Nama : Ikhwan Al Hakim
NIM : 13522147

Laporan Singkat Emulator Mesin Turing untuk Kriptografi RSA

Mesin Turing adalah model teoritis dalam ilmu komputer yang dikembangkan oleh Alan Turing pada tahun 1936. Mesin ini dirancang untuk menggambarkan bagaimana suatu komputer bekerja dalam melakukan perhitungan atau pemrosesan data. Secara umum, Mesin Turing terdiri dari pita yang dapat dianggap tak terbatas panjangnya dan dibagi menjadi sel-sel yang masing-masing dapat menyimpan simbol. Selain itu, mesin ini memiliki head yang dapat bergerak ke kiri atau ke kanan sepanjang pita dan membaca atau menulis simbol pada sel yang sedang dibacanya. Mesin Turing juga memiliki tabel aturan atau program yang menentukan tindakan apa yang harus dilakukan mesin berdasarkan simbol yang sedang dibaca atau keadaan dari mesin tersebut.

Mesin Turing memiliki kemampuan untuk mensimulasikan logika algoritma apa pun, membuatnya menjadi dasar konseptual dari komputer modern. Meskipun sederhana, Mesin Turing dapat digunakan untuk membuktikan sifat dasar komputasi, termasuk konsep kelengkapan Turing yang menyatakan bahwa setiap masalah yang dapat diselesaikan oleh algoritma dapat diselesaikan oleh Mesin Turing. Model ini juga penting dalam teori kompleksitas komputasional, yang mempelajari efisiensi algoritma dan batasan komputasi. Walaupun Mesin Turing adalah abstraksi teoretis, konsep ini membantu para ilmuwan komputer memahami dasar-dasar dari apa yang dapat dan tidak dapat dilakukan oleh komputer.

Suatu Mesin Turing dapat didefinisikan secara formal ke dalam 7 tuple (Q, Σ, Γ, δ, i, B, F) dimana:

- Q adalah himpunan finite state, yaitu keadaan-keadaan yang bisa diraih.
- Σ adalah himpunan input symbol, yaitu simbol-simbol yang hanya bisa digunakan sebagai input.
- Γ adalah himpunan tape symbol, yaitu simbol-simbol yang bisa dituliskan pada pita.
- δ adalah himpunan fungsi transisi, yaitu fungsi yang mengatur perilaku mesin menurut suatu keadaan.
- i adalah start state, yaitu keadaan awal mesin.
- B adalah blank symbol, yaitu simbol yang digunakan untuk menandai lokasi pada pita yang tidak berisi data apapun.
- F adalah himpunan final state, yaitu keadaan akhir dari mesin apabila input diterima.

dan secara umum, cara kerja Mesin Turing adalah sebagai berikut:

1. Mesin mulai dalam state awal (initial state) dan kepala pita berada pada sel pertama yang relevan di pita.
2. Mesin membaca simbol pada sel yang sedang dihadapi oleh kepala pita.
3. Berdasarkan tabel instruksi, mesin menentukan:
    a. Simbol baru yang harus ditulis pada sel tersebut.

    b. Arah gerakan kepala pita (kiri atau kanan).
    c. State baru yang harus dimasuki mesin.
4. Mesin menulis simbol baru pada sel yang sedang dihadapi, menggerakkan kepala pita ke arah yang ditentukan, dan berpindah ke state baru.
5. Langkah 2-4 diulang hingga mesin memasuki state akhir (final state) atau berhenti jika tidak ada instruksi yang berlaku untuk state dan simbol saat ini.

Untuk tugas ini, penulis melakukan pemetaan komponen Mesin Turing yang berbeda antara enkripsi dengan dekripsi. Berikut adalah pemetaan untuk fungsi enkripsi:

- Himpunan Finite State:
    - q0 (state awal): digunakan untuk membaca nilai eksponen publik (e).
    - q1: digunakan untuk membaca nilai eksponen privat (d).
    - q2: digunakan untuk membaca nilai modulus (n).
    - q3: digunakan untuk mengubah semua karakter menjadi nilai ASCII masing-masing.
    - q4: digunakan untuk mengenkripsi nilai ASCII yang telah diubah sebelumnya.
    - q5: keadaan setelah proses enkripsi selesai.
- Himpunan Input Symbol: Semua angka dan karakter.
- Himpunan Tape Symbol: _, $, |, serta semua angka dan karakter.
- Himpunan Fungsi Transisi:
    - (q0, [angka]) = (q0, [angka], R)
    - (q0, _) = (q1, _, R)
    - (q1, [angka]) = (q1, [angka], R)
    - (q1, _) = (q2, _, R)
    - (q2, [angka]) = (q2, [angka], R)
    - (q2, _) = (q3, _, R)
    - (q3, [karakter]) = (q3, [kode ASCII], R)
    - (q3, $) = (q4, $, L)
    - (q4, [kode ASCII]) = (q4, [kode ASCII terenkripsi], L)
    - (q4, _) = (q5, _, L)
- Start State: q0
- Blank Symbol: $
- Final State: q5

dan pemetaan untuk fungsi dekripsi adalah sebagai berikut:

- Himpunan Finite State:
    - q0 (state awal): digunakan untuk membaca nilai eksponen publik (e).
    - q1: digunakan untuk membaca nilai eksponen privat (d).
    - q2: digunakan untuk membaca nilai modulus (n).
    - q3: digunakan untuk mengubah semua ASCII terenkripsi menjadi ASCII asli.
    - q4: digunakan untuk mengubah semua ASCII asli menjadi karakter semula.
    - q5: keadaan setelah proses enkripsi selesai.

- Himpunan Input Symbol: Semua angka dan karakter.
- Himpunan Tape Symbol: _, $, |, serta semua angka dan karakter.
- Himpunan Fungsi Transisi:
    - (q0, [angka]) = (q0, [angka], R)
    - (q0, _) = (q1, _, R)
    - (q1, [angka]) = (q1, [angka], R)
    - (q1, _) = (q2, _, R)
    - (q2, [angka]) = (q2, [angka], R)
    - (q2, _) = (q3, _, R)
    - (q3, [kode ASCII terenkripsi]) = (q3, [kode ASCII], R)
    - (q3, $) = (q4, $, L)
    - (q4, [kode ASCII], L) = (q4, [karakter])
    - (q4, _) = (q5, _, L)
- Start State: q0
- Blank Symbol: $
- Final State: q5

Selain itu, penulis juga membuat format sendiri untuk pita yang dimasukkan kedalam mesin, yaitu sebagai berikut:

(e)_(d)_(n)_(teks)

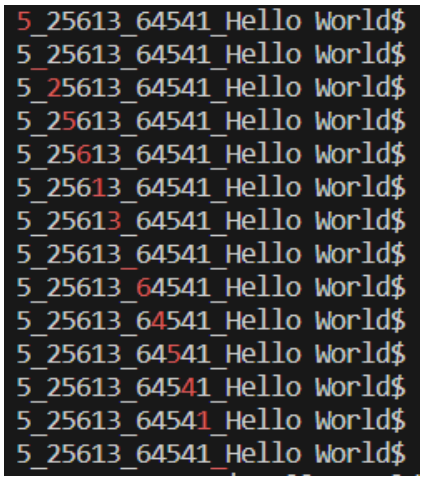
Dimana **e** adalah eksponen publik, **d** adalah eksponen privat, **n** adalah modulus, dan **teks** adalah teks yang ingin dienkripsi atau didekripsi.

Berikutnya penulis akan memberikan contoh step by step enkripsi RSA di Mesin Turing yang telah dibuat. Disini penulis akan menggunakan nilai-nilai berikut:

- Eksponen publik: 5
- Eksponen privat: 25613
- Modulus: 64541
- Teks: Hello World

dan berikut adalah langkah-langkah enkripsinya:

1. Pembacaan variabel



2. Pengubahan karakter menjadi nilai ASCII

```
5_25613_64541_|72ello World$
5_25613_64541_|72|101llo World$
5_25613_64541_|72|101|108lo World$
5_25613_64541_|72|101|108|108o World$
5_25613_64541_|72|101|108|108|111 World$
5_25613_64541_|72|101|108|108|111|32World$
5_25613_64541_|72|101|108|108|111|32|87orld$
5_25613_64541_|72|101|108|108|111|32|87|111rld$
5_25613_64541_|72|101|108|108|111|32|87|111|114ld$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108d$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
```

