SIMULASI PROSES ENKRIPSI DAN DEKRIPSI KRIPTOGRAFI KLASIK BERBASIS MULTIMEDIA DALAM BENTUK 3D

Iqbal Alhuda[1], Wenda Novayani[2]

[1]Program Studi Teknik Informatika, Politeknik Caltex Riau, Jl. Umban Sari (Patin) No.

1 Rumbai, Pekanbaru, 28265

[2]Program Studi Teknik Komputer, Politeknik Caltex Riau, Jl. Umban Sari (Patin) No. 1Rumbai, Pekanbaru, 28265

E-mail: iqbalalhuda17ti@mahasiswa.pcr.ac.id, wenda@pcr.ac.id

Abstract

Cryptography is the science of changing the form of data/information so that it cannot be understood by third parties. In cryptography, there are 2 main concepts, namely encryption, and decryption. Encryption is the process of converting data/information into incomprehensible to third parties. Decryption is the process of returning data/information to its original form. Complex encryption and decryption processes make it difficult for students to understand the processes that occur in detail. This is because the learning process only uses text/writing. Based on the results of questionnaires from students who have studied classical cryptography, the most difficult algorithms to understand are the Vigenere Cipher and Affine Cipher. Thus, learning media is built in the form of multimedia- based simulations in 3D. Application development is carried out using the method User- Centered Design (UCD), which makes the user the center of the application development process. After the application has been built, the results show that the application is by userneeds based on validation using the LORI instrument of 90.55%, which is included in the very good category.

Keywords: *Simulation, Cryptography, Encryption Decryption, Vigenere Cipher, AffineCipher, Multimedia.*

Abstrak

Kriptografi adalah ilmu mengubah bentuk data/informasi menjadi tidak dapat dimengerti oleh pihak ketiga. Dalam kriptografi terdapat 2 konsep utama, yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah data/informasi menjadi tidak dapat dimengerti oleh pihak ketiga. Dekripsi adalah proses mengembalikan data/informasi kedalam bentuk semula. Berdasarkan hasil kuesioner dari mahasiswa yang sudah mempelajari kriptografi klasik, algoritma yang paling sulit dipahami adalah Vigenere Cipher dan Affine Cipher. Dengan demikian, dibangun media pembelajaran berupa simulasi berbasis multimedia dalam bentuk animasi 3D. Pengembangan aplikasi dilakukan dengan pendekatan *User Centered Design* (UCD), yaitu menjadikan *user* sebagai pusat dari proses pengembangan aplikasi. Berdasarkan validasi dengan metode *User Acceptance Testing* (UAT) yang menggunakan instrumen penilaian *Learning Object Review Instrument* (LORI), didapatkan hasil bahwa aplikasi sudah sesuai dengan kebutuhan pengguna, sehingga dapat membantu dosen dalam proses mengajar, dengan nilai validitas sebesar 90,55%.

Kata Kunci: Simulasi, Kriptografi, Enkripsi Dekripsi, Vigenere Cipher, Affine

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021

Cipher,Multimedia.

PENDAHULUAN

Kriptografi adalah ilmu yang digunakan untuk mengubah suatu data atau informasi menjadi tidak dapat dimengerti, lalu dengan sedemikian rupa dapat diubah kembali menjadi data atau informasi yang dapat dimengerti. Dalam ilmu kriptografi terdapat 2 konsep utama, yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah data atau informasi menjadi tidak dapat dimengerti oleh pihak ketiga. Sedangkan dekripsi adalah proses mengubah data atau informasi yang dienkripsi kedalam bentuk semula.

Vigenere Cipher dan Affine Cipher termasuk kedalam algoritma kriptografi klasik. Berdasarkan kuesioner yang disebarkan kepada mahasiswa G17 Teknik Informatika Politeknik Caltex Riau, didapatkan hasil bahwa algoritma Vigenere Cipher dan Affine Cipher adalah algortima kriptografi klasik yang paling sulit dipahami. Menurut Munir (2019), ada tiga alasan mengapa algoritma kriptografi klasik perlu dipelajari, meskipun algoritma kriptografi klasik sudah kadaluarsa dan sudah banyak algoritma kriptografi modern di saat sekarang ini. Yang pertama, untuk memberikan pemahaman konsep- konsep dasar dalam kriptografi, kedua adalah sebagai dasar dari algoritma kriptografi modern, dan yang ketiga agar dapat memahami potensi-potensi kelemahan pada kriptografi. Dengan mempelajari Vigenere Cipher dan Affine Cipher, mahasiswa dapat menjadikan pemahaman tersebut sebagai dasar apabila ingin merancang algoritma kriptografi modern yang baru, dan juga sebagai pembelajaran logika berpikirmahasiswa.

