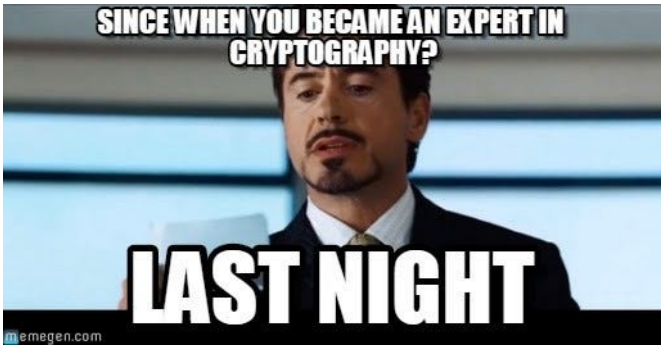
Illustration is from a fictional character in [Cytus II: Paff]

Tugas 2 IF4020-Kriptografi Semester 1 Tahun 2026/2027

Membuat Block Cipher “Baru”



Prepared for	***Prepared by***	***Deadline***
Peserta kelas IF4020-Kriptografi	A. Evander Ruizhi Xavier (18223064) Nayaka Ghana Subrata (13523090)	10 Oktober 2026 Pukul 23.59 WIB

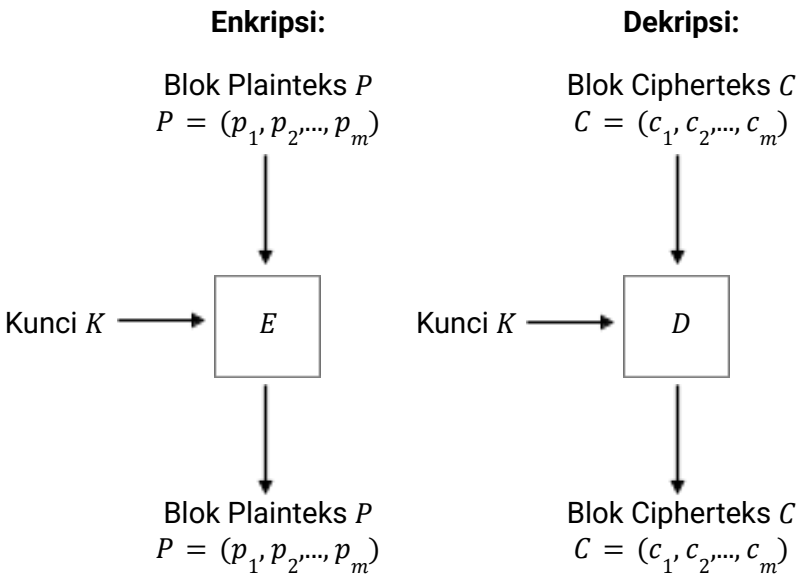
Daftar Isi

00 — *Changelog*

Belum ada perubahan pada dokumen ini.

01 — Latar Belakang

Block cipher merupakan algoritma enkripsi simetris yang mengamankan data dengan membagi pesan ke dalam blok-blok bit berukuran tetap dan mengolahnya melalui beberapa putaran transformasi. Untuk menjamin keamanannya, rancangan algoritma harus memenuhi prinsip *confusion* dan *diffusion* menggunakan operasi substitusi serta transposisi. Pada tugas ini, dilakukan perancangan dan implementasi algoritma *block cipher* baru beserta pengujian performa keamanannya yang meliputi *avalanche effect*, entropi, dan distribusi histogram dalam berbagai mode operasi enkripsi.



Gambar 2.1 Skema enkripsi dan dekripsi pada cipher blok

02 — Spesifikasi Tugas

Program yang dirancang harus dapat melakukan proses **enkripsi** dan **dekripsi** pesan menggunakan algoritma *block cipher* "baru" buatan Anda. Program wajib mengimplementasikan algoritma tersebut ke dalam berbagai **mode operasi enkripsi-dekripsi** standar serta menyediakan **fitur analisis keamanan** data hasil enkripsi.

