PERANCANGAN MEDIA PEMBELAJARAN KRIPTOGRAFI BERBASIS ANIMASI KOMPUTER UNTUK MENINGKATKAN MINAT BELAJAR DAN PEMAHAMAN MAHASISWA PADA POKOK BAHASAN ALGORITMA BLOK CIPHER GOST

Dikwan Moeis
Program Studi Sistem Informasi, STMIK Profesional Makassar
email: dikwan_moeis@stmikprofesional.ac.id

Abstrak

Penelitian ini dilatarbelakangi oleh kesulitan mahasiswa dalam memahami algoritma kriptografi yang bersifat abstrak. Hal ini merupakan salah satu penyebab hasil belajar pada matakuliah keamanan komputer mahasiswa rendah. Untuk menjembatani hasil belajar yang rendah diperlukan suatu metode yang tepat. Salah satu cara untuk membantu mahasiswa dalam memahami algoritma kriptografi yang bersifat abstrak adalah dengan menggunakan bantuan media pembelajaran berbasis animasi. Dengan bantuan media pembelajaran berbasis animasi tersebut mahasiswa dapat belajar secara lebih optimal dan dapat memberikan pemahaman yang lebih terhadap materi perkuliahan khususnya algoritma kriptografi cipher blok metode GOST pada matakuliah keamanan komputer. Disisi lain dapat mengurangi beban dosen dalam memberikan penjelasan yang berulang-ulang dan membutuhkan waktu. Penelitian ini bertujuan untuk membuat media pembelajaran dalam bentuk animasi komputer untuk membantu proses pembelajaran yang lebih efektif dan interaktif. Perangkat lunak yang dibuat berupa file animasi yang dapat di eksekusi dan berisi materi pembelajaran.

***Kata Kunci** : Animasi, Kriptografi, Media Pembelajaran.*

A. PENDAHULUAN

Pada matakuliah keamanan komputer terdapat pokok bahasan mengenai kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan [SCH96]. Kriptografi berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia).

Dalam pokok bahasan kriptografi tersebut dijelaskan beberapa algoritma *cipher* blok salah-satu diantaranya adalah algoritma kriptografi metode GOST. GOST atau *Gosudarstvennyi Standard*, artinya standard pemerintah, adalah algoritma enkripsi dari negara Uni Soviet dahulu (sekarang sudah terpecah menjadi sejumlah negara dengan Rusia sebagai negara terbesar). Algoritma ini dikembangkan pada tahun 1970. GOST dibuat oleh soviet sebagai alternatif terhadap algoritma enkripsi standard Amerika Serikat, DES. GOST beroperasi pada ukuran blok pesan yang panjangnya 64 bit, sedangkan panjang kuncinya 256 bit. Jumlah putaran di dalam GOST adalah 32 putaran, setiap putaran menggunakan kunci

internal. Kunci internal sebenarnya hanya ada 8 buah, K_1 sampai K_8, tetapi karena ada 32 putaran maka 8 buah kunci internal ini dijadwalkan penggunaannya.

Kurangnya penguasaan akan teori mengenai algoritma metode GOST, kurangnya kemampuan matematis dalam menguraikan proses algoritma ini dan terbatasnya waktu untuk menjelaskan secara detail proses dari algoritma ini menjadi penyebab kesulitan dalam mempelajari algoritma metode GOST. Teknologi komputer yang berkembang saat ini sangat membantu manusia dalam proses pembelajaran berbasis animasi komputer. Kelebihan yang didapat dari pembelajaran dengan menggunakan animasi komputer adalah adanya interaksi dalam proses belajar. Media pembelajaran animasi yang dibuat ini berusaha membantu mahasiswa/pembaca untuk memahami mengenai kriptografi yang secara khusus adalah algoritma metode GOST.

Dengan adanya media pembelajaran ini diharapkan dapat membantu mahasiswa/pembaca dalam memahami mengenai kriptografi metode GOST. Selain itu juga dapat memberikan alternatif metode belajar berbasis komputer selain dari buku maupun pendidikan di lembaga pendidikan.

Berdasarkan dari uraian di atas, maka penulis menentukan rumusan masalah dalam penelitian ini adalah bagaimana membuat media pembelajaran berbasis animasi yang dapat menampilkan uraian matematis mengenai proses enkripsi dan dekripsi algoritma kriptografi metode GOST?.

