

PERLINDUNGAN HAK CIPTA BUKU ELEKTRONIK MENGUNAKAN KAEDAH PENYULITAN BLOWFISH

NURFAJRINA NASERUDIN
RAVIE CHANDREN MUNIYANDI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Kaedah penyulitan digunakan untuk memastikan data yang dihantar tidak disalahgunakan oleh pihak ketiga yang boleh mengeksploit data tersebut. Hak cipta sangat penting bagi semua pemilik karya kerana jika berlaku pelanggaran hak cipta, karya pemilik boleh disalahgunakan. Untuk kajian ini algoritma *Blowfish* digunakan untuk melindungi hak cipta buku atas talian atau buku elektronik. Objektif bagi projek ini adalah untuk melindungi hak cipta buku elektronik. Dalam membangunkan projek ini pengaturcaraan PHP, html dan JavaScript digunakan.

1 PENGENALAN

Perkembangan teknologi pada masa kini semakin maju. Jika dahulu untuk membaca buku perlu pergi ke perpustakaan atau membeli buku tersebut terlebih dahulu. Kini, semuanya terletak di hujung jari sahaja dengan menggunakan telefon pintar atau gadget lain. Pembacaan atas talian atau buku elektronik boleh didapati dengan mudah dengan melayari laman web. Penulis yang lebih selesa menerbitkan buku mereka sendiri juga mendapat kelebihan untuk mengeluarkan karya penulisan mereka tanpa perlu melalui penerbit.

Sebaik buku atau karya penulis siap ianya terus menjadi hak cipta penulis tersebut. Namun dengan menggunakan laman web di atas talian keselamatan hak cipta karya penulis amat diragui. Kemungkinan untuk berlaku plagiat dan pelanggaran hak cipta amat tinggi. Oleh itu, untuk memastikan hak cipta buku-buku di atas talian ini terpelihara kaedah yang projek ini gunakan adalah penyulitan (*encryption*). Dengan menggunakan *text encryption* pihak lain tidak dapat mengakses salinan asal buku-buku di atas talian tanpa kebenaran.

Algoritma yang digunakan dalam kajian ini adalah algoritma *Blowfish encryption* yang direka oleh Bruce Schneier pada tahun 1993 dan digunakan sebagai pengganti algoritma

DES atau IDEA. *Blowfish* mempunyai 64-bit blok saiz dan panjang kunci pembolehubah dari 32 sehingga 448 bit (May Htet & Su Wai Phyo, 2016).

2 PENYATAAN MASALAH

Kini terdapat banyak laman pembacaan atas talian seperti buku elektronik. Laman web yang banyak ini tidak diketahui kadar keselamatannya. Penyataan masalah yang pertama bagi projek ini adalah plagiarisme yang bermaksud menggunakan hasil karya pihak lain tanpa kebenaran pemilik. Banyak laman web buku elektronik yang tidak dilindungi karya-karya penulisnya. Pihak tidak bertanggungjawab dengan senangnya boleh mengakses karya penulis dan mengambilnya untuk dijadikan karya sendiri.

Selain itu, masalah yang berlaku pada buku elektronik adalah pelanggaran hak cipta. Karya-karya penulis atas talian terutamanya penulis yang menerbitkan buku sendiri banyak diedarkan tanpa kebenaran dan imbuhananya diperoleh pengedar buku tersebut. Hal ini dapat dipastikan melalui kajian yang dilakukan pada 2011 iaitu *Digital Entertainment Survey* yang menyatakan bahawa 29% daripada pemilik (e-reader) mengakui melakukan cetak rompak ke atas karya. Manakala 36% pemilik tablet mengaku telah memuat turun buku elektronik secara haram (Beth Bacon, 2013).

3 OBJEKTIF KAJIAN

Projek ini bertujuan untuk melindungi hak cipta karya penulis atas talian (buku elektronik) melalui penggunaan teknologi encryption tanpa memerlukan penggunaan undang-undang hak cipta yang mengambil masa dan wang. Jika karya dilindungi dengan baik masalah pelanggaran hak cipta atau plagiarisme tidak akan berlaku.

Menggunakan kaedah penyulitan untuk melindungi karya penulis. Algoritma yang dipilih ialah penyulitan *Blowfish*. Dengan menggunakan penyulitan untuk menyulit karya terlebih dahulu sebelum disimpan dalam pangkalan data dalam bentuk menyulitkan.

