KEPALA BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA

NOMOR 443 TAHUN 2025

TENTANG

ALGORITMA KRIPTOGRAFI INDONESIA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 7 Peraturan Badan Siber dan Sandi Negara Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi, perlu menetapkan Keputusan Kepala Badan Siber dan Sandi Negara tentang Algoritma Kriptografi Indonesia;

Mengingat :

1. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
2. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);
3. Peraturan Badan Siber dan Sandi Negara Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi (Berita Negara Republik Indonesia Tahun 2024 Nomor 853);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA TENTANG ALGORITMA KRIPTOGRAFI INDONESIA

KESATU : Menetapkan Algoritma Kriptografi Indonesia sesuai dengan kategori sistem elektronik sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Kepala ini.

KEDUA : Algoritma Kriptografi Indonesia sebagaimana dimaksud dalam Diktum KESATU berlaku sejak tanggal ditetapkan, dan dapat dicabut serta diganti apabila terdapat keadaan khusus dan direkomendasikan oleh Komite Algoritma Kriptografi Indonesia.

KETIGA ...

KETIGA : Penyelenggara Sistem Elektronik yang menggunakan Algoritma Kriptografi Indonesia sebagaimana terdapat pada Keputusan Kepala ini tetap menerapkan langkah-langkah keamanan informasi lainnya sesuai standar dan peraturan yang berlaku.

KEEMPAT : Keputusan Kepala ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Depok
pada tanggal 21 Juli 2025

Ditandatangani secara elektronik oleh:
Kepala Badan Siber dan Sandi Negara

Drs. NUGROHO SULISTYO BUDI, M.M., M.Han.
Letnan Jenderal TNI (Purn)

LAMPIRAN KEPUTUSAN KEPALA
BADAN SIBER DAN SANDI NEGARA
NOMOR : 443 TAHUN 2025
TANGGAL : 21 JULI 2025

DAFTAR ALGORITMA KRIPTOGRAFI INDONESIA

A. Sistem Elektronik Rendah

NO.	JENIS ALGORITMA KRIPTOGRAFI	NAMA ALGORITMA
1	2	3
1.	Sandi Blok *(Block Cipher)*	AES-128 AES-192 AES-256 Camellia-128 Camellia-192 Camellia-256
2.	Sandi Alir *(Stream Cipher)*	HC-128 Salsa 20/20 Sosemanuk ChaCha20
3.	Fungsi *Hash* *(Hash Function)*	SHA-384 SHA-512/256 Whirlpool SHA3-256 SHA3-384 SHA3-512 SHAKE256 Blake2
4.	Pembangkit Bit Acak Deterministik berbasis Fungsi Hash (*Hash Deterministic Random Bit Generators*)	SHA1-DRBG SHA224-DRBG SHA512/224-DRBG SHA512/256-DRBG SHA256-DRBG SHA384-DRBG SHA512-DRBG SHA3-224-DRBG SHA3-256-DRBG SHA3-384 DRBG SHA3-512-DRBG
5.	Pembangkit Bit Acak Deterministik Kode Autentikasi Pesah *Hash (Hash Message Authentication Code Deterministic Random Bit Generators)*	HMAC-SHA1-DRBG HMAC-SHA224-DRBG HMAC-SHA512/224-DRBG HMAC-SHA512/256-DRBG HMAC-SHA256-DRBG

HMAC ...

1	2	3
		HMAC-SHA384-DRBG HMAC-SHA512-DRBG HMAC-SHA3-224-DRBG HMAC-SHA3-256-DRBG HMAC-SHA3-384-DRBG HMAC-SHA3-512-DRBG
6.	Pembangkit Bit Acak Deterministik berbasis sandi blok (*Deterministic Random Bit Generators Based on Block Cipher)*	AES128-CTR-DRBG AES192-CTR-DRBG AES256-CTR-DRBG
7.	Primitif Asimetrik Problem Faktorisasi Integer *(Integer Factorization Problem)*	minimum RSA-3072
8.	Primitif Asimetrik Problem Logaritma Diskrit *(Discrete Logarithm Problem)*	minimum DH-3072
9.	Primitif Asimetrik Problem Logaritma Diskrit Kurva Eliptis *(Elliptic Curve Discrete Logarithm Problem based Algorithm)*	P-384 P-512 Brainpool 256r1 Brainpool 384r1 Brainpool 512r1 Curve25519 Curve448 Edward25519 Edward448
10.	Skema Enkripsi Asimetrik *(Asymmetric Encryption Scheme)*	RSA-OEAP RSA-KEM
11.	Skema Tanda Tangan Digital Asimetrik *(Asymmetric Digital Signature Scheme)*	RSASSA-PKCS1-v1.5 RSASSA-PSS ECDSA EdDSA

B. Sistem Elektronik Tinggi

No	Jenis Algoritma Kriptografi	Nama Algoritma
1	2	3
1.	Sandi Blok *(Block Cipher)*	AES-192 AES-256 Camellia-192 Camellia-256
2.	Sandi Alir *(Stream Cipher)*	HC-128 Salsa 20/20 Sosemanuk ChaCha20

