

LAPORAN TASK IRK
SELEKSI LABORATORIUM ILMU REKAYASA DAN KOMPUTASI

Kriptografi RSA dengan Turing Machine



Disusun oleh:

Marvin Scifo Y. Hutahaeen 13522110

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

2024

DAFTAR ISI

DAFTAR ISI.....	2
BAB I.....	3
BAB II.....	4
BAB III.....	6
BAB IV.....	7
BAB V.....	9
DAFTAR PUSTAKA.....	10
LAMPIRAN.....	10
Link Repository:.....	10

BAB I

Landasan Teori

1.1 Pengertian *Turing Machine*

Mesin Turing adalah robot terbatas yang dapat membaca, menulis, dan menghapus simbol pada pita yang panjangnya tak terhingga. Rekaman itu dibagi menjadi beberapa kotak, dan setiap kotak berisi simbol. Mesin Turing hanya dapat membaca satu simbol dalam satu waktu, dan menggunakan seperangkat aturan (fungsi transisi) untuk menentukan tindakan selanjutnya berdasarkan keadaan saat ini dan simbol yang dibacanya.

Dalam konteks teori automata dan teori komputasi, mesin Turing digunakan untuk mempelajari sifat-sifat algoritma dan untuk menentukan masalah apa yang bisa dan tidak bisa diselesaikan oleh komputer. Mereka menyediakan cara untuk memodelkan perilaku algoritma dan menganalisis kompleksitas komputasinya, yaitu jumlah waktu dan memori yang dibutuhkan untuk memecahkan suatu masalah.

Mesin Turing adalah alat penting untuk mempelajari batasan komputasi dan untuk memahami dasar-dasar ilmu komputer. Mereka memberikan model komputasi yang sederhana namun kuat yang telah banyak digunakan dalam penelitian dan memiliki dampak besar pada pemahaman kita tentang algoritma dan komputasi.

1.2 Kriptografi RSA

RSA adalah salah satu algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi. Panjang kunci dapat diatur, dimana semakin panjang bit pembentukan kunci maka semakin sukar untuk dipecahkan karena sulitnya memfaktorkan dua bilangan yang sangat besar.

RSA ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. Nama RSA sendiri berasal dari nama belakang ketiga penemu dari algoritma ini. RSA mempunyai dua kunci yaitu kunci publik dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya boleh digunakan oleh pihak-pihak tertentu saja dan digunakan untuk proses dekripsi.

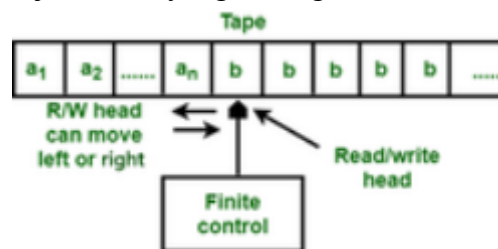
BAB II

Cara Kerja

2.1 Cara Kerja *Turing Machine*

Perilaku mesin Turing ditentukan oleh mesin keadaan berhingga, yang terdiri dari himpunan keadaan berhingga, fungsi transisi yang menentukan tindakan yang akan diambil berdasarkan keadaan saat ini dan simbol yang dibaca, serta himpunan keadaan awal dan penerimaan. Mesin Turing dimulai pada keadaan awal dan melakukan tindakan yang ditentukan oleh fungsi transisi hingga mencapai keadaan menerima atau menolak. Jika mencapai keadaan diterima, komputasi disebut berhasil dan tidak berhasil jika sebaliknya.

Mesin Turing terdiri dari pita dengan panjang tak terhingga yang dapat digunakan untuk melakukan operasi baca dan tulis. Rekaman itu terdiri dari sel-sel tak terbatas di mana setiap sel berisi simbol masukan atau simbol khusus yang disebut kosong. Ini juga terdiri dari penunjuk kepala yang menunjuk ke sel yang sedang dibaca dan dapat bergerak ke dua arah.



