**Program Studi Teknik Informatika**

**Sekolah Teknik Elektro dan Informatika**

**Institut Teknologi Bandung**

**=====================================**

**Tugas 4 IF4020 Kriptografi**

**Semester II Tahun 2023/2024**

**Serangan terhadap RSA / RSA Attack**

Deadline : Kamis, 18 April 2024

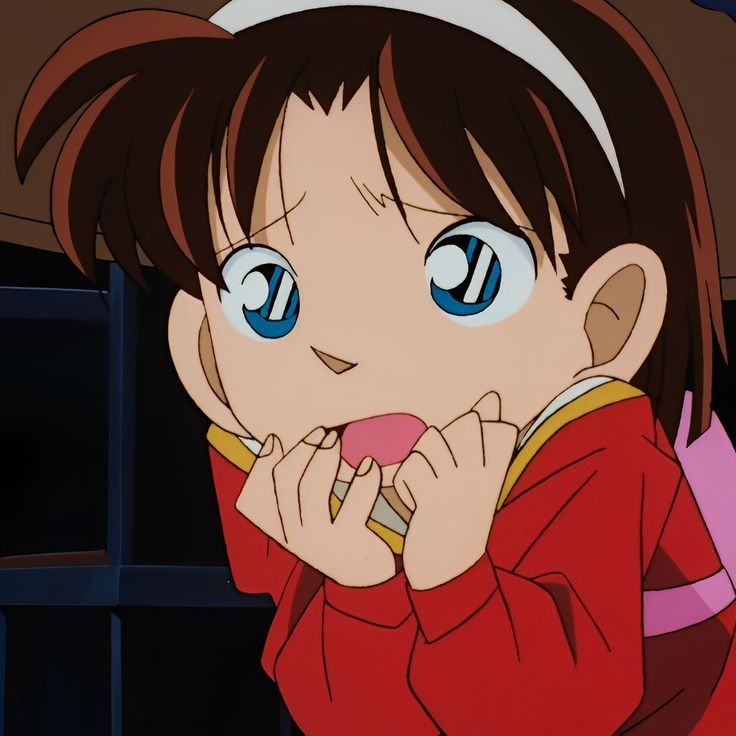
Tempat pengumpulan : <https://forms.gle/uwVu3dsaTbYREkUu9>

Berkas pengumpulan : File format PDF

Anggota kelompok : 2-3 orang

QnA : <https://docs.google.com/spreadsheets/d/1csV5V3yBy5a8KoUETKMduP8B0gwJEff7vt31KtqzbBk/edit?usp=sharing>

## **Bagian A**



Setelah kejadian pada tugas 2 lalu, Conan menyadari bahwa surat percakapan antara dirinya dengan Ai Haibara dapat dipecahkan oleh Ayumi Yoshida. Oleh sebab itu, Conan yang sudah mempelajari kriptografi kunci publik beralih ke algoritma RSA dalam merahasiakan pesan yang hendak dikirim ke Ai Haibara dan juga sebaliknya. Namun selayaknya manusia yang tidak luput akan kesalahan, ternyata Conan lalai dalam mengkonfigurasikan properti-properti dari RSA yang ia gunakan untuk mengenkripsi pesan. Hal ini tentu akan berakibat fatal sebab pesan cipher akan lebih mudah untuk dipecahkan.

Ayumi Yoshida menyadari bahwa Conan sudah tidak lagi menggunakan Hill Cipher. Termakan api cemburu, ia mengerahkan segala upaya untuk mengetahui isi surat yang dipertukarkan antara Conan dan Ai Haibara. Sejauh ini, ia telah berhasil mendapatkan akses ke *channel* yang digunakan Conan dan Ai Haibara dalam bertukar pesan cipher. Lebih lanjut, ia juga telah sukses dalam mendapatkan kode Python yang digunakan untuk mengenkripsi dengan RSA. Berikut adalah kode yang dimaksud:

| from Crypto.Util.number import \*  import random  from sympy import nextprime  flag = "RAHASIA"  tahap = 30  paket\_soal = ["A", "B", "C", "D", "E"]  print(f"Selesaikan {tahap} tahap untuk mendapatkan flag!\n")  print("Kirimkan plainteks dalam bentuk format KRIPTOGRAFIITB{secret}!\n")  print("Tips: buatlah kode untuk otomasi :D\n")  counter = 0  try:  for step in range(tahap):  print(f"---------------- Tahap-{step}----------------\n")  message\_asli = "KRIPTOGRAFIITB{" + str(random.randint(1,10000))+ "}"  message\_asli = message\_asli.encode('utf-8')  message\_int = bytes\_to\_long(message\_asli)  version = random.choice(paket\_soal)  print(f"paket\_soal = {version}\n")  if version == "A":  while True:  ran = random.randint(1, 100)  p = nextprime(getStrongPrime(1024) - ran)  q = nextprime(nextprime(nextprime(nextprime(p) + ran) + ran) - ran)  n = p \* q  e = 65537  check = GCD(e, (p-1)\*(q-1)) == 1  if check: break  enc = pow(message\_int, e, n)  elif version == "B":  p = getStrongPrime(1024)  n = p \* p  e = 65537  enc = pow(message\_int, e, n)  elif version == "C":  while True:  p = getStrongPrime(1024)  q = getStrongPrime(1024)  e = random.randrange(1,65537)  n = p \* q  tot = (p-1) \* (q-1)  e = random.randint(2\*\*15, 2\*\*16)  check = GCD(e, (p-1)\*(q-1)) == 1  if check: break  d = pow(e, -1, tot)  enc = pow(message\_int, d, n)  e = d  elif version == "D":  p = getStrongPrime(1024)  q = getStrongPrime(1024)  n = p\*q  e = 3  enc = pow(message\_int, e, n)  elif version == "E":  n = getStrongPrime(1024)  e = 65537  enc = pow(message\_int, e, n)  print(f"n = {n}\n")  print(f"e = {e}\n")  print(f"c = {enc}\n")  try:  print("Jawaban = ")  input\_dec = input().strip("\n")  if input\_dec == message\_asli.decode():  print("Uwaw keren!!!\n")  counter += 1  else:  print(":((((((\n")  except Exception as e:  print("Error\n")  except Exception as e:  print("Error\n")  finally:  if counter == tahap:  print(f"Uhuyyyy {flag}\n")  else:  print("Tetap semangat dan jangan putus asa!\n") |
| --- |

Tak mau kalah dari Conan dan Ai Haibara, Ayumi Yoshida juga turut mempelajari algoritma RSA. Ia menyadari bahwa RSA yang dipakai Conan lemah apabila ditinjau dari nilai-nilai p, q, e, dan n yang dipakai. Ayumi Yoshida lalu meminta bantuan Anda sebagai ahli IT untuk memecahkan pesan-pesan cipher dari RSA lemah tersebut.

**Tugas Anda adalah**

1. Amati kode yang dipakai Conan di atas. Perhatikan bahwa ada lima kasus (A-E) konfigurasi yang membuat RSA Conan lemah.
2. Untuk setiap kasus, jelaskan secara detail di laporan hal-hal yang membuat RSA untuk kasus tersebut lemah.
3. Untuk setiap kasus, jelaskan secara detail di laporan langkah-langkah serangan yang dapat dilakukan untuk mendapatkan plainteks dari cipherteks jika diketahui nilai n, e, dan c.
4. Buatlah sebuah kode Python untuk melakukan serangan sesuai dengan apa yang Anda jelaskan untuk poin 3.
5. Uji kode yang telah Anda buat dengan cara berikut:
6. Gunakan netcat untuk mengakses nilai n, e, dan c yang tersedia pada