4 METOD KAJIAN

Model pembangunan yang digunakan penting untuk memastikan sesuatu projek itu berjaya. Model yang digunakan untuk projek ini berdasarkan Model Air Terjun (*Waterfall model*) yang ditakrifkan oleh Winston W. Royce pada 1970. Sehingga kini model ini digunakan secara meluas untuk pelbagai projek. Antara fasa yang terdapat dalam projek ini adalah fasa perancangan, fasa keperluan, fasa reka bentuk, fasa implementasi, fasa penilaian dan fasa selenggara (Douglas Hughey, 2009).

Rajah 1 menunjukkan model pembangunan yang telah digunakan untuk membangunkan sistem Perlindungan Hak Cipta Buku Elektronik ini.

4.1 Fasa Perancangan

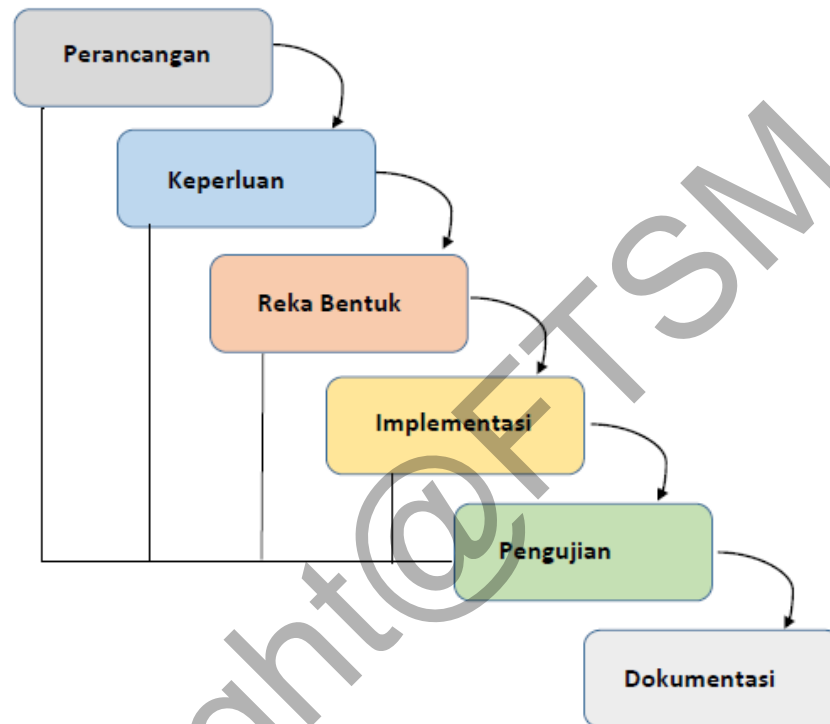
Fasa ini melibatkan proses mengenalpasti pernyataan masalah, penyelesaian masalah, objektif, skop dan metodologi kajian. Seterusnya, kajian kesusasteraan dilakukan untuk mendapatkan lebih banyak maklumat mengenai projek yang ingin dilakukan. Antara topic yang dikaji adalah hak cipta (buku elektronik), penyulitan dan algoritma *Blowfish* yang sedia ada. Pencarian maklumat menggunakan carian di internet dan juga bahan bacaan di Perpustakaan Tun Sri Lanang Universiti Kebangsaan Malaysia. Maklumat yang diperolehi dikumpul dan dianalisis untuk fasa seterusnya.

4.2 Fasa Keperluan

Fasa ini melibatkan keperluan untuk projek ini. Keperluan perkakasan dan perisian dikenalpasti dalam fasa ini. Perkakasan dan perisian yang sedia ada dikenal pasti untuk digunakan dalam sistem ini. Selain itu keperluan fungsian dan keperluan bukan fungsian juga turut dikenal pasti.

4.3 Fasa Reka Bentuk

Fasa ini sangat penting untuk kelangsungan keseluruhan projek ini. Dalam fasa ini terdapat reka bentuk seni bina, reka bentuk pangkalan data, reka bentuk antara muka dan reka bentuk algoritma.



Rajah 1 Model Pembangunan Sistem

4.4 Fasa Implementasi

Fasa implementasi ini terbahagi kepada implementasi antara muka sistem dan implementasi algoritma. Bagi implementasi projek antara muka sistem beserta fungsi dibangunkan menggunakan pengaturcaraan PHP, HTML, Bootstrap dan JavaScript. Semua maklumat yang dimasukkan akan disimpan dalam pangkalan data phpMyAdmin. Bagi reka bentuk antara muka sistem bahasa pengaturcaraan PHP, HTML dan Bootstrap digunakan untuk menghasilkan antara muka yang ringkas dan mudah difahami. Bagi implementasi algoritma pula JavaScript digunakan. Algoritma yang telah dirancang iaitu *Blowfish encryption*, akan diimplimentasikan dalam projek ini.