Untuk menjawab rumusan masalah tersebut, dalam penelitian ini akan dibuat sebuah aplikasi media pembelajaran berbasis animasi yang dapat menguraikan proses enkripsi dan dekripsi algoritma kriptografi metode GOST, kemudian menerapkannya dalam proses belajar dan mengajar di kelas.

B. METODE PENELITIAN

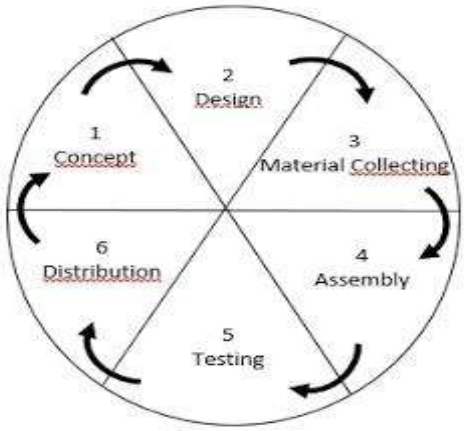
Jenis dan Tahapan Penelitian

Jenis penelitian ini adalah penelitian eksperimental yaitu pembuatan media pembelajaran berbasis animasi. Tahapan yang digunakan dalam penelitian ini adalah dengan terlebih dahulu melakukan studi literatur mengenai algoritma metode GOST pada beberapa buku, paper, maupun situs internet yang berhubungan. Kemudian penulis mengambil beberapa materi yang menjelaskan mengenai algoritma metode GOST dan membahasnya. Langkah selanjutnya adalah melakukan perancangan dan menerapkan algoritma tersebut

menggunakan aplikasi *Adobe After Effects* untuk membuat sebuah perangkat lunak yang nantinya digunakan untuk menunjang proses pembelajaran.

1. Multimedia Development Life Cycle (MDLC)

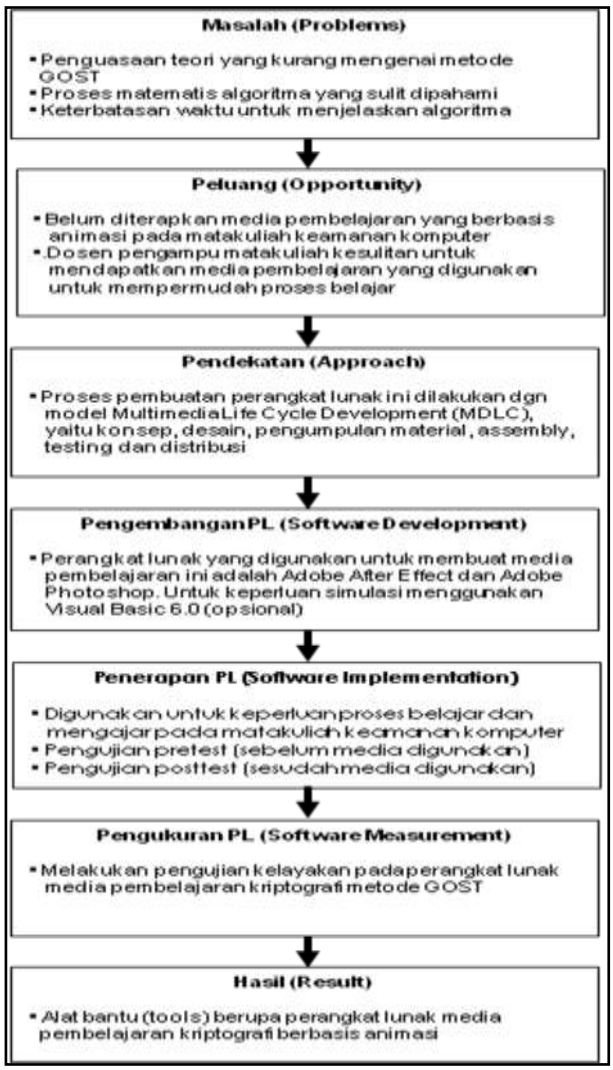
Metode yang digunakan dalam penelitian ini adalah *Multimedia Development Life Cycle*, dimana metode ini memiliki 6 tahapan, yaitu *concept*, *design*, *material collecting*, *assembly*, *testing* dan *distribution*. (Luther, 1994).



