan Tradisional dalam Kelas Keamanan Komputer Pengantar", dalam Prosiding Konferensi ACM ke-27 tentang Inovasi dan Teknologi dalam Pendidikan Ilmu Komputer Vol. 1, New York, NY, AS: ACM, Juli 2022, hlm. 470-476. doi: 10.1145/3502718.3524806.
- [12] PA Tamayo, A. Herrero, J. Martín, C. Navarro, dan JM Tránchez, "Desain chatbot sebagai asisten pembelajaran jarak jauh", Open Praxis, vol. 12, no. 1, hal. 145, Maret 2019, doi: 10.5944/openpraxis.12.1.1063.
- [13] DPP Villanueva dan I. Aguilar-Alonso, "Chatbot sebagai Sistem Pendukung Lembaga Pendidikan", dalam Konferensi Ilmiah Internasional ke-62 tentang Teknologi Informasi dan Ilmu Manajemen Universitas Teknik Riga (ITMS) 2021, IEEE, Oktober 2021, hlm. doi: 10.1109/ITMS52826.2021.9615271.
- [14] J. Walden, N. Caporusso, dan L. Atnafu, "Chatbot untuk Mengajarkan Pemrograman Aman", [Online]. Tersedia: <https://iscap.info>; <https://proc.iscap.info>.
- [15] JJ Sophia dan TP Jacob, "EDUBOT-A Chatbot untuk Pendidikan di Pandemi Covid-19 dan Perbandingan VQAbot", dalam Konferensi Internasional Kedua 2021 tentang Elektronika dan Sistem Komunikasi Berkelanjutan (ICESC), IEEE, Agustus 2021, hlm. 1707-1714. doi: 10.1109/ICESC51422.2021.9532611.
- [16] HB Essel, D. Vlachopoulos, A. Tachie -Menson, EE Johnson, dan PK Baah, "Dampak asisten pengajar virtual (chatbot) terhadap pembelajaran siswa di pendidikan tinggi Ghana", Jurnal Internasional Teknologi Pendidikan di Pendidikan Tinggi, vol. 19, no. 1, hal. 57, November 2022, doi: 10.1186/s41239-022-00362-6.
- [17] K. Rukun dan D. Irfan, "Pengembangan Media Pembelajaran Berbasis Website untuk Komputer dan Jaringan Dasar", 2020, doi: 10.32698/GCS-PSSHES345.
- [18] NF N, S. Syarif, M. Ahmad, Budu, dan YS B, "Media pembelajaran berbasis web keterampilan menjahit ruptur perineum pada mahasiswa kebidanan", Gac Sanit, vol. 35, hlm. S248-S250, Januari 2021, doi: 10.1016/j.gaceta.2021.07.017.
- [19] CM Chen, MC Li, dan TC Chen, "Sistem anotasi membaca kolaboratif berbasis web dengan mekanisme gamifikasi untuk meningkatkan kinerja membaca", Comput Educ, vol. 144, Januari 2020, doi: 10.1016/j.compedu.2019.103697.

- [20] EM Jiménez-Hernández, H. Oktaba, F. Díaz-Barriga, dan M. Piattini, "Menggunakan perangkat lunak gamifikasi berbasis web untuk mempelajari penyederhanaan aljabar Boolean dalam pengaturan pembelajaran campuran", *Aplikasi Komputer dalam Pendidikan Teknik*, vol. 28, no. 6, hlm. 1591–1611, November 2020, doi: 10.1002/cae.22335.
- [21] M. Shane, "Menerapkan Gamifikasi pada Sistem Perekrutan Berbasis Web menggunakan Kerangka Gamifikasi Marczewski: Tinjauan Umum", *Jurnal Internasional Tren Lanjutan dalam Ilmu Komputer dan Teknik*, vol. 9, no. 3, hlm. 2667–2672, Juni 2020, doi: 10.30534/ijatse/2020/27932020.
- [22] Yusfrizal, "Rancang Bangun Aplikasi Kriptografi pada Teks Menggunakan Metode Reverse Cipher dan RSA Berbasis Android", *Jurnal Teknik Informatika Kaputama (JTik)*, vol. 3, tidak. 2, hlm. 29–37, Juli 2019.
- [23] V. Švábenský, P. Čeleda, J. Vykopal, dan S. Brišáková, "Pengetahuan dan keterampilan keamanan siber yang diajarkan dalam menangkap tantangan Bendera", *Comput Aman*, jilid. 102, hal. 102154, Maret 2021, doi: 10.1016/j.cose.2020.102154.
