



## BORANG PENYERAHAN ALGORITMA

### *Algorithm Submission Form*

### SENARAI ALGORITMA KRIPTOGRAFI TERPERCAYA NEGARA (MySEAL)

MAKLUMAT SERAHAN <i>Submission Information</i>	
<input type="checkbox"/> Individu <i>Individual</i>	<input type="checkbox"/> Organisasi <i>Organisation</i>

#### A. MAKLUMAT PENYERAH

##### *Submitter Information*

MAKLUMAT PENYERAH <i>Submitter Information</i>	
NAMA PENYERAH UTAMA <i>Principal Submitter's Name</i>	
NO TELEFON PEJABAT <i>Office Tel No</i>	
NO TELEFON MUDAH ALIH <i>Mobile No</i>	
NO FAKSIMILI <i>Fax No</i>	
ALAMAT E-MEL <i>E-mail Address</i>	
ALAMAT SURAT MENYURAT <i>Postal Address</i>	

<p>NAMA PENYERAH TAMBAHAN (jika berkenaan) <i>Name of Auxiliary Submitter(s)</i> (if any)</p>	
<p>NAMA PEREKA CIPTA / PEMBANGUN ALGORITMA <i>Name of Algorithm Inventor(s) /</i> <i>Developer(s)</i></p>	
<p>NAMA PEMILIK ALGORITMA (jika berlainan daripada penyerah utama) <i>Name of Algorithm's Owner</i> (if different from the submitter)</p>	
<p>TANDATANGAN PENYERAH <i>Signature of Submitter</i></p>	

<p>MAKLUMAT ORGANISASI (untuk serahan organisasi sahaja) <i>Organisation Information (for organisation submission only)</i></p>	
<p>ORGANISASI <i>Organisation</i></p>	
<p>ALAMAT <i>Address</i></p>	

**B. MAKLUMAT ALGORITMA*****Algorithm Information***

NAMA ALGORITMA <i>Name of algorithm</i>	
PRIMITIF ALGORITMA KRIPTOGRAFI <i>Cryptographic Algorithm Primitive</i>	<input type="checkbox"/> a) <i>Symmetric Block Cipher</i> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Block Cipher</i></li> <li><input type="checkbox"/> <i>Lightweight Block Cipher</i></li> </ul> <input type="checkbox"/> b) <i>Symmetric Stream Cipher</i> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Synchronous stream cipher</i></li> <li><input type="checkbox"/> <i>Self- Synchronous stream cipher</i></li> </ul> <input type="checkbox"/> c) <i>Asymmetric</i> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Encryption</i></li> <li><input type="checkbox"/> <i>Key agreement</i></li> <li><input type="checkbox"/> <i>Digital signature</i></li> </ul> <input type="checkbox"/> d) <i>Cryptographic Hash Function</i> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Cryptographic hash function</i></li> <li><input type="checkbox"/> <i>Lightweight hash function</i></li> </ul> <input type="checkbox"/> e) <i>Cryptographic Key Generation</i>
CADANGAN TAHAP KESELAMATAN <i>Proposed Security Level</i>	<input type="checkbox"/> 40 – bit <input type="checkbox"/> 80 – bit <input type="checkbox"/> 128 – bit <input type="checkbox"/> 192 – bit <input type="checkbox"/> 256 – bit <input type="checkbox"/> Lain-lain. Sila nyatakan. <i>Other(s). Please specify</i> <hr style="width: 20%; margin-left: 0;"/>
CADANGAN PLATFORM <i>Proposed Environment</i>	<input type="checkbox"/> <i>Perkakasan Hardware</i> <input type="checkbox"/> <i>Perisian Software</i>

**C. MAKLUMAT TAMBAHAN*****Additional Information***

<p>PENGGUNAAN <i>Implementation</i></p>	<ul style="list-style-type: none"><li><input type="checkbox"/> <i>Bluetooth</i></li><li><input type="checkbox"/> <i>Global System for Mobile communications (GSM)</i></li><li><input type="checkbox"/> <i>Radio-Frequency Identification (RFID)</i></li><li><input type="checkbox"/> <i>Smart cards</i></li><li><input type="checkbox"/> <i>Mobile devices</i></li><li><input type="checkbox"/> <i>Sensor network</i></li><li><input type="checkbox"/> <i>Microcontroller</i></li><li><input type="checkbox"/> <i>Microprocessor</i></li><li><input type="checkbox"/> <i>Field-programmable gate array (FPGA)</i></li><li><input type="checkbox"/> <i>Lain-lain. Sila nyatakan.</i> <i>Other(s). Please specify</i> _____</li></ul>
---	---

**D. PENYATAAN PENYERAH**

*Statement by the Submitter*

**1. Submission statement**

I/We do hereby understand that my/our submitted algorithm may not be selected for inclusion in MySEAL. I/We also understand and agree that after the close of the submission period, my/our submission may not be withdrawn. I/We further understand that I/we will not receive financial compensation from MySEAL project for my/our submission.

**2. Statement that there are no hidden weaknesses in the algorithm design**

I/We certify that, to the best of my knowledge, I/we have fully disclosed there are no hidden weaknesses in my/our algorithm.