3. Enkripsi nilai ASCII

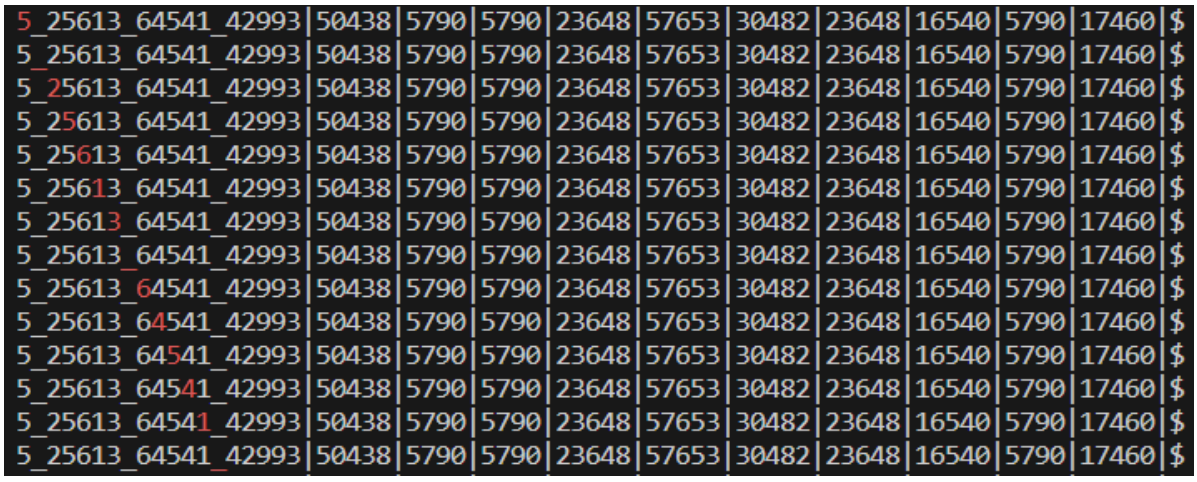
```
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|10817460|$
5_25613_64541_|72|101|108|108|111|32|87|111|114|10817460|$
5_25613_64541_|72|101|108|108|111|32|87|111|114|10817460|$
5_25613_64541_|72|101|108|108|111|32|87|111|114|10817460|$
5_25613_64541_|72|101|108|108|111|32|87|111|1145790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|111|1145790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|111|1145790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|111|1145790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|11116540|5790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|11116540|5790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|11116540|5790|17460|$
5_25613_64541_|72|101|108|108|111|32|87|11116540|5790|17460|$
5_25613_64541_|72|101|108|108|111|32|8723648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|111|32|8723648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|111|32|8723648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|111|3230482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|111|3230482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|111|3230482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|11157653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|11157653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|11157653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|108|11157653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|10823648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|10823648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|10823648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|108|10823648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
```

Terakhir, penulis akan memberikan step by step dekripsi RSA dengan mendekripsi hasil sebelumnya. Berikut adalah nilai-nilai yang digunakan:

- Eksponen publik: 5
- Eksponen privat: 25613
- Modulus: 64541
- Teks: 42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|