Gambar 1. Tahapan MDLC

2. Kerangka Konseptual

Kerangka konseptual merupakan suatu bentuk kerangka berpikir yang dapat digunakan sebagai pendekatan dalam memecahkan masalah. Biasanya kerangka penelitian ini menggunakan pendekatan ilmiah dan memperlihatkan hubungan antar variabel dalam proses analisisnya. Gambar kerangka berpikir dalam penelitian ini dapat dilihat pada Gambar 2 dibawah ini:



Gambar 3. Kerangka Konseptual

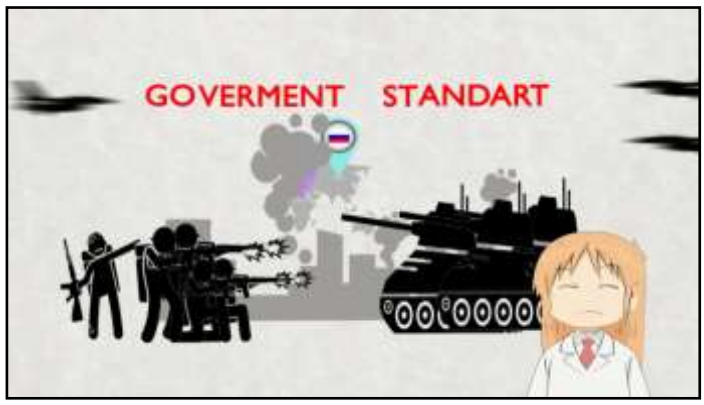
C. HASIL DAN PEMBAHASAN

Spesifikasi Perangkat Keras dan Perangkat Lunak Untuk Menjalankan Aplikasi

1. Processor Intel Core2 Duo atau AMD Phenom II (64 bit support)
2. Sistem Operasi Microsoft Windows 7 Service Pack 1 (64 bit)
3. 8 GB RAM (16 GB Recommended)
4. Space Disk 5 GB
5. 1280 x 1080 display

Hasil Pembuatan Aplikasi

Animasi ini akan menampilkan proses enkripsi dan dekripsi dari algoritma kriptografi blok *cipher* GOST. Berikut beberapa tampilan halaman dari animasi tersebut:

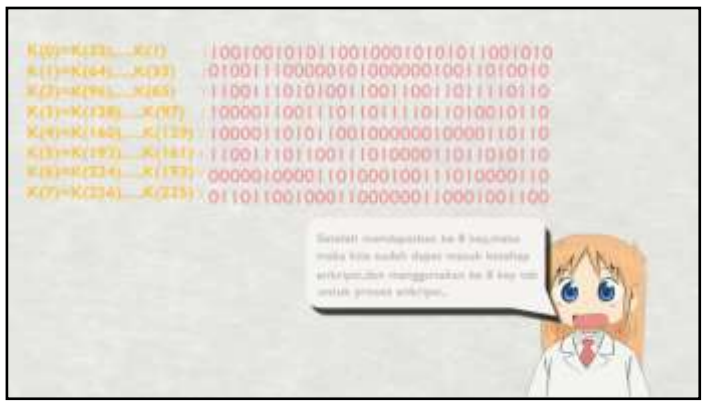


Gambar 4. Halaman utama

Gambar 4 memperlihatkan bagian dari halaman utama saat animasi dijalankan. Selanjutnya, halaman akan menampilkan beberapa teori singkat mengenai kriptografi blok *cipher* GOST. Beberapa teori singkat tersebut diperlihatkan pada gambar 4:

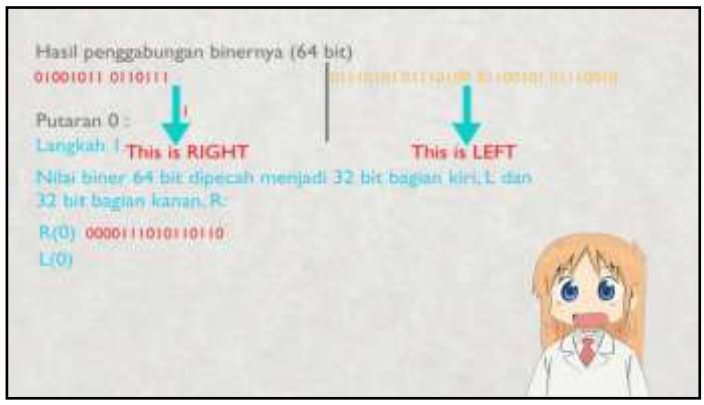
Gambar 5. Halaman teori

Pada gambar 5 memperlihatkan tahapan dari proses pembentukan kunci internal. Kunci internal ini ada 8 buah, yaitu K_0 sampai K_7.