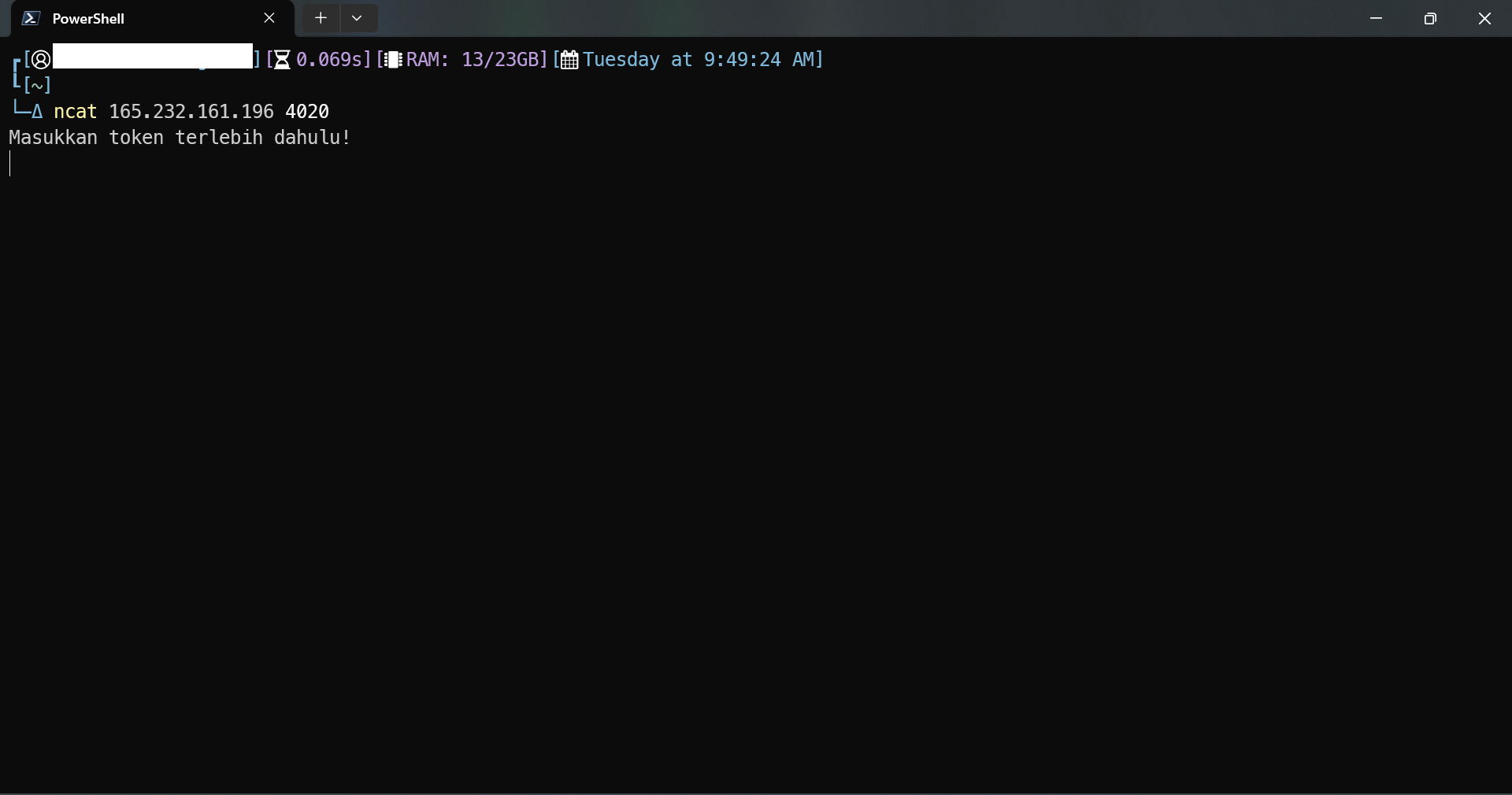
host: **165.232.161.196**

