

LAPORAN UTS

KRIPTOGRAFI (TEMA: ROT13)

Tugas ini disusun untuk memenuhi tugas mata kuliah Kriptografi

Dosen Pengampu:

Saiful Nur Budiman, S.Kom., M.Kom



DISUSUN OLEH:

KELOMPOK 2

| | |
|----------------------------|---------------|
| ARVILANTI DEVANI | (22104410075) |
| RIZKI RAMADHAN | (22104410088) |
| NUR CINDY INTAN FANDERELLA | (22104410098) |
| HANIK HATUL HALIMAH | (22104410101) |
| WASI'ATUL JANNAH | (22104410121) |
| SAHRUL RAMADHAN | (22104414002) |

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS ISLAM BALITAR

2025

DAFTAR ISI

| | |
|--|----|
| DAFTAR ISI..... | i |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 2 |
| 1.3 Tujuan Proyek..... | 2 |
| BAB II LANDASAN TEORI..... | 3 |
| 2.1 Kriptografi | 3 |
| 2.2 Kriptografi Klasik..... | 3 |
| 2.3 Caesar Cipher..... | 4 |
| 2.4 ROT13 | 4 |
| 2.5 Python | 5 |
| BAB III PEMBAHASAN..... | 6 |
| 3.1 Cara Kerja Algoritma ROT13 dalam Proses Enkripsi dan Dekripsi Teks | 6 |
| 3.2 Implementasi Algoritma ROT13 Menggunakan Bahasa Pemrograman Python | 7 |
| 3.3 Hasil Uji Coba Proses Enkripsi dan Dekripsi ROT13..... | 8 |
| BAB IV PENUTUP | 9 |
| 4.1 Kesimpulan..... | 9 |
| DAFTAR PUSTAKA..... | 10 |
| LAMPIRAN..... | 12 |

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang sangat pesat telah mendorong peningkatan kebutuhan akan keamanan data dalam berbagai bidang kehidupan manusia. Setiap hari, jutaan data pribadi, transaksi digital, dan komunikasi elektronik berpindah melalui jaringan internet, sehingga risiko penyadapan, peretasan, serta penyalahgunaan informasi menjadi semakin tinggi. Dalam konteks ini, keamanan data menjadi aspek penting yang harus diperhatikan oleh setiap individu maupun organisasi.

Salah satu cara yang umum digunakan untuk melindungi data dari akses yang tidak sah adalah melalui kriptografi. Kriptografi merupakan salah satu teknik dasar dalam keamanan informasi yang mencakup proses-proses penting seperti enkripsi dan dekripsi. Enkripsi adalah prosedur mengubah pesan terbaca (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext), sedangkan dekripsi adalah proses kebalikannya, yaitu mengembalikan ciphertext ke bentuk plainteks sehingga dapat dipahami oleh pihak yang berwenang (Hulu & Putri, 2022). Selain hanya untuk mengamankan pesan, penerapan kriptografi dalam konteks digital modern meliputi autentikasi, tanda tangan digital, penyimpanan data rahasia, serta mekanisme non-repudiasi, yaitu memastikan bahwa pengirim tidak dapat menampik telah mengirim pesan tersebut (Harahap & Salim, 2018).

Secara umum, kriptografi dibagi menjadi dua kategori besar, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik menggunakan teknik sederhana berbasis penggantian (substitusi) atau pergeseran (transposisi) huruf pada teks, sedangkan kriptografi modern menggunakan operasi matematis dan kunci digital yang lebih kompleks untuk menjaga keamanan data (Dewi, 2024). Meskipun metode klasik dianggap kurang aman terhadap serangan modern, kriptografi jenis ini tetap relevan dalam konteks pembelajaran dasar mengenai konsep enkripsi dan dekripsi karena mudah dipahami serta dapat diimplementasikan menggunakan algoritma sederhana seperti Caesar Cipher atau Vigenère Cipher.