Gambar 6. Proses pembentukan kunci internal

Selanjutnya, pada gambar 6 memperlihatkan bagian dari proses enkripsi.



Gambar 7. Proses enkripsi

Perancangan

Pemodelan dan simulasi digunakan dalam rangka penelitian, penyelidikan ataupun pengujian suatu sistem atau objek dengan maksud untuk mengetahui karakteristik tertentu dari aktivitas atau prosesnya, sehingga dengan adanya simulasi kita bisa mengetahui detail-detail kerja dari sistem. Proses perancangan animasi dapat dilihat pada gambar 7:

Gambar 8. Proses perancangan animasi

Pemberian Efek

Pada *Adobe After Effect*, proses pemberian efek itu sangat berguna dan bermanfaat dalam pembuatan animasi. Beberapa efek yang digunakan dalam pembuatan animasi adalah:

1. *Track Matte alpha*

   Merupakan layer yang tidak terlihat (*invisible layer*) yang digunakan untuk mengontrol transparansi pada layer secara langsung.

2. *Ekspression Script*

   Proses memberikan efek dengan menggunakan *script* yang dimasukkan dalam aplikasi *Adobe After Effect*, misalnya: gaya gravitasi ataupun memantul dalam animasi.

3. *Position*

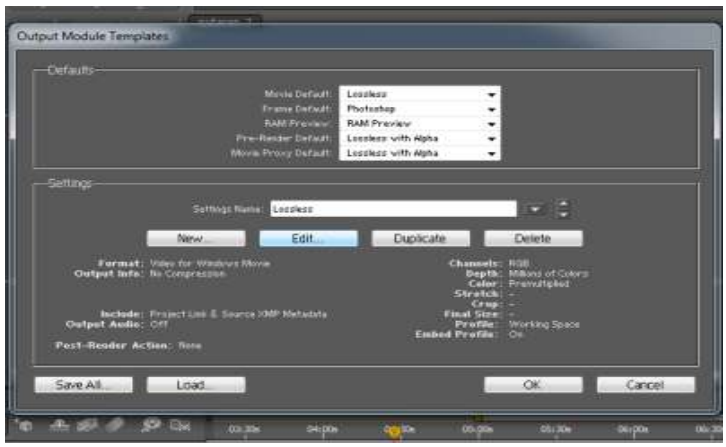
   Merupakan proses menggerakkan ke arah atas, bawah, kiri atau kanan pada text, gambar atau video agar terlihat nyata dan menyatu dengan animasi.

4. *Opacity*

   Merupakan suatu proses transparansi layer pada text, gambar atau video dari yang full color menjadi lama kelamaan menjadi hilang atau lenyap maupun sebaliknya dan akhirnya menyatu dengan animasi video.

Audio

Proses pemberian suara/audio tidak kalah penting dalam pembuatan video dan animasi ini. Audio merupakan faktor penting penghias dalam dunia visual karena dengan suara yang pas dapat membuat materi akan mudah dimengerti atau dipahami dibagian mana titik penting dalam animasi ini. Langkah-langkah dalam memasukkan audio adalah pada menu utama **Edit**, pilih sub menu **Template**, kemudian pilih **Output Module** dan centang, kemudian tekan tombol **Ok**.

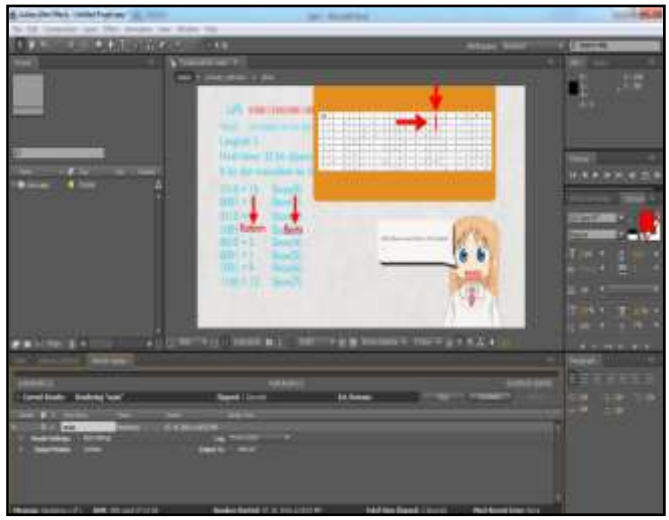


Gambar 9. Proses Audio

Render

Render adalah proses akhir menyatukan dan membangun gambar dari sebuah model menggunakan program komputer untuk menghasilkan animasi video yang berkualitas. Proses