2.1 Perancangan Algoritma *Block Cipher*

Anda harus merancang sebuah algoritma *block cipher* baru dengan ketentuan sebagai berikut:

- Ukuran blok dibebaskan, dengan ukuran blok minimum adalah sebesar **64 bit**.
- Panjang kunci utama (*master key*) **minimum adalah sepanjang ukuran blok**.
- Algoritma dapat beroperasi pada tingkat **bit, byte, atau heksadesima**l.
- Penggunaan jaringan Feistel (*Feistel network*) bersifat **opsional**, disesuaikan dengan rancangan skema enkripsi dan dekripsi.
- Proses ***enciphering*** wajib memenuhi prinsip ***confusion*** dan ***diffusion***.
- Diwajibkan untuk menerapkan minimal 2 teknik dasar, yaitu **substitusi** bit/byte berbasis ***table lookup*** (Kotak-S / *S-box*) dan **transposisi** (permutasi).
- Gunakan skema ***iterated cipher*** sebanyak n putaran (*rounds*). Setiap putaran (*rounds*) wajib menggunakan kunci putaran (*round key*) yang dibangkitkan dari kunci utama (*master key*).
- Diwajibkan untuk menerapkan minimal **1 teknik operasi tambahan di luar substitusi dan transposisi** (seperti penjumlahan modulo, kompresi, ekspansi bit, atau rotasi) untuk meningkatkan kompleksitas algoritma.
- Diizinkan untuk mengimplementasikan fitur kriptografi tambahan di luar ketentuan di atas. Silakan buat algoritma Anda dengan **sekompleks mungkin**.
- **Berikan nama** algoritma *block cipher* Anda dengan nama yang unik dan kreatif.

2.2 Implementasi Program

Setelah merancang algoritma *block cipher*, Anda harus mengimplementasikan proses enkripsi dan dekripsi algoritma tersebut dalam suatu program. Komponen masukan dan keluaran program yang diperlukan dapat dilihat pada Tabel 2.1.

Tabel 2.1 Ringkasan masukan dan keluaran program

Komponen	Keterangan
Berkas Masukan (*Input*)	Teks atau berkas biner sembarang yang akan dienkripsi atau didekripsi
Kunci Utama (*Master Key*)	Kunci rahasia masukan pengguna untuk membangkitkan *round key*
Mode Operasi	ECB (*Electronic CodeBook*), CBC (*Cipher Block Chaining*), CFB (*Cipher Feedback*), OFB (*Output FeedBack*), atau CTR (*Counter*)
***Initialization Vector* / Counter**	*Initialization Vector* (IV) untuk mode CBC, CFB, dan OFB; nilai *counter* awal untuk mode CTR
Keluaran (*Output*)	Berkas *ciphertext* hasil enkripsi atau berkas *plaintext* hasil dekripsi

Ketentuan Implementasi Program:

- Implementasi algoritma *block cipher* dan seluruh mode operasi **wajib dibuat sendiri** tanpa menggunakan pustaka (*library*) atau modul kriptografi pihak ketiga.
- Bahasa pemrograman dan bentuk antarmuka (CLI, GUI, *web-based*) **dibebaskan**.
- Program dapat dijalankan setidaknya pada sistem operasi **Windows** atau **Linux**.
- Program wajib mendukung 5 mode operasi enkripsi standar: **ECB**, **CBC**, **CFB**, **OFB**, dan ***Counter* (CTR)**.
- Program wajib menerapkan **skema penanganan sisa data (*padding*)** apabila ukuran berkas masukan bukan merupakan kelipatan dari ukuran blok. Metode *padding* yang digunakan dibebaskan (misalnya PKCS#7, ANSI X.923, zero padding, atau lainnya),

namun justifikasi pemilihan dan mekanisme *padding* harus dijelaskan di dalam laporan.

- Program harus menjamin **integritas** data hasil dekripsi.

2.3 Pengujian dan Analisis Keamanan

Setelah program diimplementasikan, lakukan pengujian untuk menganalisis keandalan dan tingkat keamanan algoritma *block cipher* yang telah Anda rancang. Pengujian dilakukan dengan ketentuan sebagai berikut:

- **Cakupan Pengujian**:
  - **Uji *Avalanche Effect***: Menghitung persentase perubahan bit pada *ciphertext* ketika 1 bit *plaintext* atau 1 bit kunci diubah.
  - **Analisis Entropi**: Menghitung derajat keacakan byte *ciphertext*. Untuk *ciphertext* tingkat byte, nilai maksimum entropinya adalah 8 bit/byte.
  - **Analisis Histogram**: Membandingkan grafik distribusi frekuensi kemunculan byte antara *plaintext* dan *ciphertext* untuk melihat apakah sebaran *ciphertext* mendekati distribusi seragam (*uniform*) atau tidak.
  - **Pengujian Tambahan (Opsional)**: Bentuk pengujian lain di luar tiga pengujian utama (sebagai contoh, pengujian dengan masukan berkas berukuran kecil, sedang, dan besar).
- Metode pengujian dibebaskan. Pengujian dapat dilakukan melalui fitur bawaan program utama, skrip terpisah, maupun *tools*/pustaka eksternal. **Pengujian dan analisis harus dilakukan pada semua mode operasi enkripsi-dekripsi**.

2.4 Bonus

1. Video (+5)
2. API *documentation* (+5)

03 — Ketentuan Umum

Batas Pengumpulan	Sabtu, 10 Oktober 2026 Pukul 23.59 WIB
Tempat Pengumpulan	https://forms.gle/rE7Hu1VaiG8xziLF6
Anggota Kelompok	3 - 4 orang (bebas pilih, boleh dengan anggota yang sama dengan tugas sebelumnya)
Sheets Kelompok	Daftar Kelompok IF4020 Kriptografi - 2026/2027
Sheets QnA	QnA Tugas IF4020 Kriptografi - 2026/2027

3.1 Berkas Pengumpulan (*deliverables*)

Pengumpulan dilakukan dengan melakukan ***release*** pada repositori Github sebelum tenggat waktu pengerjaan dan mengumpulkan tautan tersebut ke *forms* yang telah disediakan.

1. **Repositori Perangkat Lunak**

Repositori harus memuat:

a. Kode sumber (*source code*).
b. Dokumen laporan.
c. Berkas eksekutabel (*executable file*) jika relevan.
d. Folder berisi berkas uji beserta hasil pengujian (*test case*).
e. README yang minimal berisi:
    i. Nama dan deskripsi program.
    ii. Teknologi yang digunakan (*tech stack*).
    iii. Dependensi.
    iv. Tata cara menjalankan program.

2. Video Demo (Bonus)

Video demo berdurasi **maksimal 20 menit**, dengan isi sebagai berikut:

a. Deskripsi singkat program
b. Penjelasan rancangan *block cipher* dan program, termasuk bagian yang dibebaskan atau dirancang sendiri
c. Demonstrasi program dan pengujian yang dilakukan pada laporan

Apabila terdapat proses yang memerlukan waktu lama untuk dijalankan, video demo dapat dipotong atau di-*speed-up* pada bagian tersebut selama alur demonstrasi tetap jelas. Untuk ketentuan tambahan dari bonus video, silakan untuk membaca bagian 3.2 Informasi Tambahan.

3. API *Documentation* (Bonus)

Buatlah dokumentasi API yang Anda *host* ke *public service* dengan isi sebagai berikut:

a. Deskripsi API
b. Penjelasan parameter masukan (*input*) dan keluaran (*output*), beserta tipe data dari masing-masing masukan (*input*) dan keluaran (*output*)
c. Contoh penggunaan API
d. Penjelasan tambahan (jika diperlukan)

Cantumkan tautan dokumentasi API pada README repositori atau pada bagian “*details*” repositori. Untuk melakukan *hosting*, Anda dapat melakukan *host* dengan menggunakan *free services* seperti Github *pages*, Vercel *app* maupun *resource* yang sudah Anda miliki seperti *virtual machines* dan *virtual private server*.

Untuk ketentuan kakas (*tools*), pustaka (*library*), dan modul (*module*) yang Anda pilih dalam pembuatan dokumentasi, Anda dibebaskan untuk memilih dan menggunakan hal tersebut, tetapi Anda tetap perlu menjelaskan penggunaannya pada README maupun laporan. Sebagai contoh bentuk API *documentation*, Anda bisa melihat referensi berikut:

1. https://pycryptodome-master.readthedocs.io/en/latest/src/api.html
2. https://doc.sagemath.org/html/en/reference/modules/sage/modules/free_quadratic_module_integer_symmetric.html
3. https://spsdk.readthedocs.io/en/2.2.0/api/crypto.html
4. https://developer.mozilla.org/en-US/docs/Web/API/Crypto