Salah satu algoritma kriptografi klasik yang terkenal dan mudah diterapkan adalah ROT13 (Rotate by 13 Places). Algoritma ini merupakan bentuk modifikasi dari Caesar Cipher, di mana setiap huruf digeser sejauh 13 posisi dalam alfabet. Keunggulan ROT13 terletak pada sifat simetrisnya, yaitu proses enkripsi dan dekripsi dapat dilakukan

menggunakan metode yang sama tanpa memerlukan kunci tambahan (Milian & Sulistyo, 2023). Meskipun algoritma ini tidak memberikan tingkat keamanan yang tinggi, ROT13 masih sering digunakan dalam konteks edukatif dan penyamaran teks ringan, seperti penyembunyian pesan sederhana, teka-teki, maupun pengaburan konten tertentu pada forum daring (Sitompul et al., 2024).

Meskipun tergolong sederhana, algoritma ROT13 memiliki nilai penting dalam pengenalan konsep dasar kriptografi karena mudah diimplementasikan dan dipahami. Melalui algoritma ini, pengguna dapat mempelajari bagaimana proses substitusi huruf bekerja serta memahami prinsip simetri antara enkripsi dan dekripsi. Dalam konteks pendidikan dan penelitian dasar, ROT13 sering digunakan untuk melatih pemahaman terhadap logika enkripsi sebelum beralih ke algoritma yang lebih kompleks. Pengembangan varian ROT13 dapat dijadikan model pembelajaran efektif dalam memahami keamanan data berbasis substitusi sederhana (Milian & Sulistyo, 2023). Oleh karena itu, pembahasan mengenai algoritma ROT13 dalam laporan ini bertujuan untuk memberikan pemahaman mendasar mengenai penerapan kriptografi klasik, sekaligus menjadi langkah awal dalam mengembangkan sistem enkripsi yang lebih aman dan efisien di masa mendatang.

1.2 Rumusan Masalah

1. Bagaimana cara kerja algoritma ROT13 dalam melakukan proses enkripsi dan dekripsi pada data teks?
2. Bagaimana cara mengimplementasikan algoritma ROT13 menggunakan bahasa pemrograman Python tanpa menggunakan library enkripsi bawaan?
3. Bagaimana hasil uji coba proses enkripsi dan dekripsi ROT13 terhadap input teks yang berbeda?

1.3 Tujuan Proyek

1. Untuk memahami dan menjelaskan prinsip kerja algoritma ROT13 dalam proses enkripsi dan dekripsi teks.
2. Untuk mengimplementasikan algoritma ROT13 menggunakan bahasa pemrograman Python secara manual, tanpa memanfaatkan library enkripsi bawaan.
3. Untuk menguji hasil enkripsi dan dekripsi menggunakan ROT13 terhadap berbagai input teks guna memastikan bahwa algoritma bekerja secara simetris.

BAB II

LANDASAN TEORI

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yang berarti "penulisan rahasia", yaitu ilmu dan seni pengamanan informasi yang menjadi dasar penting dalam keamanan sistem komputer (Wardana, 2019). Kriptografi merupakan praktik perlindungan informasi baik yang diam (pada *hard drive*), bergerak (komunikasi elektronik), maupun yang sedang digunakan melalui penggunaan teknik matematis, algoritma kode, *hash*, dan tanda tangan digital (Rahman et al., 2024; Wardana, 2019). Tujuan fundamental dari sistem kriptografi adalah menjaga kerahasiaan data (memastikan hanya pihak berwenang yang dapat mengaksesnya menggunakan kunci yang tepat), mempertahankan integritas data (mencegah manipulasi atau perubahan tidak sah seperti penyisipan atau penghapusan), dan menjamin autentikasi (mengidentifikasi kebenaran pihak-pihak yang berkomunikasi), serta menyediakan ketiadaan penyangkalan (Rahman et al., 2024; Wardana, 2019). Proses inti dalam kriptografi melibatkan penggunaan algoritma kriptografi, yaitu sebuah fungsi matematika yang bergantung pada nilai kunci untuk mengubah data jelas (*plaintext*) menjadi data sandi (*ciphertext*) melalui enkripsi, dan mengembalikannya melalui dekripsi (Munawar et al., 2023; Rahman et al., 2024; Wardana, 2019). Kekuatan algoritma ini diukur dari seberapa sulitnya memperoleh nilai kunci yang benar dari seluruh ruang kunci yang memungkinkan (Munawar et al., 2023).