port: **4020**

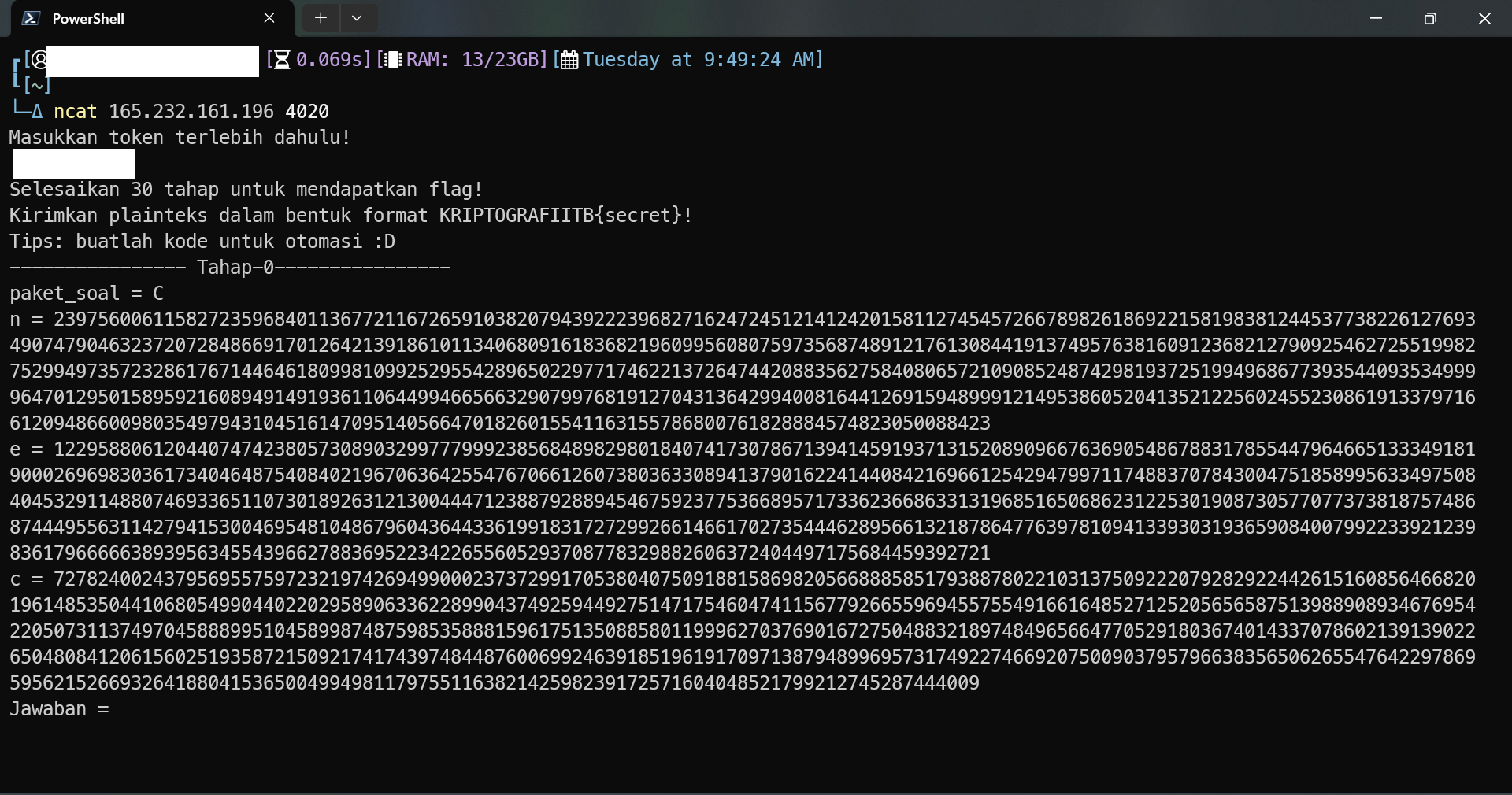
Contoh:

| ## Pada Windows  ncat 165.232.161.196 4020  ## Pada Linux dan Mac  nc 165.232.161.196 4020 |
| --- |

1. Setelah terhubung ke server, Anda akan diminta untuk menginput sebuah token. Silakan masukkan token yang diberikan untuk kelompok Anda. Catatan: Token akan diberikan melalui email setelah deadline pengisian kelompok.



1. Setelah memasukkan token, Anda akan disajikan 30 (tiga puluh / *trente*) kasus uji yang masing-masing memiliki nilai n, e, c, dan versi kasus yang digunakan.



1. Silahkan pecahkan nilai m menggunakan kode yang telah anda buat. Sebelum dimasukkan sebagai jawaban. Ubah m yang Anda dapatkan dari tipe long ke bentuk bytes untuk mendapatkan jawaban dalam format b'KRIPTOGRAFIITB{secret}'. Lalu, Masukkan bagian KRIPTOGRAFIITB{secret} sebagai jawaban.
2. Setelah berhasil menjawab seluruh kasus uji dengan benar, Anda akan menerima sebuah flag dalam format Uhuyyyy KRIPTOGRAFIITB{secret}. Silakan cantumkan flag tersebut ke laporan.
3. Ambil satu contoh test case untuk masing-masing kasus (A-E). Jelaskan pada laporan terkait bagaimana program anda menyelesaikan test case tersebut.
4. **Kode disimpan dalam GitHub dan pranala dicantumkan dalam laporan**

## Bagian B



Kriptografi ITB membuat sebuah arsip digital yang dapat digunakan untuk menyimpan suatu informasi. Pengguna dapat memasukkan nomor arsip yang diinginkan, kemudian nomor arsip tersebut akan dienkripsi menggunakan RSA untuk menghasilkan suatu akses token yang rahasia. Untuk melakukan akses ke suatu arsip, pengguna perlu memasukkan token rahasia, kemudian program akan mendekrip token tersebut dan melakukan akses ke nomor arsip berdasarkan token yang didekrip.

Sonoko melamar kerja di Kriptografi ITB sebagai admin. Dia menyimpan suatu rahasia pada arsip tersebut yang tidak ingin diketahui oleh orang lain. Conan memberi tahu Sonoko bahwa arsip digital pada Kriptografi ITB tersebut tidaklah aman jika orang lain mengetahui nomor arsip dimana Sonoko menyimpan rahasianya. Sonoko kemudian memberikan tantangan kepada Conan untuk membaca isi dari pesan rahasia yang dia simpan pada nomor arsip admin. Bantulah Conan menemukan isi pesan rahasia tersebut! Sebagai hint, Conan diperbolehkan melihat kode arsip digital.

| from Crypto.Util.number import \*  import random  flag = "RAHASIA"  def main():  arsip = {}  p = getStrongPrime(512)  q = getStrongPrime(512)  n = p \* q  tot = (p-1) \* (q-1)  e = random.randint(2\*\*15, 2\*\*16)  while GCD(e, tot) != 1:  e = random.randint(2\*\*15, 2\*\*16)  d = pow(e, -1, tot)  nomor\_arsip\_admin = random.randint(2, 100000000)  while isPrime(nomor\_arsip\_admin):  nomor\_arsip\_admin = random.randint(2, 100000000)  arsip[nomor\_arsip\_admin] = flag  try:  perintah = "0"  while perintah != "4":  print("Selamat datang di arsip dijital Kriptografi ITB!")  print("Ketik angka untuk menjalankan perintah: ")  print("1. Tambah Arsip")  print("2. Baca Arsip")  print("3. Nomor Arsip Admin")  print("4. Keluar")  print("")  print("Masukkan perintah: ", end="")  perintah = input().strip("\n")  if perintah == "1":  print("Masukkan nomor arsip (dalam bentuk integer): ")  nomor\_arsip = input().strip("\n")  if int(nomor\_arsip) == int(nomor\_arsip\_admin):  print("Nomor arsip admin tidak boleh diganti")  continue  print("Masukkan isi arsip: ", end="")  input\_arsip = input().strip("\n")  arsip[int(nomor\_arsip)] = input\_arsip  cipher\_nomor\_arsip = pow(int(nomor\_arsip), e, n)  print(f"Token akses nomor arsip: {cipher\_nomor\_arsip}")  elif perintah == "2":  try:  print("Masukkan token akses nomor arsip (dalam bentuk integer): ", end="")  nomor\_arsip = input().strip("\n")  plain\_nomor\_arsip = pow(int(nomor\_arsip), d, n)  print(f"Isi arsip: {arsip[int(plain\_nomor\_arsip)]}")  except Exception as e:  print("Token akses nomor arsip invalid")  elif perintah == "3":  print(f"Nomor arsip admin: {nomor\_arsip\_admin}")  elif perintah == "4":  exit()  else:  print("Perintah tidak dikenal")  except Exception as e:  print("Terjadi kesalahan")  if \_\_name\_\_ == "\_\_main\_\_":  main() |
| --- |

