THE APPLICATION OF RANDOM NUMBER GENERATOR FOR INTERVAL MODELING IN MULTIPLE AUTHENTICATION PROCESS OF ONLINE COMPUTER BASED TRAINING

BY:

FAKHRUL HAZMAN B. YUSOFF
SHAIFIZAT BT MANSOR
SYARIFAH ADILAH BT MOHAMED YUSOFF

JANUARY 2006

UNIVERSITI
TEKNOLOGI
MARA
PERLIS
02600 Arau Perlis
Tel : 04-9874289
Fax : 04-9874255

Unit Penyelidikan, Pembangunan
& Pengkomersilan

Rujukan : 600-UiTMPs (URDC-5/1/114)
Tarikh : 13 Mei 2004

Kepada :
En. Fakrul Hazman Yusoff
Pensyarah
UiTM Perlis

Tuan,

Projek : The Impact Of Implementing Thumbprint-Based Smart Card Multiple Authentications Method For Attendance Monitoring System In Online Computer Based Training

Perkara di atas adalah dirujuk.

Sukacita dimaklumkan bahawa Mesyuarat Jawatankuasa Induk Penyelidikan pada 17 Mac 2004 telah membuat keputusan :

i) Bersetuju meluluskan cadangan penyelidikan yang telah dikemukakan oleh tuan, Cik Shaifizat Mansor dan Cik Syarifah Adilah Mohamed Yusoff.
ii) Tempoh projek penyelidikan ini ialah **12 bulan**, mulai 1 Jun 2004 hingga 31 Mei 2005.
iii) Kos yang diluluskan ialah sebanyak **RM 20,000** sahaja.
iv) Penggunaan geran yang diluluskan hanya akan diproses setelah perjanjian ditandatangani.
v) Semua pembelian peralatan yang kosnya melebihi RM 500.00 satu item perlu menggunakan Pesanan Jabatan UiTM (LO). Pihak tuan juga dikehendaki mematuhi peraturan penerimaan peralatan.
vi) Pihak tuan juga dikehendaki mengemukakan Laporan Kemajuan Projek Penyelidikan setiap 6 bulan. Laporan Akhir perlu dihantar sebaik sahaja projek penyelidikan disiapkan.

Bersama-sama ini disertakan Perjanjian untuk ditandatangani oleh pihak tuan. Sila penuhkan perjanjian berkenaan dengan menggunakan pen berdakwat hitam dan kembalikan ke pejabat ini untuk tindakan selanjutnya.

Sekian, terima kasih.

Yang benar,

PROF. MADYA DR. MAHADZIR HJ. DIN
Ketua URDC

s.k. 1. Penolong Naib Canselor (Penyelidikan), UiTM Shah Alam
2. Timbalan Bendahari UiTM Perlis

Tarikh : 15 JANUARI 2006

No. Fail Projek : 600-UiTMPs (URDC-5/1/114)

Penolong Naib Canselor (Penyelidikan)
Institut Penyelidikan, Pembangunan dan Pengkomersilan (IRDC)
UiTM, Shah Alam

Puan,

LAPORAN AKHIR PENYELIDIKAN 'THE APPLICATION OF RANDOM NUMBER GENERATOR FOR INTERVAL MODELING IN MULTIPLE AUTHENTICATION PROCESS OF ONLINE COMPUTER BASED TRAINING'.

Merujuk kepada perkara di atas, bersama-sama ini disertakan 3 (tiga) naskah Laporan Akhir Penyelidikan bertajuk 'The Application Of Random Number Generator For Interval Modeling In Multiple Authentication Process Of Online Computer Based Training'.

Sekian, terima kasih.

Yang benar,

FAKHRUL HAZMAN YUSOFF
Ketua
Projek Penyelidikan

TABLE OF CONTENTS

ABSTRACT

The Application of Random Number Generator for Interval Modeling in Multiple Authentication Process of Online Computer Based Training.

Online Computer-based Training (CBT) demand a method to ensure that the user maintain its present in-front of the computer throughout the session. One of the solutions is to force the application to invoke authentication process at regular interval. The challenge however is to ensure that the intervals are random and cannot be predicted by the user. This research compared three random number generators (RNG) that can be used to generate the interval for the authentication. The compared RNGs are Built-in VB, MRG32ka and Mersenne Twister. The comparison is to determine the suitability of the selected RNG for producing good authentication process for online CBT. The research also investigates the impact of using different seed source namely built-in clock and values derived from a Smart Card. The investigation is to determine whether usage of one of the seed source can enhance the quality of the RNG in term of better distribution and produced number sequence. The result of this research showed that although Mersenne Twister claimed that it can produce the longest sequence among the three RNGs, MRG32ka and Built-n VB RNG turn out to be a better RNG to be implemented for multiple authentications for online CBT. Meanwhile usage of different seed source did not contribute much to the quality of the RNG.