2.2 Kriptografi Klasik

Kriptografi klasik adalah teknik kriptografi yang digunakan sebelum era komputerisasi (Sasono et al., 2023). Algoritma ini umumnya beroperasi pada level karakter atau alfabet. Ciri utamanya adalah penggunaan pena dan kertas atau alat mekanis sederhana. Algoritmanya juga relatif mudah dipecahkan dengan teknik modern.

Metode kriptografi klasik secara umum dibagi menjadi dua (Sasono et al., 2023):

1. *Cipher* Substitusi: Mengganti setiap karakter *plaintext* dengan karakter lain. Contoh: *Caesar Cipher*, *Vigenere Cipher*.
2. *Cipher* Transposisi: Mengubah urutan (permutasi) karakter dalam *plaintext*. Contoh: *Rail Fence Cipher*.

ROT13 termasuk dalam kategori *cipher* substitusi.

2.3 Caesar Cipher

Caesar Cipher merupakan salah satu metode algoritma yang dipakai untuk sistem kriptografi simetri. Metode ini sering dipakai sebelum adanya sistem kriptografi kunci publik (Hidayah et al., 2023). Caesar Cipher termasuk jenis metode cipher substitusi yang membuat cipher melalui proses pergantian satu karakter yang diubah dengan karakter lain di beberapa jumlah digit sebelah kanan atau kirinya, sesuai arah pergeserannya (Dwi Putri et al., 2019). Caesar Cipher memiliki kelebihan untuk menyamarkan suatu pesan yang bisa tersandi karena hanya pengirim dan penerima saja yang bisa mengetahui sandinya. Selain itu, Caesar Cipher juga memiliki kelemahan yaitu tidak dapat melakukan enkripsi ataupun dekripsi terhadap pesan yang tersusun dari beberapa kalimat dan juga rumus yang ditemukan (Hidayah et al., 2023).

2.4 ROT13

ROT13 merupakan sebuah fungsi yang memakai kode kaisar dengan melakukan pergeseran $k=13$. ROT13 dirancang untuk keamanan pada sistem operasi UNIX yang banyak terdapat pada forum-forum *online* yang bermanfaat untuk melindungi isi artikel. Proses enkripsi dari ROT13 dengan menggeser maju karakter sebanyak 13 kali terhitung mulai 1 karakter yang ada didepannya, sedangkan untuk deskripsinya dengan menggeser mundur karakter 13 kali yang terhitung 1 karakter dibelakangnya. Pergeseran karakter tersebut dengan berdasar pada urutan karakter pada tabel ASCII.

Formula yang digunakan sebagai berikut (Milian & Sulistyo, 2023).

$$C = (P + K) \text{ Mod } n$$

$$P = (C - K) \text{ Mod } n$$

Keterangan :

C = *Ciphertext*

P = *Plaintext*

K = *Key (13)*

Mod = *Modulo*

n = Jumlah karakter *plaintext*

2.5 Python

Bahasa pemrograman Python merupakan bahasa pemrograman yang populer dalam bidang analisis data. Hal tersebut karena Python mudah untuk dipelajari dan digunakan di semua kalangan usia. Selain itu, bahasa pemrograman Python memiliki Library yang bervariasi yang memiliki kegunaannya masing-masing dan dapat digunakan oleh siapa saja di berbagai sistem operasi atau dengan kata lain bersifat *open source*. Beberapa contoh Library Python antara lain adalah NumPy, Pandas, Matplotlib, dan Scikit-learn yang masing-masing berguna untuk analisis data, pemodelan statistik, visualisasi data, dan machine learning. Tidak hanya itu, Python juga mudah diintegrasikan dengan teknologi lain, seperti database, big datatools, frameworkweb, dan lain sebagainya yang berhubungan dengan analisis data dengan tujuan untuk mengakses dan mengelola data dari berbagai sumber (Angelina M. T. I. Sambi Ua et al., 2023).

BAB III

PEMBAHASAN

3.1 Cara Kerja Algoritma ROT13 dalam Proses Enkripsi dan Dekripsi Teks

Algoritma ROT13 (Rotate by 13 places) merupakan salah satu bentuk sederhana dari Caesar Cipher, yaitu algoritma substitusi yang menggantikan setiap huruf dengan huruf lain yang berjarak 13 posisi setelahnya dalam urutan alfabet. Proses ini bekerja pada huruf-huruf dalam alfabet Latin (A–Z), dan karena total huruf alfabet adalah 26, maka jika dilakukan pergeseran sebanyak 13 posisi dua kali, huruf tersebut akan kembali ke bentuk semula. Hal ini membuat ROT13 bersifat simetris, yaitu proses enkripsi dan dekripsi menggunakan algoritma yang sama.