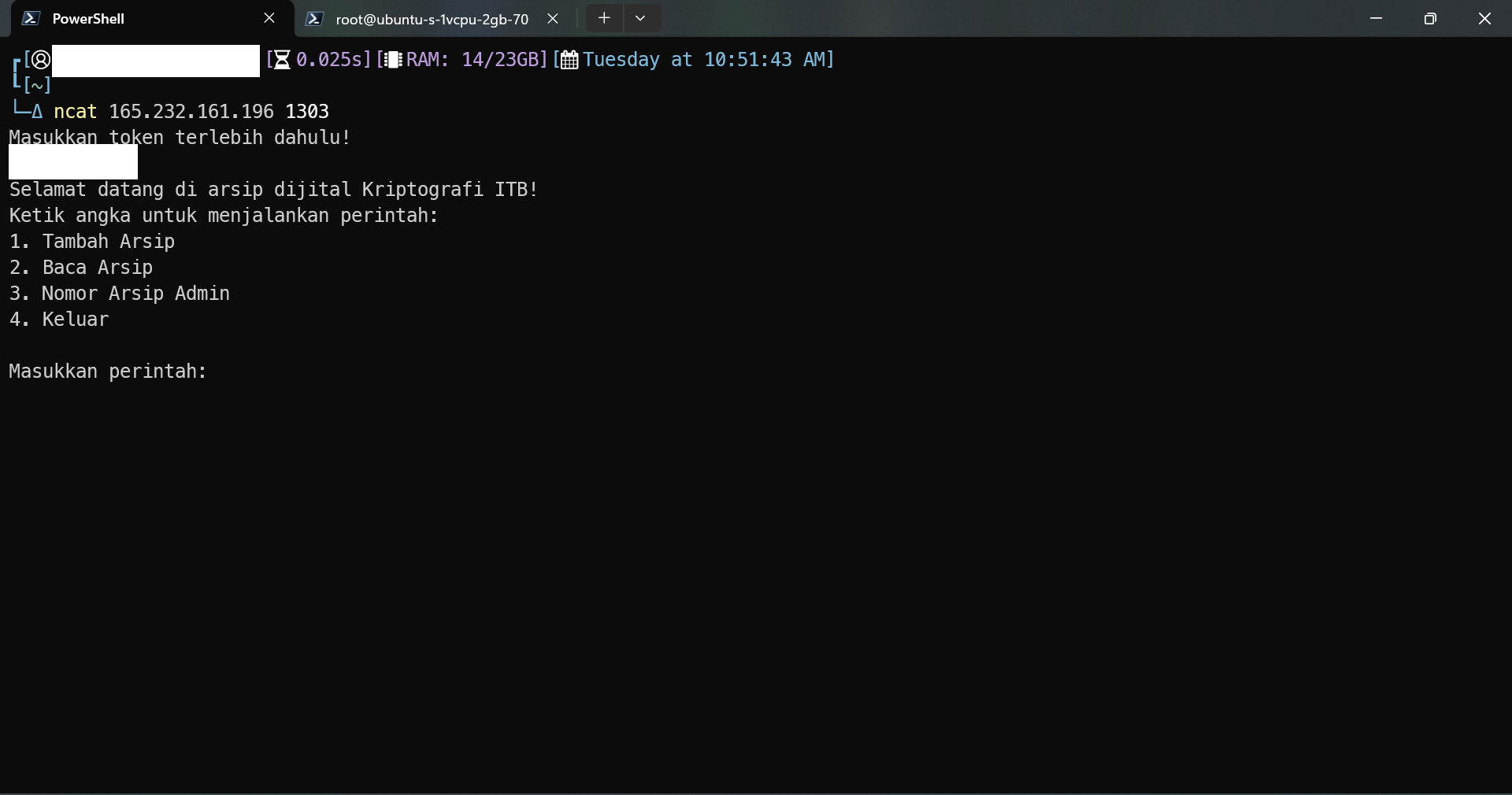
**Tugas Anda adalah**

1. Akses arsip dijital Kriptografi ITB menggunakan netcat ke

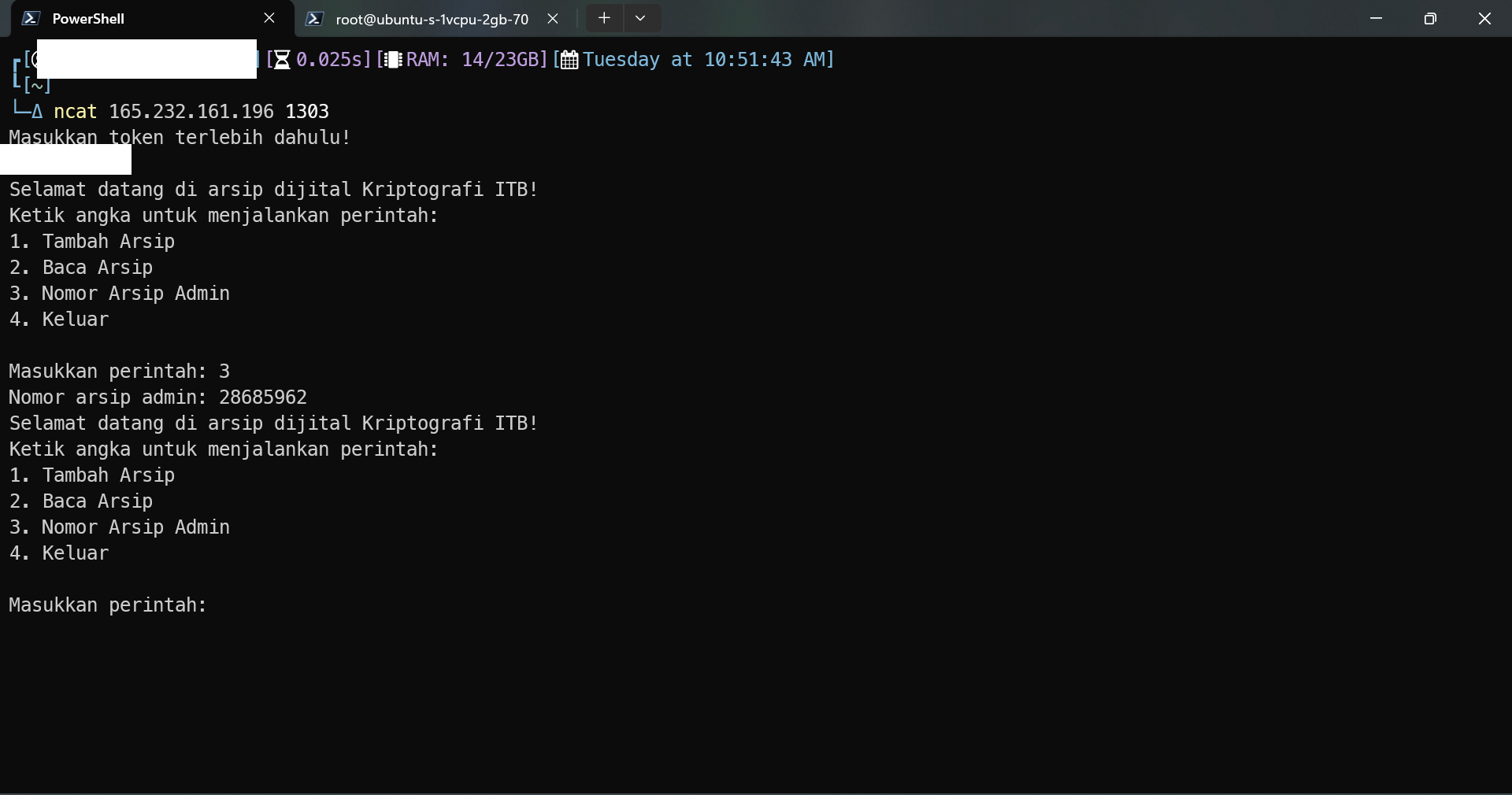
host: **165.232.161.196**

port: **1303**