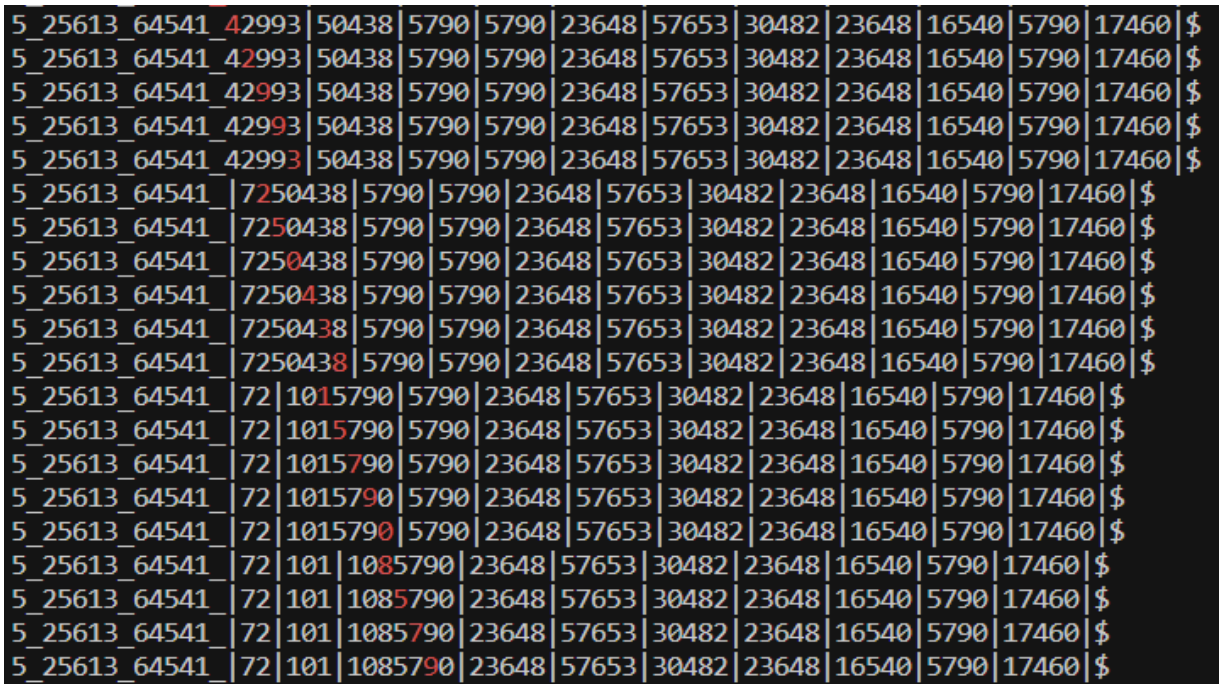
dan berikut adalah langkah-langkah dekripsinya:

1. Pembacaan variabel

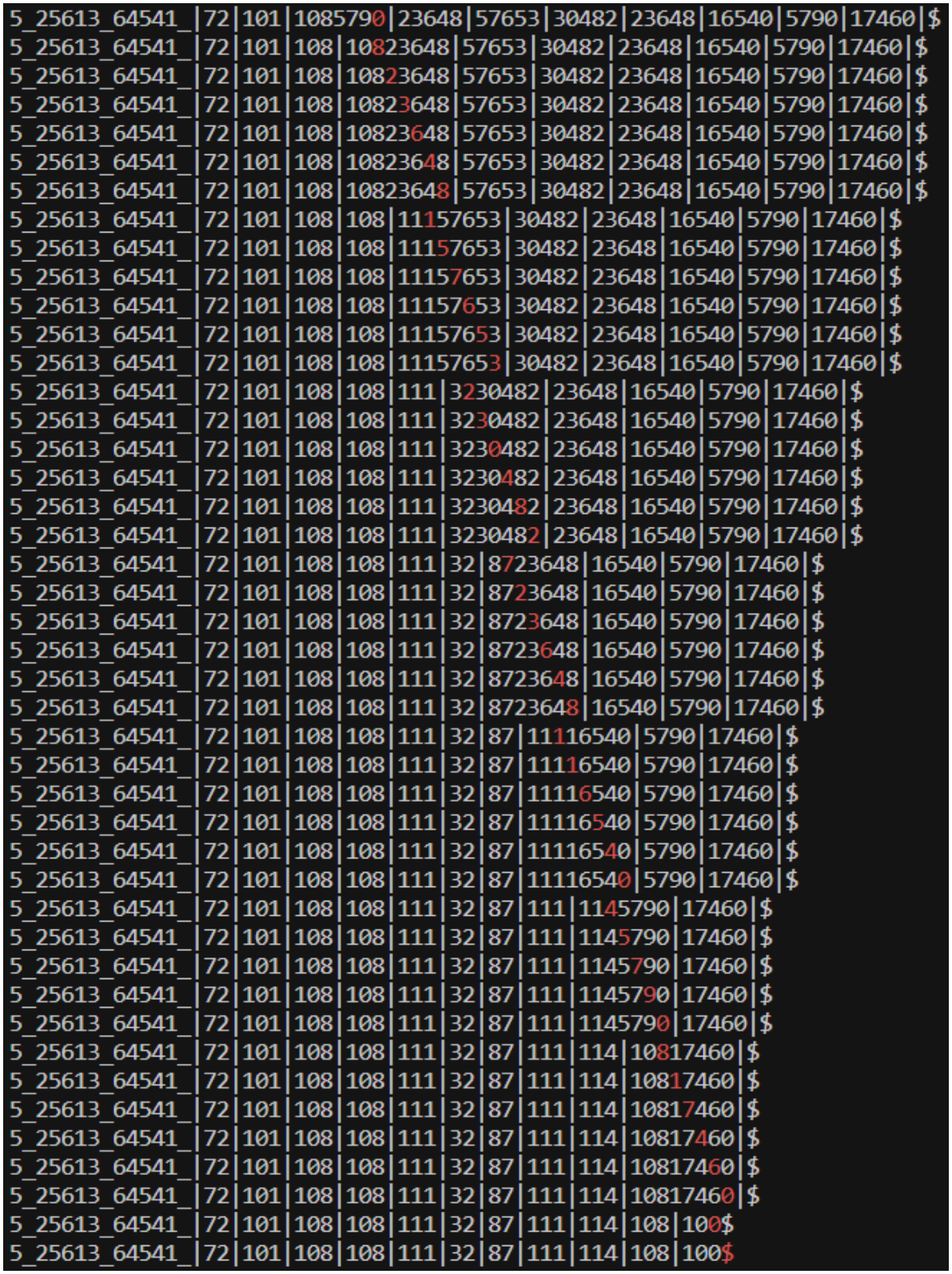


```
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
```