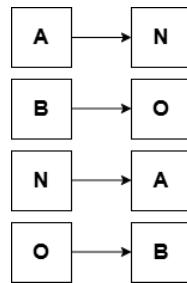
Langkah kerja algoritma ROT13 :

1. Setiap huruf teks diubah ke huruf kapital agar konsisten.
2. Huruf dikonversi menjadi nilai numerik berdasarkan posisinya dalam alfabet ($A=0$, $B=1, \dots, Z=25$).
3. Nilai posisi digeser sebanyak 13 langkah dengan operasi modulo 26:

$$\text{posisi baru} = (\text{posisi lama} + 13) \bmod 26$$

4. Nilai hasil dikonversi kembali menjadi huruf alfabet.
5. Spasi dan karakter non-huruf tidak diubah.

Karena menggunakan operasi modulo 26, huruf yang melewati “Z” akan kembali ke “A”. Misalnya:



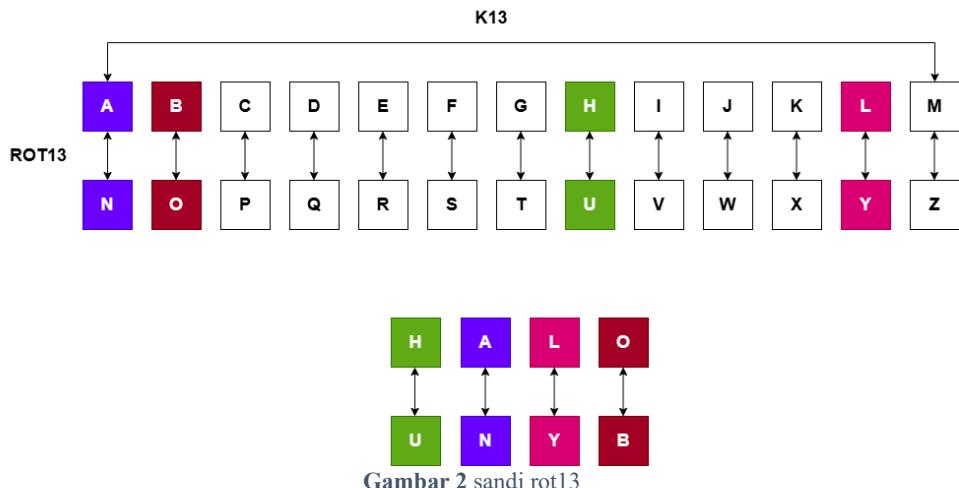
Gambar 1 operasi modulo

Proses dekripsi dilakukan dengan algoritma yang sama, karena jika huruf digeser 13 kali dua kali ($13 + 13 = 26$), maka akan kembali ke posisi awal. Contoh :

Teks asli : HALO

Enkripsi : UNYB

Dekripsi : HALO



3.2 Implementasi Algoritma ROT13 Menggunakan Bahasa Pemrograman Python

Algoritma ROT13 dapat diimplementasikan dengan sangat sederhana menggunakan bahasa Python, tanpa bantuan library kriptografi bawaan. Implementasi dilakukan dengan memanfaatkan fungsi dasar Python seperti `ord()` dan `chr()`.

```

1 def rot13(teks):
2     hasil = ""
3     teks = teks.upper() # Mengubah huruf ke kapital agar seragam
4
5     for huruf in teks:
6         if huruf == " ":
7             hasil += " " # Spasi tidak diubah
8         elif huruf.isalpha():
9             pos = ord(huruf) - ord('A') # Ubah huruf jadi angka (0-25)
10            pos = (pos + 13) % 26 # Geser huruf 13 posisi
11            hasil += chr(pos + ord('A')) # Ubah kembali ke huruf
12
13    return hasil

```

Gambar 3 fungsi ROT13

Fungsi `rot13()` di atas digunakan baik untuk enkripsi maupun dekripsi, karena sifat simetris dari algoritma ROT13. Program utama kemudian meminta input dari pengguna, melakukan validasi agar hanya huruf dan spasi yang diterima, serta menampilkan hasil enkripsi dan dekripsi. Semua proses dicatat ke dalam list riwayat untuk menampilkan seluruh hasil yang telah diproses.