Gambar 1: Mesin Turing

Sebuah mesin Turing M dilambangkan dengan notasi formal sbb:

$$M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$$

Q : himpunan berhingga status (a, b, c, \dots atau q_0, q_1, q_2, \dots)

Γ : himpunan berhingga simbol-simbol yang muncul di pita

$B \in \Gamma$: melambangkan melambangkan simbol blank

Σ : himpunan simbol-simbol, subset dari Γ , termasuk di dalamnya B

δ : fungsi pergerakan yang memetakan $Q \times \Gamma \rightarrow Q \times \Gamma \times \{ L, R \}^*$

$q_0 \in Q$: status awal

$F \subseteq Q$: himpunan status akhir

2.2 Cara Kerja Kriptografi RSA

Skema algoritma kunci publik Sandi RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Sebelumnya diberikan terlebih dahulu beberapa konsep perhitungan matematis yang digunakan RSA.

Beginilah Algoritma yang digunakan untuk membuat kunci:

1. Tentukan p dan q bernilai dua bilangan Prima besar, acak dan dirahasiakan dengan $p \neq q$, p dan q memiliki ukuran yang sama.
2. Hitung n dengan mengalikan p dengan q lalu cari juga Toitent N dengan mengalikan $(p-1)$ dengan $(q-1)$.
3. Tentukan e yang merupakan kunci enkripsi dan bilangan prima acak dengan syarat angka tersebut diantara 1 dan Toitent N dan relatif prima dengan Toitent N .

4. Mencari kunci dekripsi dengan menggunakan $d = (1 + \text{ToitentN} * k) / e$ dengan d adalah bilangan bulat
5. Ketika terdapat teks yang ingin dienkripsi. Carilah e, d, n , dan Toitent N . Gunakan rumus $\Rightarrow a^n \pmod n$ dengan a merepresentasikan huruf ke- n yang telah diserialisasikan ke angka untuk dicari modulusnya.
6. Untuk mendekripsi kode tersebut, carilah kunci dekripsi dengan rumus yang disebutkan sebelumnya dan gunakan rumus $b^n \pmod n$ dengan b merepresentasikan angka ke- n yang telah dienkripsi dan siap untuk didekripsi

BAB III

Pemetaan Masalah dan Struktur

3.1 Pemetaan Kriptografi RSA menjadi *Turing Machine*

Dalam pemetaan Kriptografi RSA menjadi Turing Machine, 2 hal akan dilakukan dalam proses enkripsi dan 2 hal juga akan dilakukan dalam proses dekripsi. Dalam enkripsi, *Turing Machine* akan melakukan serialisasi akan string ASCII dengan mengubah setiap karakter menjadi angka dan angka tersebut akan dienkripsi. Dalam setiap huruf dari masukan string ASCII, akan diberikan tanda bahwa huruf tersebut adalah "PlainText". Ini menjadi pengganti tipe state seperti 0, 1, X, Y, dll. Hal ini dilakukan untuk melakukan generalisasi akan jenis-jenis huruf yang akan dimasukkan ke dalam *Turing Machine* karena mereka selalu mempunyai jenis hasil yang sama yaitu hasil enkripsi RSA yang akan diberikan nama "Encrypt". Pada proses enkripsi, *Turing Machine* akan selesai jika semua pita kecuali Blank sudah mempunyai status "Encrypt" dengan pita sebenarnya sudah dienkripsi sesuai rumus yang diberikan. Enkripsi mempunyai 3 state yaitu "PlainText", "Serialized" (Huruf yang sudah diganti menjadi angka), dan "Encrypt" (Angka-angka yang sudah dienkripsi). Sama halnya dengan enkripsi, dekripsi mempunyai 3 state yaitu "Encrypt", "Decrypt" (Angka yang sudah didekripsi), dan "PlainText" (Angka hasil dekripsi yang sudah dijadikan huruf).

3.2 Struktur *Turing Machine*

1. Proses Enkripsi

$$M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$$
$$Q : \{q_0, q_1, q_2\}$$
$$\Gamma : \{\text{PlainText}, \text{Serialized}, \text{Encrypt}, B\}$$
$$\Sigma : \{\text{PlainText}, B\}$$
$$q_0 = q_0$$
$$F = \{q_2\}$$
$$\delta(q_0, \text{PlainText}) = (q_0, \text{Serialized}, R)$$
$$\delta(q_0, B) = (q_1, B, L)$$
$$\delta(q_1, \text{Serialized}) = (q_1, \text{Encrypt}, B)$$
$$\delta(q_1, B) = (q_2, B, R)$$