Mempelajari bagaimana proses enkripsi dan dekripsi pada Vigenere Cipher dan Affine Cipher dapat diperoleh dari berbagai sumber seperti buku atau modul. Tetapi, buku atau modul ajar yang hanya berupa tulisan/teks membuat orang menjadi lebih cepat bosan bila membacanya, ditambah dengan kurangnya minat mahasiswa dalam mempelajari materi kuliah, karena materinya relatif sulit dipahami dan banyaknya istilah asing (Prana, 2009). Sehingga menjadi salah satu penyebab rendahnya nilai mahasiswa pada matakuliah kriptografi (Sry Yunarti, 2018). Bu Shumaya selaku dosen pengajar mata kuliah Keamanan Data di kampus Politeknik

ISSN: 2339 – 2053

Caltex Riau, mengatakan bahwa metode pembelajaran yang hanya memanfaatkan teks/tulisan membuat mahasiswa kesulitan memahami dan cenderung tidak *excited* dalam mempelajari proses enkripsi dan dekripsi yang kompleks. Jika terdapat aplikasi yang dapat menampilkan simulasi proses enkripsi dan dekripsi secara detail, akan membuat proses pembelajaran menjadi lebih baik, serta dapat meningkatkan pemahaman dan ketertarikan terhadap materi yang diberikan.

Oleh karena itu, dibuatlah proyek akhir yang berjudul simulasi proses enkripsi dan dekripsi kriptografi klasik berbasis multimedia dalam bentuk 3D. Aplikasi dan simulasi dibangun dengan pendekatan *User Centered Design* (UCD), agar sesuai dengan kebutuhan pengguna yang dalam hal ini adalah dosen mata kuliah Keamanan Data. Simulasi dimuat dalam bentuk aplikasi berbasis *android* yang dilengkapi dengan animasi, konverter untuk melakukan enkripsi dan dekripsi, serta uji pemahaman berupa kuis. Simulasi ini digunakan sebagai media pembelajaran alternatif pada mata kuliah Keamanan Data, sehingga membantu dosen dalam proses belajar mengajar.

METODE PENELITIAN

Metode penelitian yang dilakukan dengan beberapa cara yaitu sebagai berikut:

A. *User Centered Design* (UCD)

User Centered Design (UCD) adalah sebuah metode perancangan sistem yang menjadikan *user* sebagai pusat dari proses pengembangan tersebut. Menurut Widhiarso, dkk (2007), UCD adalah filosofi perancangan suatu aplikasi yang menempatkan pengguna sebagai pusat studi proses pengembangan sistem. Terdapat 4 langkah yang dilakukan apabila menggunakan UCD sebagai metode perancangan, yaitu:

1. *Specify the Context of Use*, yaitu mengidentifikasi kegunaan dari aplikasi yangdibangun.
2. *Specify User and Organizational Requirements*, yaitu mengidentifikasikebutuhan pengguna dan organisasi yang akan menggunakan sistem.

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021

3. *Produce Design Solutions*, yaitu membuat desain dan rancangan sebagai solusi.
4. *Evaluate Design*, yaitu mengevaluasi desain dan rancangan yang sudah dibuatpada tahap sebelumnya.

B. Pengujian *User Acceptence Testing* (UAT)

User Acceptance Testing (UAT) adalah suatu proses pengujian yang dilakukan untuk memastikan bahwa solusi yang dibuat dalam bentuk aplikasi telah diterima dan sesuai dengan pengguna. Proses ini dilakukan untuk memastikan bahwa solusi dalam aplikasi yang dibuat, akan bekerja dengan baik untuk pengguna (Telkom University, 2017). Pengujian dilakukan oleh ahli yaitu bu Shumaya Resty Ramadhani, S.ST., M.Sc. yang merupakan Dosen Teknik Informatika dalam bidang Keamanan Data. Pengujian ini dilakukan dengan menggunakan *Learning Object Review Instrument* (LORI) (Nesbit, dkk, 2007).