Struktur utama program:

1. Input teks dari pengguna.
2. Validasi input agar hanya huruf/spasi yang diproses.
3. Panggil fungsi rot13() untuk enkripsi dan dekripsi.
4. Tampilkan hasil ke layar.
5. Simpan riwayat hasil enkripsi dan dekripsi dalam list.

3.3 Hasil Uji Coba Proses Enkripsi dan Dekripsi ROT13

Pengujian dilakukan dengan beberapa input teks berbeda untuk melihat hasil proses enkripsi dan dekripsi. Karena algoritma ROT13 bersifat simetris, hasil dekripsi akan selalu sama dengan teks aslinya.

```
== PROGRAM ROT13 ==
Ketik exit untuk berhenti.

Masukkan teks : Halo
Hasil Enkripsi : UNYB
Hasil Dekripsi : HALO

Masukkan teks : Kami dari kelompok dua
Hasil Enkripsi : XNZV QNEV XRYBZCBX QHN
Hasil Dekripsi : KAMI DARI KELOMPOK DUA

Masukkan teks : exit

== RIWAYAT ENKRIPSI & DEKRIPSI ==
1. HALO -> UNYB -> HALO
2. KAMI DARI KELOMPOK DUA -> XNZV QNEV XRYBZCBX QHN -> KAMI DARI KELOMPOK DUA

Program selesai. Terima kasih!
```

Gambar 3 hasil percobaan

Analisis:

1. Setiap huruf bergeser 13 posisi dalam alfabet.
2. Spasi tidak berubah.
3. Saat hasil enkripsi diproses kembali dengan ROT13, hasilnya kembali ke teks semula.
4. Hal ini menunjukkan algoritma berjalan benar dan konsisten.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan analisis dan implementasi yang telah dilakukan dapat ditarik kesimpulan bahwa algoritma ROT13 adalah cipher substitusi klasik yang merupakan varian spesifik dari Caesar Cipher dengan pergeseran tetap 13 posisi. Karakteristik utama dari algoritma ini adalah sifatnya yang simetris. Karena alfabet Latin memiliki 26 huruf pergeseran 13 langkah (setengah dari total alfabet) menyebabkan proses enkripsi dan dekripsi dapat dilakukan menggunakan fungsi yang identik.

Implementasi algoritma ini telah berhasil dibangun menggunakan bahasa pemrograman Python sesuai dengan tujuan proyek, yaitu tanpa memanfaatkan library kriptografi bawaan. Logika pergeseran ini diterapkan secara manual dengan mengonversi huruf ke nilai numerik ($A=0$), menerapkan rumus matematis ($\text{posisi} + 13 \bmod 26$), dan mengonversinya kembali menjadi huruf.

Hasil pengujian program telah memvalidasi bahwa algoritma bekerja dengan benar dan konsisten. Teks yang dienkripsi (contoh: "HALO" menjadi "UNYB") terbukti dapat dikembalikan ke bentuk *plaintext* aslinya ("HALO") saat diproses kembali menggunakan fungsi ROT13 yang sama. Hal ini membuktikan bahwa ROT13 meskipun tidak dirancang untuk keamanan data yang tinggi, tetapi merupakan alat yang sangat efektif untuk memahami konsep dasar kriptografi terutama prinsip substitusi dan simetri antara enkripsi dan dekripsi.