3. Fungsi ...

1	2	3
3.	Fungsi *Hash* *(Hash Function)*	SHA-384 SHA-512/256 Whirlpool SHA3-256 SHA3-384 SHA3-512 SHAKE256 Blake2
4.	Pembangkit Bit Acak Deterministik berbasis Fungsi *Hash* (*Hash Deterministic Random Bit Generators*)	SHA224-DRBG SHA512/224-DRBG SHA512/256-DRBG SHA256-DRBG SHA384-DRBG SHA512-DRBG SHA3-224-DRBG SHA3-256-DRBG SHA3-384-DRBG SHA3-512-DRBG
5.	Pembangkit Bit Acak Deterministik Kode Autentikasi Pesah *Hash* *(Hash Message Authentication Code Deterministic Random Bit Generators)*	HMAC-SHA224-DRBG HMAC-SHA512/224-DRBG HMAC-SHA512/256-DRBG HMAC-SHA256-DRBG HMAC-SHA384-DRBG HMAC-SHA512-DRBG HMAC-SHA3-224-DRBG HMAC-SHA3-256-DRBG HMAC-SHA3-384-DRBG HMAC-SHA3-512-DRBG
6.	Pembangkit Bit Acak Deterministik berbasis sandi blok (*Deterministic Random Bit Generators Based on Block Cipher)*	AES192-CTR-DRBG AES256-CTR-DRBG
7.	Primitif Asimetrik Problem Faktorisasi Integer *(Integer Factorization Problem)*	minimum RSA-3072
8.	Primitif Asimetrik Problem Logaritma Diskrit *(Discrete Logarithm Problem)*	minimum DH-3072
9.	Primitif Asimetrik Problem Logaritma Diskrit Kurva Eliptis *(Elliptic Curve Discrete Logarithm Problem based Algorithm)*	P-384 P-512 Brainpool 256r1 Brainpool 384r1 Brainpool 512r1

Curve25519 ...

1	2	3
		Curve25519 Curve448 Edward25519 Edward448
10.	Skema Enkripsi Asimetrik *(Asymmetric Encryption Scheme)*	RSA-OEAP RSA-KEM
11.	Skema Tanda Tangan Digital Asimetrik *(Asymmetric Digital Signature Scheme)*	RSASSA-PKCS1-v1.5 RSASSA-PSS ECDSA EdDSA

C. Sistem Elektronik Strategis

No	Jenis Algoritma Kriptografi	Nama Algoritma
1	2	3
1.	Sandi Blok *(Block Cipher)*	AES-256 Camellia-256
2.	Sandi Alir *(Stream Cipher)*	HC-128 Salsa 20/20 Sosemanuk ChaCha20
3.	Fungsi *Hash* *(Hash Function)*	SHA-384 SHA-512/256 Whirlpool SHA3-256 SHA3-384 SHA3-512 SHAKE256 Blake2
4.	Pembangkit Bit Acak Deterministik berbasis Fungsi *Hash* (*Hash Deterministic Random Bit Generators*)	SHA512/256-DRBG SHA256-DRBG SHA384-DRBG SHA512-DRBG SHA3-256-DRBG SHA3-384-DRBG SHA3-512-DRBG
5.	Pembangkit Bit Acak Deterministik Kode Autentikasi Pesah *Hash* *(Hash Message Authentication Code Deterministic Random Bit Generators)*	HMAC-SHA512/256-DRBG HMAC-SHA256-DRBG HMAC-SHA384-DRBG HMAC-SHA512-DRBG HMAC-SHA3-256-DRBG HMAC-SHA3-384-DRBG HMAC-SHA3-512-DRBG

6. Pembangkit ...

1	2	3
6.	Pembangkit Bit Acak Deterministik berbasis sandi blok (*Deterministic Random Bit Generators Based on Block Cipher)*	AES256-CTR-DRBG
7.	Primitif Asimetrik Problem Faktorisasi Integer *(Integer Factorization Problem)*	minimum RSA-3072
8.	Primitif Asimetrik Problem Logaritma Diskrit *(Discrete Logarithm Problem)*	minimum DH-3072
9.	Primitif Asimetrik Problem Logaritma Diskrit Kurva Eliptis *(Elliptic Curve Discrete Logarithm Problem based Algorithm)*	P-384 P-512 Brainpool 256r1 Brainpool 384r1 Brainpool 512r1 Curve25519 Curve448 Edward25519 Edward448
10.	Skema Enkripsi Asimetrik *(Asymmetric Encryption Scheme)*	RSA-OEAP RSA-KEM
11.	Skema Tanda Tangan Digital Asimetrik *(Asymmetric Digital Signature Scheme)*	RSASSA-PKCS1-v1.5 RSASSA-PSS ECDSA EdDSA