4. Laporan

Laporan diunggah dalam format PDF dengan penamaan **NIM1_NIM2_NIM3_Tugas2_IF4020.pdf** (jika kelompok Anda memiliki anggota berjumlah 4 orang, maka tambahkan NIM untuk anggota keempat), yang memuat sistematika sebagai berikut:

a. Halaman *cover*, sertakan nama algoritma *block cipher* dan foto anggota kelompok (sebagai pengganti logo gajah pada *cover*).
b. Pernyataan tidak melakukan kecurangan (di bagian awal laporan) yang ditandatangani dengan format sebagai berikut:

Tugas dan laporan ini disusun sepenuhnya tanpa bantuan kecerdasan buatan (*Generative AI*), melainkan hasil pemikiran dan analisis mandiri. [Tanda tangan mahasiswa 1] [Tanda tangan mahasiswa 2] [Nama mahasiswa 1 (NIM)] [Nama mahasiswa 2 (NIM)]

[Tanda tangan mahasiswa 3]	[Tanda tangan mahasiswa 4]
[Nama mahasiswa 3 (NIM)]	[Nama mahasiswa 4 (NIM)]

c. **Pendahuluan:** Latar belakang, *review* singkat *block cipher* sejenis (DES, AES, dll.) sebagai pembanding, serta gagasan/pendekatan utama yang digunakan dalam rancangan *block cipher* baru.
d. **Dasar Teori:** Konsep, teori dasar, dan related works yang digunakan dalam merancang algoritma *block cipher* (**dibuat ringkas dan tidak menyita banyak halaman**).
e. **Perancangan *Block Cipher*:** Rancangan rinci algoritma *block cipher* yang dibuat, mencakup alur enkripsi, dekripsi, skema pembentukan kunci putaran (*round key*), serta seluruh komponen algoritma yang dirancang (seperti Kotak-S, permutasi, dan fungsi putaran). Penjelasan **wajib diperjelas menggunakan diagram, bagan, tabel, atau penggambaran lainnya**.
f. **Implementasi dan Simulasi:** Deskripsi ringkas antarmuka/program, hasil uji coba enkripsi dan dekripsi pada berkas teks dan biner untuk seluruh mode operasi (ECB, CBC, CFB, OFB, CTR), serta analisis bukti penanganan *padding* dan verifikasi integritas data.
g. **Analisis Keamanan:** Pembahasan dan analisis dari hasil pengujian *Avalanche Effect*, Entropi, Histogram, serta pengujian tambahan lainnya (jika ada). Silakan pelajari beberapa paper yang dilampirkan pada referensi dokumen ini.
h. **Kesimpulan dan Saran Pengembangan (*Future Works*).**
i. **Daftar Pustaka (Referensi).**
j. **Lampiran:**

i. Pranala repositori *source code*.
ii. Pranala video demo program (jika ada).
iii. Tabel pembagian tugas masing-masing anggota.

3.2 Informasi Tambahan

***Assistant notes*:**

1. Batas pengisian *sheets* kelompok adalah **Sabtu, 26 September 2026 Pukul 23.59 WIB**. Jika ada peserta kelas yang belum mendapatkan kelompok atau belum mengisi *sheets* kelompok dalam batas waktu yang ditentukan, asisten akan melakukan *shuffle* anggota kelompok secara *random* untuk peserta kelas yang belum mendapatkan atau belum mengisi *sheets* kelompok.
2. Karena penggunaan *generative AI* tidak diperbolehkan (*web based* maupun *agentic*), Anda di-*encourage* untuk memahami kembali salindia perkuliahan, melakukan eksplorasi di internet, ataupun bertanya kepada teman Anda atau peserta kelas lainnya.

   Mengutip perkataan dari **Terence Tao**, seorang *prodigy mathematician*:

   “You actually do need a certain level of distractions in your life”

   Sumber: Why Great Thinking Needs Distraction – Terence Tao
3. Anda tidak boleh melakukan *copy paste* pada implementasi algoritma yang sudah ada (sebagai contoh: AES, DES, Blowfish), tetapi tetap diperbolehkan untuk mengambil beberapa ide dari algoritma yang sudah ada sebagai inspirasi untuk implementasi algoritma yang Anda rancang. **Pelanggaran pada aturan ini akan berakibat pada diberikannya nilai 0 untuk tugas ini**.
4. **[Khusus untuk bonus video]** Video harus di-*upload* ke Youtube dan bersifat *public* (format penamaan dan deskripsi video bebas, asalkan tetap menggambarkan isi dari

tugas) dan semua anggota wajib untuk menjelaskan bagiannya masing masing (wajib *oncam* dan melakukan perkenalan). Video tidak boleh berupa tautan lain selain dari *domain* youtube.com (langsung cantumkan di laporan). Oleh karena itu, jika Anda melakukan *submit* dengan *google drive*, bit.ly, dan tautan lainnya, bonus akan dianulir dan dianggap invalid.