- [24] TE dan SIBUA Sultan, "Teknologi Open Source Untuk Lomba Keamanan Jaringan Berbasis CTF", dalam *Seminar Nasional Teknik Elektro dan Informatika (SNTEI)*, 2021, hlm.215–218.
- [25] L. Smith, MM Chowdhury, dan S. Latif, "Peretasan Etis: Keterampilan untuk Melawan Ancaman Keamanan Siber", hlm. 102–91. doi: 10.29007/vwww.
- [26] Buku Pegangan untuk CTFers. Singapura: Springer Nature Singapore, 2022. doi: 10.1007/978-981-19-0336-6.
- [27] AS Tulshan dan SN Dhage, "Survei asisten virtual: Asisten Google, Siri, Cortana, Alexa", dalam *Komunikasi dalam Ilmu Komputer dan Informasi*, Springer Verlag, 2019, hlm. 190–201. doi: 10.1007/978-981-13-5758-9_17.
- [28] N. Carlini et al., "Mengekstraksi Data Pelatihan dari Model Bahasa Besar", dalam *Simposium Keamanan USENIX ke-30 (USENIX Security 21)*, Asosiasi USENIX, Agustus 2021, hlm. 2633–2650. [Online]. Tersedia: <https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting>.
- [29] R. Mao, G. Chen, X. Zhang, F. Guerin, dan E. Cambria, "GPTEval: Survei Penilaian ChatGPT dan GPT-4", 2023.
- [30] S. Al-Saqqah, S. Sawalha, dan H. Abdelnabi, "Pengembangan perangkat lunak Agile: Metodologi dan tren", *Jurnal Internasional Teknologi Seluler Interaktif*, vol. 14, no. 11, hlm. 246–270, 2020, doi: 10.3991/ijim.v14i11.13269.
- [31] LTM Blessing dan A. Chakrabarti, *DRM, Metodologi Penelitian Desain*. London: Springer London, 2009. doi: 10.1007/978-1-84882-587-1.
- [32] D. Hellhake, T. Schmid, dan S. Wagner, "Menggunakan kriteria cakupan berbasis aliran data untuk pengujian integrasi kotak hitam pada sistem perangkat lunak terdistribusi", dalam *Prosiding - Konferensi Internasional IEEE ke-12 tentang Pengujian, Verifikasi, dan Validasi Perangkat Lunak 2019, ICST 2019, Institute of Electrical and Electronics Engineers Inc.*, April 2019, hlm. doi: 10.1109/ICST.2019.00051.
- [33] E. Suprpto, "User Acceptance Testing (UAT) Refreshment PBX Situs Outlet BNI Kanwil Padang", *Jurnal Sastra Sipil Unbari*, vol. 6, no. 2, hal. 54, Oktober 2021, doi: 10.33087/civronlit.v6i2.85.
- [34] E. Rahmi, N. Ibrahim, dan D. Kusumawardani, "Pengembangan Modul Online Sistem Belajar Terbuka dan Jarak Jauh Untuk Meningkatkan Kualitas Pembelajaran pada Program Studi Teknologi Pendidikan", *Visipena*, vol.12, no.1, pp.44–66, Juni 2021, doi: 10.46244/visipena.v12i1.1476.
- [35] Nuzul Hikmah, Dyah Ariyanti, dan Ferry Agus Pratama, "Implementasi Chatbot Sebagai Asisten Virtual di Universitas Panca Marga Probolinggo menggunakan Metode TF-IDF", *JTIM : Jurnal Teknologi Informasi dan Multimedia*, vol. 4, tidak. 2, hlm. 133–148, Agustus 2022, doi: 10.35746/jtim.v4i2.225.
- [36] A. Lahitani, US Aesyi, N. Wulandari, dan BD Santosa, "Kesamaan Kosinus untuk Mengukur Tingkat Kesadaran pada Topik Keamanan Perangkat Lunak Berbasis Teks Komentar di Media Sosial Youtube", *Jurnal Sains dan Informatika*, vol.8, no.2, Desember 2022, doi: 10.34128/jsi.v8i2.535.
- [37] F. Rahmat Halim dkk., "Rancang Bangun Sistem Informasi Pengumuman Kelulusan Siswa Berbasis Web Menggunakan Metode Agile Perancangan Sistem Informasi Pengumuman Kelulusan Mahasiswa Berbasis Web Menggunakan Metode Agile".