2. Proses Dekripsi

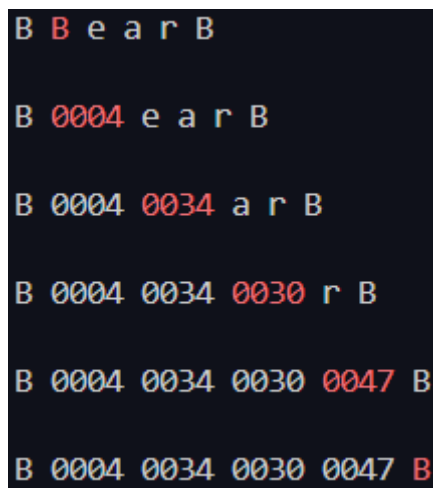
$$M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$$
$$Q : \{q_0, q_1, q_2\}$$
$$\Gamma : \{\text{Encrypt}, \text{Decrypt}, \text{PlainText}, B\}$$
$$\Sigma : \{\text{Encrypt}, \text{Decrypt}, B\}$$
$$q_0 = q_0$$
$$F = \{q_2\}$$
$$\delta(q_0, \text{Encrypt}) = (q_0, \text{Decrypt}, R)$$
$$\delta(q_0, B) = (q_1, B, L)$$
$$\delta(q_1, \text{Decrypt}) = (q_1, \text{PlainText}, B)$$
$$\delta(q_1, B) = (q_2, B, R)$$

BAB IV

Step By Step Enkripsi dan Dekripsi

4.1 Step By Step Enkripsi

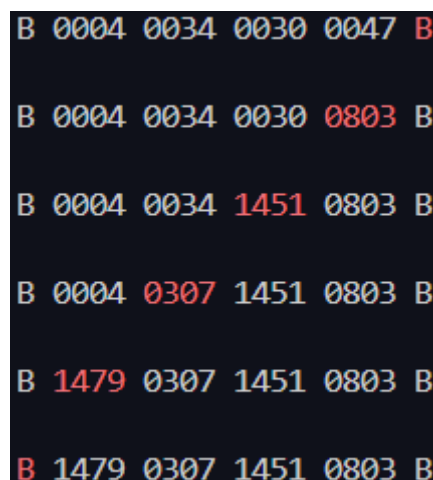
1. Masukkan string ASCII agar string tersebut bisa dienkripsi/dekripsi
2. Tentukan nilai p, q, e, dan d. N dan Toitent N akan didapatkan dengan sendirinya
3. Objek Turing dibuat dan metode encrypt() dipanggil untuk memulai enkripsi.
4. Pada tahap pertama, huruf-huruf ASCII akan diserialisasikan menjadi kode angka sampai mencapai *state* Blank



```
B B e a r B
B 0004 e a r B
B 0004 0034 a r B
B 0004 0034 0030 r B
B 0004 0034 0030 0047 B
B 0004 0034 0030 0047 B
```

Gambar 2: Proses Serialisasi

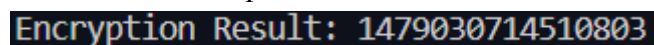
5. Pada tahap selanjutnya, huruf-huruf yang telah diserialisasikan akan menjadi kode enkripsi. Kode enkripsi didapat dengan menggunakan rumus RSA yang telah disebutkan sebelumnya.



```
B 0004 0034 0030 0047 B
B 0004 0034 0030 0803 B
B 0004 0034 1451 0803 B
B 0004 0307 1451 0803 B
B 1479 0307 1451 0803 B
B 1479 0307 1451 0803 B
```

Gambar 3: Proses Enkripsi

6. Hasil akan ditunjukkan setelah enkripsi selesai.



```
Encryption Result: 1479030714510803
```

Gambar 4: Hasil Enkripsi

4.2 Step By Step Dekripsi

1. String yang telah dienkripsi bisa didekripsi dengan menggunakan kunci dekripsi yang didapat dari rumus RSA yaitu $d = (1 + \text{ToitentN} * k) / e$, $d \in \mathbb{N}$, $k \in \mathbb{N}$
2. Objek Turing akan memanggil metode decrypt() untuk melakukan dekripsi
3. Pada tahap pertama, string ASCII yang telah dienkripsi tersebut akan dikonversi menjadi string dekripsi yaitu string yang bentuk serial dari huruf sebenarnya. Rumus yang digunakan adalah mencari modulus n dari perpangkatan antara angka enkripsi dengan d

```
B 1479 0307 1451 0803 B
B 0004 0307 1451 0803 B
B 0004 0034 1451 0803 B
B 0004 0034 0030 0803 B
B 0004 0034 0030 0047 B
B 0004 0034 0030 0047 B
```