4.5 Fasa Pengujian

Fasa pengujian ini dilakukan untuk menguji sistem yang dibangunkan. Bagi proses pengujian ini, bermula dari perancangan ujian, reka bentuk kes-kes ujian, bersedia untuk pelaksanaan dan menilai status sehingga penutupan ujian. Langkah-langkah dalam aktiviti proses pengujian adalah seperti berikut.

1. Perancangan dan Kawalan

Tugas-tugas utama perancangan dan kawalan:

- a. Untuk menentukan skop dan risiko dan mengenal pasti objektif pengujian.
- b. Untuk menentukan pendekatan pengujian.
- c. Melaksanakan dasar pengujian atau strategi pengujian.
- d. Untuk mengetahui sumber pengujian yang diperlukan seperti persekitaran pengujian, komputer dan lain-lain.

2. Analisis dan Reka Bentuk

Tugas-tugas utama analisis dan pengujian reka bentuk:

- a. Untuk mengkaji asas kajian.
- b. Untuk mengenal pasti keadaan pengujian.
- c. Untuk mereka bentuk pengujian.
- d. Untuk menilai kebolehan keperluan dan sistem.
- e. Untuk mereka bentuk persekitaran pengujian dan mengenal pasti perkakasan yang diperlukan.

3. Melaksana dan Pelaksanaan

Tugas-tugas utama melaksana ujian:

- a. Membangunkan dan mengutamakan kes-kes ujian dengan menggunakan sebarang teknik dan mewujudkan data untuk ujian tersebut.
- b. Membuat set ujian daripada kes-kes ujian untuk pelaksanaan ujian yang cekap.

- c. Melaksana dan mengesahkan persekitarannya.

Antara fungsi yang akan diuji adalah berdasarkan Jadual 1.

ID Fungsi	Butiran fungsi Sistem
B011	Log Masuk
B012	Daftar Pengguna Baru
B013	Muat Naik Buku
B014	Penyulitan Maklumat

Jadual 1

5 HASIL KAJIAN

Bahagian ini membincangkan hasil daripada proses pembangunan sistem. Bagi pembangunan antara muka pengguna dari segi kebolegunaan fungsi Log Masuk seperti rajah (A). Menunjukkan pengguna Log Masuk Sistem. Setelah pengguna berjaya Log Masuk ke dalam sistem antara muka yang seterusnya seperti rajah (B) akan ditunjukkan.

Seterusnya, hasil pengujian dari segi keselamatan dapat dilihat dalam fungsi penyulitan yang dilakukan semasa menekan butang muat naik. Rajah (C) menunjukkan antara muka untuk muat naik buku. Dalam antara muka ini pengguna dikehendaki untuk memasukkan tajuk buku kemudian memilih buku yang ingin di muat naik. Kemudian, pengguna juga perlu memasukkan kunci untuk digunakan dalam penyulitan *Blowfish*. Penyulitan *Blowfish* dilakukan dan kemudian buku yang sudah disulitkan akan disimpan didalam pangkalan data phpMyAdmin. Setelah proses muat naik berjaya dilakukan mesej akan dipaparkan untuk memberitahu pengguna bahawa buku telah berjaya dimuat naik.

Log In

 Remember Me

Don't have an account? [Sign Up](#)

Rajah (A)

Selamat Datang ke BooksOnline

[Sign Out](#)

Rajah (B)