I/We hereby enclosed information on the known weaknesses of my/our algorithm [..... (file/attachment name)]

**3. Intellectual Property Statement for the Submission of ..... [name of algorithm] to the MySEAL Project**

..... [Submitter] currently has patents pending / has not filed for patents on the ..... [name of algorithm]. The ..... [name of algorithm] is provided royalty-free for commercial and non-commercial use in non-embedded applications. Licenses for use of the ..... [name of algorithm] in embedded applications may be obtained from ..... [name]. Aside from legal restrictions applying to encryption algorithms (if any), these licenses will be issued on a non-discriminatory basis. We will undertake to update the MySEAL project when necessary.

Diserahkan oleh (Tandatangan & Cop): <i>Submitted by (Signature &amp; Stamp):</i>  Tarikh: <i>Date:</i>	Diterima oleh (Tandatangan & Cop): <i>Received by (Signature &amp; Stamp):</i>  Tarikh: <i>Date:</i>
---	--

**SENARAI SEMAK****Checklist**

<b>Bil No</b>	<b>Perkara / Dokumen diperlukan <i>Document(s) needed</i></b>	<b>Disertakan oleh Penyerah (✓) <i>Supplied by Submitter (✓)</i></b>	<b>Disemak oleh Penerima (✓) <i>Checked by Receiver (✓)</i></b>	<b>Catatan Notes</b>
1	Profil Syarikat  <i>Company Profile</i>			
2	Laporan analisis  <i>Analysis Report</i>  <i>a) Symmetric Block Cipher</i> <input type="checkbox"/> Ujian statistik NIST <i>NIST statistical tests</i> <input type="checkbox"/> <i>Linear cryptanalysis</i> <input type="checkbox"/> <i>Differential cryptanalysis</i> <input type="checkbox"/> Lain-lain. Sila nyatakan. <i>Other(s). Please specify.</i> _____  <i>b) Symmetric Stream Cipher</i> <input type="checkbox"/> Ujian statistik NIST <i>NIST statistical tests</i> <input type="checkbox"/> <i>Algebraic attack</i> <input type="checkbox"/> <i>Correlation attack</i> <input type="checkbox"/> <i>Distinguishing attack</i> <input type="checkbox"/> <i>Guess-and-Determine attack</i> <input type="checkbox"/> Lain-lain. Sila nyatakan. <i>Other(s). Please specify.</i> _____			

Bil No	Perkara / Dokumen diperlukan <i>Document(s) needed</i>	Disertakan oleh Penyerah (v) <i>Supplied by Submitter (v)</i>	Disemak oleh Penerima (v) <i>Checked by Receiver (v)</i>	Catatan <i>Notes</i>
	<p><i>c) Asymmetric Cryptographic Algorithm</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Hard Mathematical Problems and assumptions</i></li> <li><input type="checkbox"/> <i>Security Model and its proof</i></li> <li><input type="checkbox"/> <i>Lain-lain. Sila nyatakan. Other(s). Please specify.</i></li> </ul> <hr/> <p><i>d) Cryptographic Hash Function</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Pre-image resistance</i></li> <li><input type="checkbox"/> <i>Second pre-image resistance</i></li> <li><input type="checkbox"/> <i>Collision resistance</i></li> <li><input type="checkbox"/> <i>Lain-lain. Sila nyatakan. Other(s). Please specify.</i></li> </ul> <hr/> <p><i>e) Cryptographic Key Generation</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>Probabilistic Prime Generators</i></li> <li><input type="checkbox"/> <i>Deterministic Prime Generators</i></li> <li><input type="checkbox"/> <i>Distinguishing Carmichael numbers from prime numbers</i></li> <li><input type="checkbox"/> <i>Generation of pseudo primes samples from the generator</i></li> <li><input type="checkbox"/> <i>Ujian statistik NIST NIST statistical tests</i></li> <li><input type="checkbox"/> <i>Lain-lain. Sila nyatakan. Other(s). Please specify.</i></li> </ul> <hr/>			

Bil No	Perkara / Dokumen diperlukan <i>Document(s) needed</i>	Disertakan oleh Penyerah (v) <i>Supplied by Submitter (v)</i>	Disemak oleh Penerima (v) <i>Checked by Receiver (v)</i>	Catatan <i>Notes</i>
	<p><i>f) Cryptographic Pseudo Random Number Generator Primitive</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>PRNG based on asymmetric methodologies</i></li> <li><input type="checkbox"/> <i>PRNG based on symmetric methodologies</i></li> <li><input type="checkbox"/> <i>PRNG not based on asymmetric or symmetric methodologies</i></li> <li><input type="checkbox"/> <i>Ujian statistik NIST NIST statistical tests</i></li> <li><input type="checkbox"/> <i>Lain-lain. Sila nyatakan. Other(s). Please specify.</i></li> </ul> <p>_____</p>			
3	<p>Laporan prestasi algoritma mengikut keupayaan perkakasan dan/atau perisian <i>Implementation and performance reports on hardware and/or software</i></p>			
4	<p>Laporan reka bentuk <i>Justification on design principles</i></p>			
5	<p>Vektor ujian <i>Test vectors</i></p>			
6	<p>Penyata / perjanjian / pendedahan Harta Intelek <i>Intellectual Property statements / agreements / disclosures</i></p>			