HASIL DAN PEMBAHASAN

A. Hasil *User Centered Design* (UCD)

1. Specify the Context of Use

Pada *specify the context of use*, didefenisikan bahwa aplikasi akan digunakan sebagai media pembelajaran alternatif tentang kriptografi klasik pada mata kuliah keamanan data.

2. Specify User and Organizational Requirements

Dalam pendekatan UCD yang dilakukan dengan cara *interview*, *user* yang menjadi target adalah dosen mata kuliah Keamanan Data yaitu ibu Shumaya Resty Ramadhani, S.ST., M.Sc., kebutuhan dalam aplikasi dapat didefenisikan sebagai berikut.

1) Menu panduan belajar untuk menggunakan aplikasi.
2) Menu info aplikasi.
3) Materi pengantar yang berisi istilah/terminologi dalam kriptografi klasik dalambentuk animasi 3D.
4) Simulasi enkripsi dan dekripsi Vigere Cipher dan Affine Cipher dalam bentukanimasi 3D, dengan masing-masing 4 *case* simulasi.
5) Konverter Vigenere Cipher dan Affine Cipher yang memuat proses enkripsi dandekripsi secara dinamis menggunakan teks.

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021

6) Kuis untuk evaluasi pemahaman pengguna.

3. Produce Design Solution

Pada tahap ini, dibuatlah *design* sebagai solusi dari sistem yang akan dibangun.

1) Animasi

a. Produksi

Tahap ini adalah tahapan membuat objek komponen simulasi serta objek pendukung saat proses enkripsi dan dekripsi dalam bentuk 3D, mengatur *texturing*, pencahayaan, lalu mengatur tempat kamera tempat kejadian saat animasi dibuat, sesuai dengan *storyboard*.

b. Pasca Produksi

Tahap ini adalah tahapan terakhir pada pembuatan film. Semua hasil dari proses produksi yang telah dikerjakan akan di*rendering* menjadi sebuah video,setelah itu hasil *rendering* akan disusun sesuai dengan alur *storyoard* yang dibuat menggunakan *software* Adobe Premiere Pro. Dan terakhir, video *diexport* kedalam Unity untuk *dibuild* menjadi sebuah aplikasi *android*.

2) Antarmuka Aplikasi

a. Halaman Utama

Terdapat 3 menu, menu “Mulai Belajar” adalah menu untuk menampilkan materi pembelajaran, ikon di pojok kiri atas adalah menu untuk menampilkan informasi seputar aplikasi dan penulis, dan menu “Panduan Belajar” dibuat untuk menampilkan alur yang direkomendasikan dalam penggunaan aplikasi.

Gambar 1. Halaman Utama

b. Halaman Mulai Belajar

ISSN: 2339 – 2053

Terdapat tiga menu yang dapat diakses oleh pengguna. Namun masing-masingmenu harus dibuka secara berurutan mulai dari menu Pengantar Kriptografi.

Gambar 2. Halaman Mulai Belajar

c. Halaman Simulasi

Pengguna dapat memilih beberapa contoh plainteks/cipherteks dan kunci dari4 *case* yang disediakan untuk melakukan simulasi.

Gambar 3. Halaman Simulasi

d. Halaman Konverter

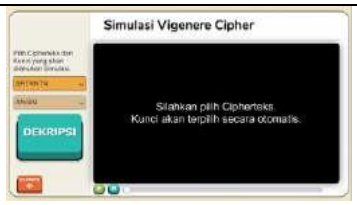
Pengguna bisa menginputkan teks dan kunci sesuai dengan keinginan, kemudian akan ditampilkan penjelasan dalam bentuk teks.

Gambar 4. Halaman Konverter

4. *Evaluate Design*

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021

1	Pada Simulasi Vigenere Cipher, tambahkan simulasi untuk proses fungsi matematika.	
2	Pada Menu Simulasi, saat pengguna ingin melakukandekripsi sebaiknya cipherteks otomatis terpilihsesuai plainteks sebelumnya.	
3	Pada Konverter Affine Cipher, saat pengguna menginputkan kunci yang salah, seharusnya proses enkripsi/dekripsi tidak bisa ditampilkan agar tidak membingungkan pengguna.	
4	*Case* atau pilihan inputanpada Simulasi enkripsi dekripsi kedua algoritma disamakan saja.	