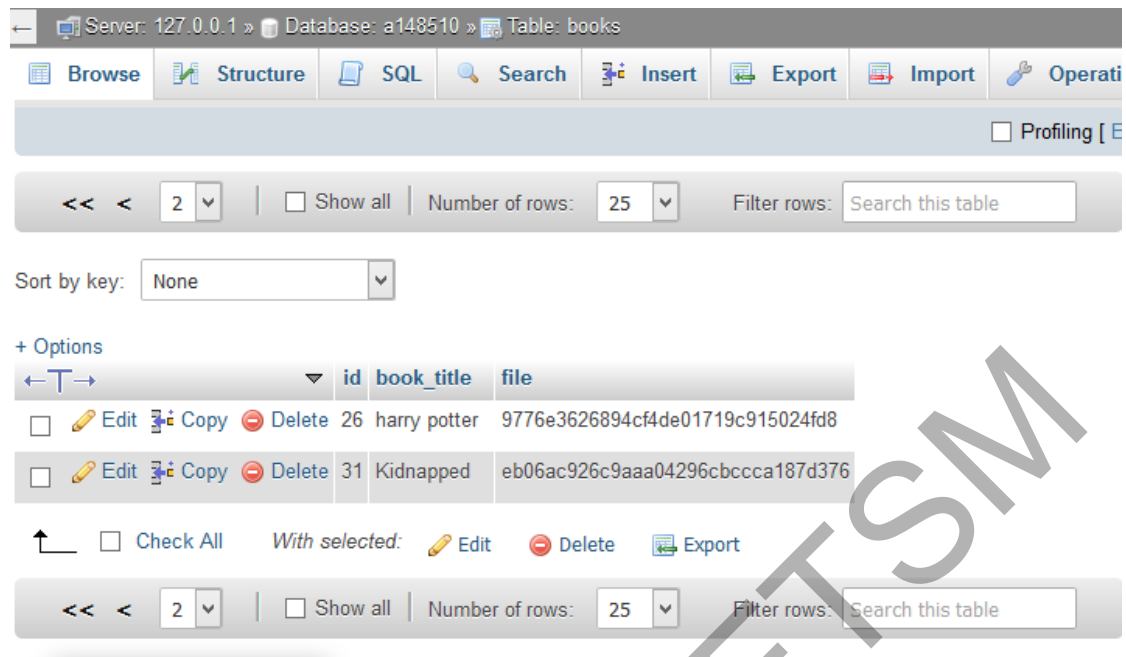
BooksOnline

Tajuk Buku

Pilih Buku Kidnapped_NT.pdf
Masukkan kunci

[Sign Out](#)

Rajah (C)



Server: 127.0.0.1 » Database: a148510 » Table: books

Profile [E]

<< < 2 | Show all | Number of rows: 25 | Filter rows: Search this table

Sort by key: None

+ Options

			id	book_title	file	
<input type="checkbox"/>	Edit	Copy	Delete	26	harry potter	9776e3626894cf4de01719c915024fd8
<input type="checkbox"/>	Edit	Copy	Delete	31	Kidnapped	eb06ac926c9aaa04296cbccca187d376

↑ Check All | With selected: Edit Delete Export

<< < 2 | Show all | Number of rows: 25 | Filter rows: Search this table

Rajah (D)

Seperti yang ditunjukkan rajah (D) iaitu pangkalan data yang menyimpan buku yang telah disulitkan.

6 KESIMPULAN

Penggunaan penyulitan *Blowfish* dapat menyulit data dengan berkesan. Hak cipta (buku elektronik) juga dapat dipelihara dengan baik jika buku tersebut disulitkan terlebih dahulu sebelum disimpan ke pangkalan data. Kelebihan sistem ini adalah algoritma *Blowfish* mudah untuk didapati. Terdapat banyak buku dan laman web yang menerangkan tentang algoritma *Blowfish* yang digunakan dalam sistem ini. Antara muka pengguna yang digunakan juga mudah difahami oleh pengguna. Pengguna yang bukan dalam bidang pembelajaran yang berkaitan juga dapat memahami sistem ini.

Selain itu, projek ini menggunakan pengaturcaraan PHP dan JavaScript untuk mengimplementasikan penyulitan *Blowfish* dalam sistem ini. Proses penyulitan dilakukan dalam sistem kemudian disimpan dalam pangkalan data.

7 RUJUKAN

- Valmik, Prof. V. K Kshirsagar. (2014). Blowfish Algorithm. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16(2), 80-83.
- Schneie, Bruce r. (n.d.). Description of a new variable-length key, 64-bit block cipher (Blowfish).
- Cornwell, Jason W. (n.d.). Blowfish Survey.
- Yang Sun. (2014). Rightholder as the Center: the DRM system in Copyright after So Many Years. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430424
- T-Institute. (2013). Transnational Journal of Science and Technology. *Transnational Journal of Science and Technology*, 3, 25- 29.
- May Htet., & Wai Phyo. (2016) A Novel Text Steganographic Technique Using Specific Alphabets. *Journal of Computer Science(JCS)*, 2(1), 1–11.
- Mathur, M., & Kesarwani, A. (2013). Comparison between DES, 3DES, RC2, RC6, Blowfish, and AES. *National Conference on New Horizons in IT (NCNHIT)*.
- Bacon, Beth. (2013). How to stop ebook pirates. Retrieved from: <http://www.digitalbookworld.com/2013/how-to-stop-ebook-pirates/>
- Hughey, Douglas. (2009). The Traditional Waterfall Approach. Retrieved from: <http://www.umsl.edu/~hugheyd/is6840/waterfall.html>