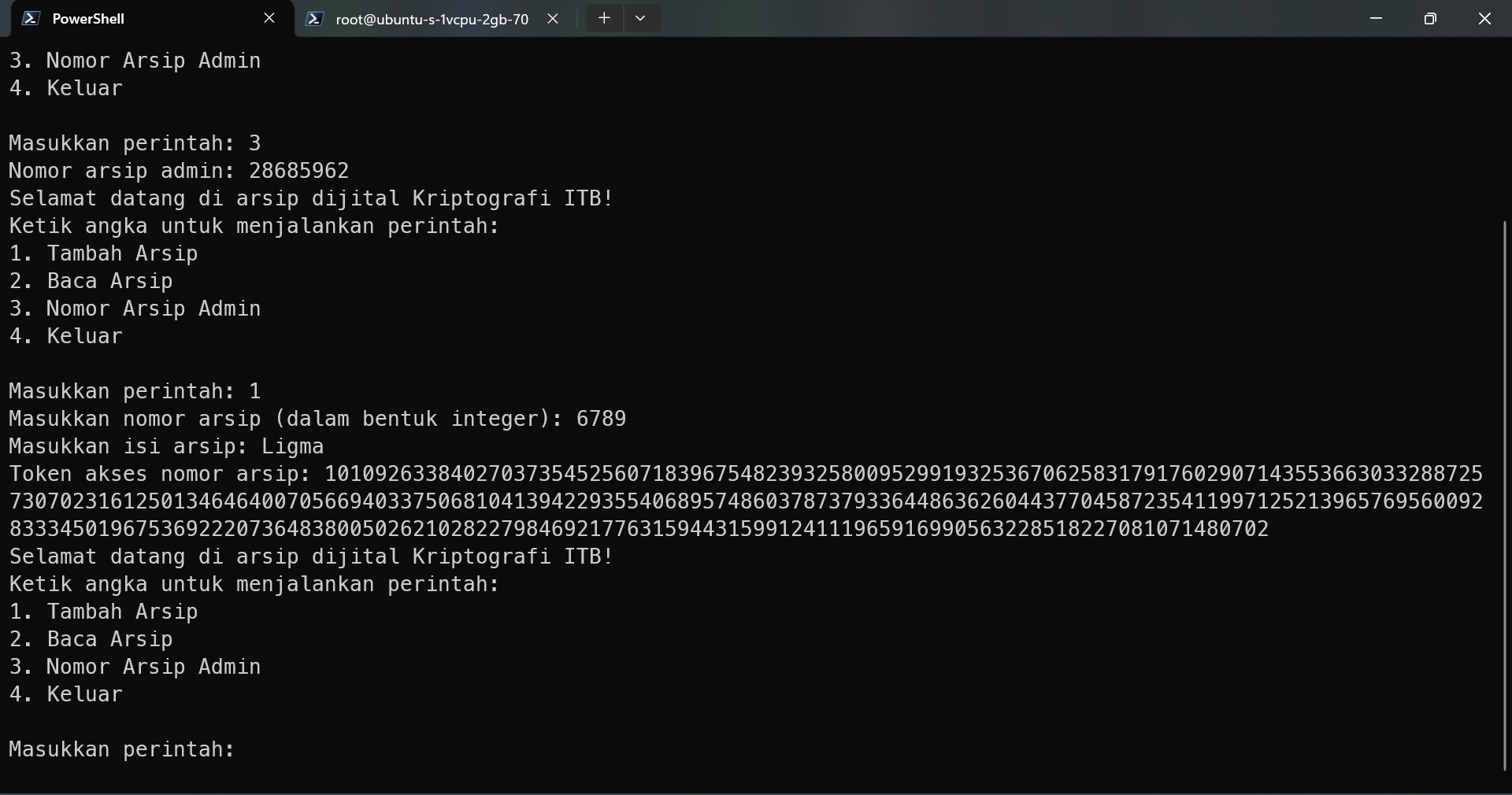
1. Sama seperti sebelumnya, Anda akan diminta untuk memasukkan token terlebih dahulu.
2. Setelah memasukkan token Anda akan disajikan sebuah menu dengan empat pilihan.