B. Tahap terakhir adalah mengevaluasi *design* yang sudah dibuat apakah sudah sesuai dengan *user* atau belum. Berdasarkan *interview* yang dilakukan kepada *user*, berikut adalah daftar evaluasi yang didapatkan.

C. Hasil Pengujian *User Acceptence Testing* (UAT)

Validasi dilakukan dengan menggunakan standar baku *Learning Object Review Instrument* (LORI). LORI adalah aturan yang sering digunakan dalam mengukur media pembelajaran. Aspek-aspek yang diperhatikan dalam LORI yaitu *content quality*, *learning goal alignment, feedback and adaption*, *motivation*, *presentation design*, *interaction usability*, *accessibility*, *reusability*, dan *standard compliance*.

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021

Berikut validasi ahli sesuai dengan *Learning Object Review Instrument* (LORI).

Tabel 2

Hasil Validasi Materi dan Media

Aspek	Skor Penilaian	Presentase	Kategori
Content Quality	16	80%	Baik
Learning Goal Alignment	15	75%	Baik
Feedback and Adaptation	5	100%	Sangat Baik
Motivation	5	100%	Sangat Baik
Presentation Design	5	100%	Sangat Baik
Interaction Usability	12	80%	Baik
Accessibility	10	100%	Sangat Baik
Reusability	5	100%	Sangat Baik
Standards Compliance	4	80%	Baik
Rata-rata		90,55%	Sangat Baik

Berdasarkan hasil validasi yang terdapat pada Tabel 2, didapatkan rata-rata validitas keseluruhan sebesar 90,55%. Dapat disimpulkan bahwa aplikasi Simulasi Proses Enkripsi dan Dekripsi Kriptografi Klasik ini sudah sesuai dengan kebutuhan pengguna, sehingga dapat membantu dosen dalam proses mengajar.

SIMPULAN

Berdasarkan penelitian yang telah dilakukan, beberapa hal yang dapat disimpulkan dari penelitian ini, yaitu:

1. Dengan menggunakan pendekatan *User Centered Design* (UCD), aplikasi

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021

berhasil dibangun sesuai dengan kebutuhan pengguna.

2. Berdasarkan hasil validasi yang didapatkan sebesar 90,55%, aplikasi Simulasi Proses Enkripsi dan Dekripsi Kriptografi Klasik Berbasis Multimedia dalam Bentuk 3D telah berhasil diimplementasikan sesuai dengan kebutuhan pengguna, sehingga dapat membantu dosen dalam proses mengajar.

DAFTAR PUSTAKA

Nesbit, J., Belfer, K., & Leacock, T. (2009, January 01). Learning Object ReviewInstrument (LORI). Retrieved from African Virtual University: http://www.avu.org/avuorg/images/Documents/ODeLPD/lori_pt.pdf

Rinaldi Munir. (2019). "Kriptografi Edisi Kedua." Bandung: Informatika Bandung Sry Yunarti, D. M. (2018, Agustus 25). Penerapan Media Pembelajaran KriptografiBerbasis Animasi Untuk Meningkatkan Kualitas Pembelajaran Keamanan

Komputer [Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2018)].Seminar nasional, Bandung.

Suprapto, A. D. (2017). "Proses Produksi Film Animasi 3D." Retrieved from Arts of

Apple: http://www.artsofapple.com/2017/05/proses-produksi-film-animasi-3d.htmlUnity. (2020). Unity - Products. Diakses pada 1 Desember, 2020, dari

https://unity.com/products/unity-platform

Unversity, T. (2017). Panduan Dokumen User Acceptance Test (UAT). 1-4. Retrievedhttp://dac.telkomuniversity.ac.id/wp-content/uploads/2015/06/PAKA06A- Panduan-User-Acceptance-Test-UAT-20170410.pdf

Wira Sakti Prana. (2009). "Pembuatan Modul Ajar Network Security Berbasis

Multimedia."

W. Widhiarso, Jessianti, and Sutini, (2007). "Metode UCD (User Centered Design) Untuk Rancangan Kios Informasi (Studi Kasus: Rumah Sakit Bersalin XYZ)," Algoritma, vol. 3, no. 3, pp. 6–10, 2007.

ISSN: 2339 – 2053

Pekanbaru, 25 Agustus 2021