DAFTAR PUSTAKA

- Angelina M. T. I. Sambi Ua, Diandra Lestriani H, Elizabeth Sonia Kristanty Marpaung, Jesslyn Ong, Michelle Savinka, Putri Nurhaliza, & Rahmi Yulia Ningsih. (2023). Penggunaan Bahasa Pemrograman Python Dalam Analisis Faktor Penyebab Kanker Paru-Paru. *Jurnal Publikasi Teknik Informatika*, 2(2), 88–99. <https://doi.org/10.55606/jupti.v2i2.1742>
- Dewi, S. K. (2024). Perbandingan Cryptography Klasik Vigenere Cipher Dengan Cryptography Modern RC4 Dalam Tingkat Keamanan Jaringan Komputer. *JoMMiT : Jurnal Multi Media Dan IT*, 8(2), 130–137. <https://doi.org/10.46961/jommit.v8i2.1302>
- Dwi Putri, Y., Rosihan, R., & Lutfi, S. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. *JIKO (Jurnal Informatika Dan Komputer)*, 2(2), 87–94. <https://doi.org/10.33387/jiko.v2i2.1319>
- Harahap, A. R., & Salim, T. A. (2018). *Sistem Kriptografi pada Pengamanan Autentikasi Dokumen Elektronik: Systematic Literature Review*. 16(2), 203–220.
- Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsi Pesan Teks. *Journal on Education*, 5(3), 8563–8573. <https://doi.org/10.31004/joe.v5i3.1647>
- Hulu, F. N., & Putri, M. (2022). Metode Analitis Enkripsi Dan Dekripsi Dengan Penerapan Algoritma Kriptografi Klasik Ke Dalam Cipher. *Jurnal Elektro Dan Telkomunikasi*, 26–34.
- Milian, Y. C., & Sulistyo, W. (2023). Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher. *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)*, 7(2), 208–216. <https://doi.org/10.35870/jtik.v7i2.716>
- Munawar, Z., Putri, N. I., Kharisma, I. L., Sid, S. S. K., Insany, P. G., Mogi, I Komang Ari, N., Ma'sum, H., Sastradipraja, C. K., Sukmana, R. N., & Barus, O. P. (2023). *KEAMANAN INFORMASI : Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep* (R. Komalasari (ed.)). Kaizen Media Publishing.
- Rahman, R., Ariantini, M. S., Hadi, A., Hayati, N., Gunawan, P. W., Mandowen, S. A., Widiyasono, N., Gede Arna Jude Saskara, I. K., Salim, B. S., & Thantawi, A. M. (2024).

Buku Ajar Keamanan Jaringan Komputer (E. Efitra & N. Safitri (eds.)). PT. Sonpedia Publishing Indonesia.

Sasono, D., Thir, M., Angel, F., Azizah, M., Utami, L., & Septiana, N. (2023). Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer. *Jurnal Informasi, Sains Dan Teknologi*, 6(1), 72–77.

Sitompul, D. S., Lubis, M. G. R., & Indra, Z. (2024). Implementasi ROT13 sebagai Algoritma Enkripsi Sederhana dalam Python untuk Keamanan Komunikasi Digital. *Journal of Accounting Law Communication and Technology*, 2(1), 41–45. <https://doi.org/10.57235/jalakotek.v2i1.4030>

Wardana. (2019). *Belajar Pemrograman dan Hacking Menggunakan Python* (Wardana (ed.)). Elex Media Komputindo.

LAMPIRAN

```
● ● ●

1 def rot13(teks):
2     hasil = ""
3
4     teks = teks.upper()
5
6     for huruf in teks:
7         if huruf == " ":
8             hasil += " "
9         elif huruf.isalpha():
10            pos = ord(huruf) - ord('A')
11            pos = (pos + 13) % 26
12            hasil += chr(pos + ord('A'))
13
14    return hasil
15
16 # Program utama
17 if __name__ == "__main__":
18     print("== PROGRAM ROT13 ==")
19     print("Ketik exit untuk berhenti.\n")
20
21     riwayat = []
22
23     while True:
24         teks = input("Masukkan teks (exit untuk selesai): ").upper()
25
26         if teks == "EXIT":
27             print("\n== RIWAYAT ENKRIPSI & DEKRIPSI ==")
28             for i, r in enumerate(riwayat, 1):
29                 print(f"{i}. {r['input']} -> {r['encrypt']} -> {r['decrypt']}")
30             print("\nProgram selesai. Terima kasih!")
31             break
32
33         if not all(c.isalpha() or c == " " for c in teks):
34             print("Masukkan Inputan huruf!\n")
35             continue
36
37         hasil_encrypt = rot13(teks)
38         hasil_decrypt = rot13(hasil_encrypt)
39
40         print("Hasil Enkripsi :", hasil_encrypt)
41         print("Hasil Dekripsi :", hasil_decrypt, "\n")
42
43         riwayat.append({
44             "input": teks,
45             "encrypt": hasil_encrypt,
46             "decrypt": hasil_decrypt
47         })
```