Gambar 5: Proses Dekripsi

4. Pada tahap selanjutnya, huruf-huruf yang telah didekripsi akan menjadi huruf biasa. Konversi angka ke huruf sudah ada fungsinya sendiri.

```
B 0004 0034 0030 0047 B
B 0004 0034 0030 0047 B
B 0004 0034 0030 r B
B 0004 0034 a r B
B 0004 e a r B
B B e a r B
B B e a r B
```

Gambar 6: Proses Konversi ke huruf biasa

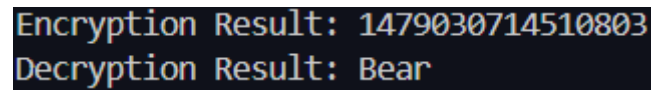
5. Hasilnya akan menjadi seperti ini

```
Decryption Result: Bear
```

Gambar 7: Hasil Dekripsi

4.3 Perbandingan Hasil Enkripsi/Dekripsi

Hasil Enkripsi dan Dekripsi akan diperlihatkan untuk membandingkan kedua string (string berkedok angka jika enkripsi). Hasil yang ditunjukkan adalah seperti ini.

A screenshot of a terminal window with a black background and yellow text. The first line reads "Encryption Result: 1479030714510803" and the second line reads "Decryption Result: Bear".

```
Encryption Result: 1479030714510803
Decryption Result: Bear
```

Gambar 8: Hasil Enkripsi dan Dekripsi

BAB V

Penutup

5.1 Kesimpulan

Turing Machine adalah salah satu jenis automata yang dapat memanipulasi simbol pada pita yang panjangnya beragam. *Turing Machine* dapat digunakan dalam beberapa permasalahan dan salah satunya adalah Kriptografi RSA. Kriptografi RSA adalah jenis kriptografi yang melibatkan 2 kunci yaitu kunci publik (enkripsi) dan kunci privat (dekripsi). Kunci publik adalah sebuah bilangan prima dan kunci privat adalah bilangan yang jika dikalikan dengan e bersisa 1 jika dimoduluskan dengan n yang merupakan hasil perkalian p dan q . Dengan menggunakan *Turing Machine*, satu per satu pita yang merupakan huruf biasa akan dijadikan string serial lalu string enkripsi. Setelah enkripsi, satu per satu pita akan didekripsikan lalu dijadikan huruf biasa sesuai dengan kunci yang dimiliki.

5.2 Saran

Untuk meningkatkan keamanan Kriptografi RSA pastikan angka-angka yang ditentukan adalah angka yang besar sehingga orang-orang yang ingin mendapatkan informasi secara sembarangan perlu mencari kunci dekripsi tersebut dalam waktu yang lama. Semakin besar bilangan e , kemungkinan besar bilangan d yang perlu dicari juga semakin besar dan tidak semua komputer memiliki tenaga yang cukup untuk menghitung angka-angka yang besar.

Selain *Turing Machine*, terdapat metode-metode lain untuk mengimplementasikan Kriptografi RSA seperti dengan memisahkan huruf-huruf ini ke dalam sebuah array untuk diserialisasikan dan dienkripsikan. *Turing Machine* bisa menjadi kakas yang baik untuk menyelesaikan permasalahan ini tetapi terdapat kakas-kakas lain yang bisa digunakan untuk melakukan enkripsi/dekripsi RSA dengan waktu yang lebih cepat.

DAFTAR PUSTAKA

<https://www.geeksforgeeks.org/turing-machine-in-toc/>

<https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/18-Algoritma-RSA-2024.pdf>

[https://informatika.stei.itb.ac.id/~rinaldi.munir/TeoriKomputasi/2014-2015/IF5110%20-%20Mesin%20Turing%20\(Bagian%201\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/TeoriKomputasi/2014-2015/IF5110%20-%20Mesin%20Turing%20(Bagian%201).pdf)

<https://www.neliti.com/publications/68446/penerapan-algoritma-kriptografi-asimetris-rsa-untuk-keamanan-data-di-oracle#:~:text=RSA%20merupakan%20salah%20satu%20algoritma,dua%20bilangan%20yang%20sangat%20besar.>

LAMPIRAN

Link Repository: <https://github.com/scifo04/RSA-Turing-IRK>