		No.FO.11.3.2-V2	HAL. 1/2
PPPM	DIR	Format PPPM: Catatan Kegiatan Harian (<i>Logbook</i>)	
30 Agustus 2017			

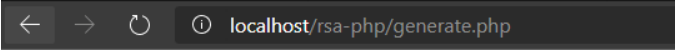

Implementasi Digital Signature dengan Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Penilaian Usulan Penelitian dan Pengabdian di Aplikasi SIMP3M

Supardianto

***Pusat Penelitian dan Pengabdian Masyarakat
Politeknik Negeri Batam
Tahun 2020***

Cara mengisi logbook :

- *Setiap melakukan kegiatan yang berhubungan dengan kegiatan penelitian/pengabdian diharuskan mengisi logbook ini.*
- *Diisi minimal seminggu sekali*
- *Kegagalan dan keberhasilan dalam melakukan uji coba juga harus ditulis disini*
- *Masalah dan hambatan juga harus ditulis disini*

No	Tanggal	Kegiatan
1	4 Juli 2020	Pengumpulan beberapa paper terkait untuk dilakukan review terkait penggunaan RSA pada pembuatan digital signature
2	18 Juli 2020	Mencoba RSA dengan melakukan perhitungan algoritma untuk mendapatkan <i>public key encryption</i> .
3	7 Agustus 2020	<p>Memimplementasikan perhitungan algoritma RSA dengan menggunakan bahasa pemrograman PHP</p>  <p>Membuat public & private key RSA</p> <pre> p=1151 q=1151 n=1324801 totient=1322500 gcd = 1 e=3 ((totient*1) + 1) / e=440833 ; sisa= 2 ((totient*2) + 1) / e=881667 ; sisa= 0 d=881667 hasil test d.e mod totient = 1 </pre> <hr/> <p>Ringkasan</p> <pre> Desimal : n =1324801 e =3 d =881667 Hexadesimal : n =143701 e =3 d =d7403 Biner : n =101000011011100000001 e =11 d =11010111010000000011 Basis 36 : n =se81 e =3 d =iwar </pre>
4	21 Agustus 2020	Mencari literature review terkait enkripsi data. Data yang dienkripsi akan menjadi message digest yang akan di gabungkan bersama algoritma RSA untuk menghasilkan digital signature.
5	28 Agustus	<p>Menggunakan enkripsi SHA3 untuk menghasilkan data yang terenkripsi.</p>  <p>Data: Ini kalimat yang akan dikunci b58a1d2f44b4ea27c9321ddd5b613cc369d4393b8edf6065eea214170c8edd335b08c7811c4e73fa70099f48b39df1d150473366bfbc8d3f4e97ae6db623</p>

Keterangan: hasil yang dicapai pada setiap kegiatan (foto, grafik, tabel, catatan, dokumen, data dan sebagainya) dilampirkan.