2. Dekripsi nilai ASCII



```
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_42993|50438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|7250438|5790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|1015790|5790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
5_25613_64541_|72|101|1085790|23648|57653|30482|23648|16540|5790|17460|$
```



3. Pengubahan nilai ASCII menjadi karakter

```
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108|100$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108d$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108d$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108d$
5_25613_64541_|72|101|108|108|111|32|87|111|114|108d$
5_25613_64541_|72|101|108|108|111|32|87|111|114ld$
5_25613_64541_|72|101|108|108|111|32|87|111|114ld$
5_25613_64541_|72|101|108|108|111|32|87|111|114ld$
5_25613_64541_|72|101|108|108|111|32|87|111|114ld$
5_25613_64541_|72|101|108|108|111|32|87|111rld$
5_25613_64541_|72|101|108|108|111|32|87|111rld$
5_25613_64541_|72|101|108|108|111|32|87|111rld$
5_25613_64541_|72|101|108|108|111|32|87|111rld$
5_25613_64541_|72|101|108|108|111|32|87orld$
5_25613_64541_|72|101|108|108|111|32|87orld$
5_25613_64541_|72|101|108|108|111|32|87orld$
5_25613_64541_|72|101|108|108|111|32World$
5_25613_64541_|72|101|108|108|111|32World$
5_25613_64541_|72|101|108|108|111|32World$
5_25613_64541_|72|101|108|108|111 World$
5_25613_64541_|72|101|108|108|111 World$
5_25613_64541_|72|101|108|108|111 World$
5_25613_64541_|72|101|108|108|111 World$
5_25613_64541_|72|101|108|108o World$
5_25613_64541_|72|101|108|108o World$
5_25613_64541_|72|101|108|108o World$
5_25613_64541_|72|101|108|108o World$
5_25613_64541_|72|101|108lo World$
5_25613_64541_|72|101|108lo World$
5_25613_64541_|72|101|108lo World$
5_25613_64541_|72|101|108lo World$
5_25613_64541_|72|101llo World$
5_25613_64541_|72|101llo World$
5_25613_64541_|72|101llo World$
5_25613_64541_|72|101llo World$
5_25613_64541_|72ello World$
5_25613_64541_|72ello World$
5_25613_64541_|72ello World$
5_25613_64541_Hello World$
5_25613_64541_Hello World$
```