Pengecualian:

1. **[Untuk poin 2 pada *assistant notes*]** Jika muncul hasil *AI overview* dari *search engine*, Anda boleh untuk tetap menggunakannya (atau tambahkan *flag* `-ai` bagi pengguna Google Chrome di akhir *query* jika tidak ingin memunculkan *AI overview*), tetapi tidak boleh untuk lanjut melakukan *prompt*. Penggunaan *code completion* seperti Copilot diperbolehkan.

04 — Referensi

Referensi berikut disediakan sebagai bahan pendukung, bukan sebagai batasan atau standar implementasi. Sumber lain yang relevan tetap dapat digunakan.

[1] H. M. Heys, “A Tutorial on the Implementation of Block Ciphers: Software and Hardware Applications,” Cryptology ePrint Archive, Report 2020/1545, 2020. [Online]. Available: https://eprint.iacr.org/2020/1545.pdf

[2] National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication (FIPS) 197, NIST FIPS 197-upd1, updated May 9, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

[3] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, “The RC6 Block Cipher,” ver. 1.1, Aug. 20, 1998. [Online]. Available: https://people.csail.mit.edu/rivest/pubs/RRSY98.pdf

[4] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “The Twofish Encryption Algorithm,” Sep. 2000. [Online]. Available: https://www.researchgate.net/publication/234781510_The_Twofish_Encryption_Algorithm

[5] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” in Cryptographic Hardware and Embedded Systems - CHES 2006, Lecture Notes in Computer Science, vol. 4249, pp. 46–59, Springer, 2006. [Online]. Available: https://link.springer.com/chapter/10.1007/11894063_4

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” in Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727, pp. 450–466, Springer, 2007. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-74735-2_31

[7] Z. Gong, S. Nikova, and Y. W. Law, “KLEIN: A New Family of Lightweight Block Ciphers,” in RFID. Security and Privacy – 7th International Workshop, RFIDSec 2011, Lecture Notes in Computer Science, vol. 7055,

pp. 1–18, Springer, 2011. [Online]. Available: https://ris.utwente.nl/ws/files/5095833/The_KLEIN_Block_Cipher.pdf

[8] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, “The 128-Bit Blockcipher CLEFIA (Extended Abstract),” in Fast Software Encryption - FSE 2007, Lecture Notes in Computer Science, vol. 4593, pp. 181–195, Springer, 2007. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-74619-5_12

[9] R. M. Needham and D. J. Wheeler, “Tea Extensions,” Technical Report, Computer Laboratory, University of Cambridge, Oct. 1997. [Online]. Available: http://www.club.cc.cmu.edu/~ajo/docs/xtea.pdf

[10] S. Banik, Z. Bao, T. Isobe, H. Kubo, F. Liu, K. Minematsu, K. Sakamoto, N. Shibata, and M. Shigeri, “WARP: Revisiting GFN for Lightweight 128-Bit Block Cipher,” in Selected Areas in Cryptography – SAC 2020, Lecture Notes in Computer Science, vol. 12804, pp. 535–564, Springer, 2021. [Online]. Available: https://eprint.iacr.org/2020/1320.pdf. doi: 10.1007/978-3-030-81652-0_21.

[11] C. Burwick, D. Coppersmith, E. D’Avignon, R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas Jr., L. O’Connor, M. Peyravian, D. Safford, and N. Zunic, “MARS - A Candidate Cipher for AES,” IBM Corporation, revised Sep. 22, 1999. [Online]. Available: https://shaih.github.io/pubs/mars/mars.pdf

05 — End Of File

“*Must’ve been the wind* 🥀 (*Also* semangat buat UTS-nya OwO)”
~ Nayaka

baru nguli tugas 1 lgsg muncul tugas 2… (maaf yhh.. smgt jg 🫠)
~ Evan