render dapat dilakukan dengan masuk ke menu **Composition**, kemudian pilih sub menu **Make Movie**, lalu pilih **Render**, seperti terlihat pada gambar 9.



Gambar 10. Proses Render

D. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan rumusan masalah dan hasil penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Dari penelitian ini dihasilkan sebuah perangkat lunak (*software*) animasi baru tentang media pembelajaran kriptografi. Media pembelajaran animasi tersebut dapat menguraikan beberapa proses matematis dari kriptografi blok *cipher* metode GOST, yaitu: proses pembentukan kunci, proses enkripsi dan proses dekripsi.
2. Media pembelajaran animasi yang telah dihasilkan ini diterapkan pada proses belajar dan mengajar dikelas dengan metode pembelajaran *Computer Aided Learning* (CAL), yaitu metode pembelajaran yang menggunakan sistem komputer dalam menyampaikan materi pengajaran kepada mahasiswa.
3. Media pembelajaran animasi ini juga membantu mahasiswa dalam proses belajar, baik proses belajar dikelas maupun proses belajar secara mandiri. Selain itu, dengan media pembelajaran tersebut dapat meningkatkan hasil belajar mahasiswa.

Saran

Penulis ingin memberikan beberapa saran yang mungkin dapat membantu dalam pengembangan media pembelajaran berbasis animasi ini agar menjadi lebih baik, yaitu:

1. Adanya penambahan metode kriptografi lain selain metode blok *cipher* GOST.
2. Dapat dipertimbangkan untuk menambahkan beberapa teori dan tutorial pada media pembelajaran animasi tersebut agar lebih mudah dipahami.

DAFTAR PUSTAKA

[1]. Muslim, Atep. 2017. *Kreasi Animasi Menggunakan Adobe After Effect*. Andi Publisher, Yogyakarta.

[2]. MADCOMS. 2013. *Kupas Tuntas Adobe After Effect CS6*. Andi Publisher, Yogyakarta.

[3]. PIU. 2010. *Photoshop: World Best Effect Collection*. Jasakom, Jakarta.

[4]. Pressman Roger S, 2005, "Software Engineering", 6th Edition, The MacGraw-Hill Companies, Inc., Newyork.

[5]. Sommerville Ian, 2003, *"Software Engineering", 6th Edition*, Erlangga, Jakarta.

[6]. Ariyus, Dony. 2006. *Kriptografi: Keamanan Data dan Komunikasi*. Graha Ilmu, Yogyakarta.

[7]. Ariyus, Dony. 2008. *Kriptografi: Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Andi Yogyakarta, Yogyakarta.

[8]. Effendi, Empy dan Zhuang, Hartono. 2005. *e-learning: Konsep dan Aplikasi*. Andi Yogyakarta, Yogyakarta.

[9]. Moleong, Lexy. J. 1989. *Metodologi Penelitian Kualitatif*. Bandung: P.T. Rosda Karya.

[10]. HM, Jogiyanto. 2001. *Analisa & Disain Sistem Informasi: Pendekatan Ter struktur Teori dan Praktek Aplikasi Bisnis*. Andi Yogyakarta, Yogyakarta.

[11]. Agung Nugroho, Bhuono. 2005. *Strategi Jitu Memilih Metode Statistik Penelitian dengan SPSS*. Andi Yogyakarta, Semarang.

[12]. Munir, Rinaldi. 2006. *Kriptografi*. Informatika, Bandung.

[13]. Arifin, Rachmat. 2009. *Data Encryption Standard (DES)*. Jurnal STEI ITB.

[14]. Susanto, Alvin. 2009. *Analisis Feistel Cipher Sebagai Dasar Berbagai Algoritma Blok Cipher*. Jurnal STEI ITB.