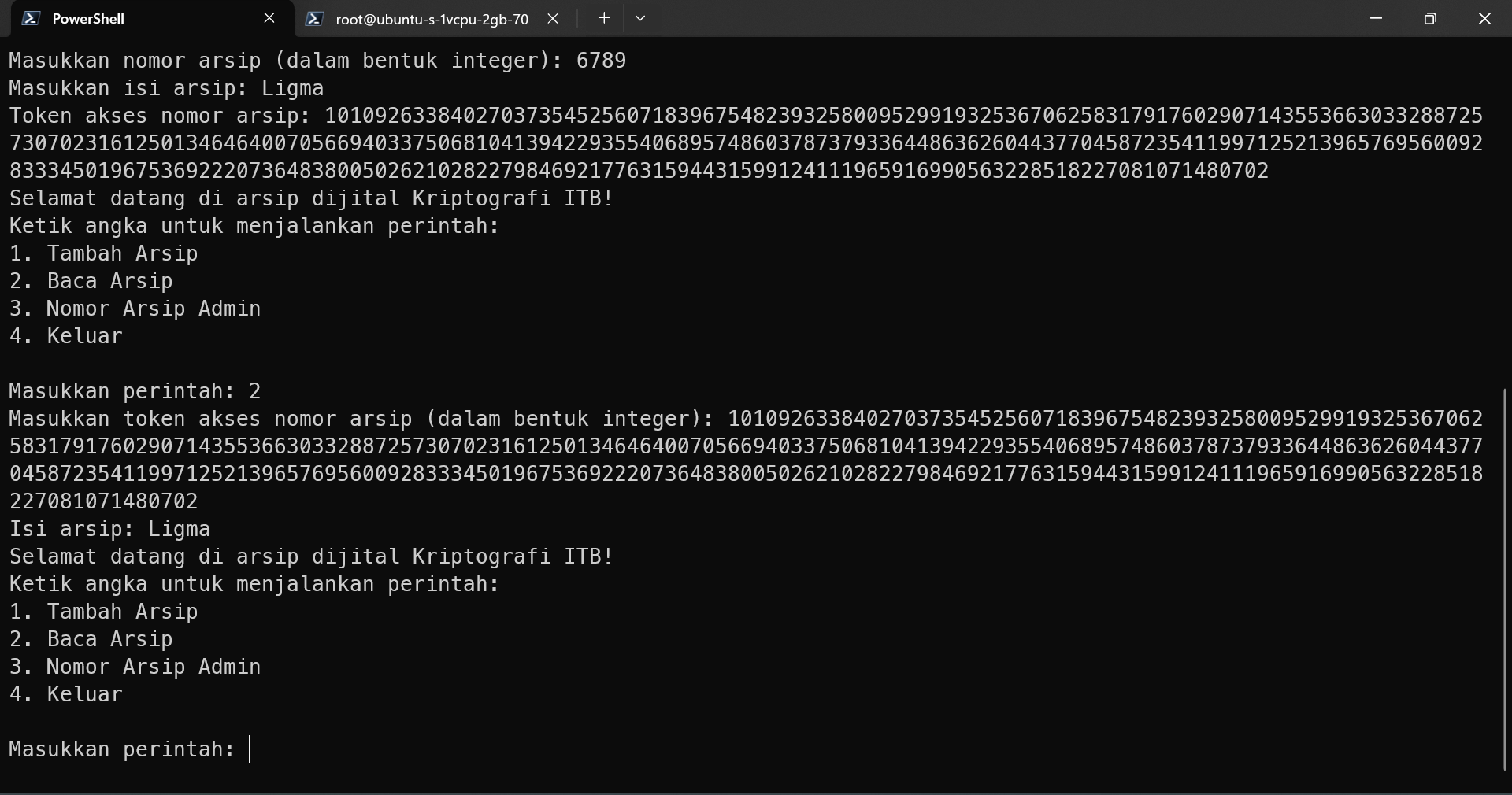
1. Jika memilih “3. Nomor Arsip Admin”, anda akan diberikan sebuah angka yang menunjukkan nomor arsip milik admin.



1. Jika memilih “1. Tambah Arsip”, Anda akan diminta memasukkan nomor untuk arsip Anda beserta isi dari arsip tersebut. Kemudian arsip akan tersimpan dan Anda akan menerima sebuah token akses arsip. Perlu diingat, token akses arsip berasal dari nomor arsip yang dienkripsi menggunakan algoritma RSA. Selain itu, Anda tidak bisa memasukan nomor arsip admin sebagai nomor arsip baru.



1. Jika memilih “2. Baca Arsip”, Anda akan diminta memasukkan token akses arsip untuk membaca isi arsip.



1. Tujuan Anda adalah membaca isi dari arsip milik admin. Untuk itu tulislah secara jelas di laporan Anda:
2. Permasalahan yang ada
3. Dasar Teori Penyelesaian Masalah
4. Langkah-langkah yang Anda lakukan untuk menyelesaikan masalah. Sertakan *screenshot*
5. Isi dari arsip admin.

## Catatan

1. Buatlah sebuah kelompok beranggotakan 2-3 orang. Tulis nama anggota kelompok pada sheets: <https://docs.google.com/spreadsheets/d/1busxpgDMwxme4ZsOTJNqbuBAc4pCe1qb7CckufXIcjA/edit?usp=sharing>

Maksimal pengisian adalah **Kamis, 4 April 2024 sebelum jam kuliah**.

1. Format laporan bebas, pastikan penjelasan Anda logis dan mudah dimengerti.
2. Mohon untuk tidak melakukan hal aneh-aneh kepada server demi kebaikan bersama :D.
3. Anda diperbolehkan memanfaatkan library untuk kode serangan. Tetapi tidak boleh library yang fungsinya adalah mengcrack RSA.
4. Untuk bagian A, disarankan melakukan pengujian secara lokal terlebih dahulu dengan menyesuaikan dan menggunakan kode yang telah diberikan.
5. Kumpulkan laporan dengan format nama Tugas4\_<Nomor Kelompok> disesuaikan dengan nomor di sheets daftar kelompok. Contoh: Tugas4\_Z.pdf

## Referensi

1. <https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf>
2. <https://www.cs.purdue.edu/homes/jblocki/courses/555_Spring17/slides/Lecture31.pdf>
3. <https://www.nku.edu/~christensen/Mathematical%20attack%20on%20RSA.pdf>