## BAB 5 PENGUJIAN DAN ANALISIS

### Hasil Pengujian

Setelah dilakukan keseluruhan tahapan sistem, maka selanjutnya dilakukan pengujian ketahanan enkripsi dengan menggunakan exhaustive attack, yakni menghitung peluang keadaan terburuk peluang memecahkan key dan keadaan terbaik pemecahan key. Tabel testing echaustive attack dapat dilihat pada tabel 3.1

**Tabel 5.1** exhaustive attack

| Panjang Plaintext | Karakter yang mungkin | Total |
|---|---|---|
| 1 | | |
| … | | |
| 16 | | |

### Pengukuran avalanche effect

dilakukan dengan menghitung jumlah yang berbeda pada dua cipher teks yang telah dienkripsi, tabel perhitungan avallance effect terdapat pada tabel 3.2

**Tabel 5.2** Pengujian *Avalanche Effect*

| **Key** | **Bit Berubah** | **Persentase (%)** |
|---|---|---|
| | | |
| | | |
| …. | | |
| | | |
| | | |
| Rata – rata | | |

**Skenario Pengujian**

Pada applikasi kriptografi dengan menggunakan metode rijndael akan dilakukan pengujian untuk mengetahui ketahanan hasil enkripsi rijndael. Penghujian dilakukan dengan dua cara yakni exhaustive attack dan avalanche effect.

Pada exhaustive attack dilakukan perhitungan peluang untuk memecahkan kunci dan perkiraan waktu yang dibutuhkan untuk memecahkan kunci tersebut. Pada avalanche effect dilakukan testing sebanyak tiga kali dengan perbandingan dua data untuk dua kondisi yakni untuk perubahan 1 bit key dan 1 bit plaintext.

### 1.1.1 Data Pengujian

Data yang digunakan pada testing exhaustive attack adalah berdasarkan kemungkinan karakter pada key yang mungkin. Kemudian untuk data pengujian avalanche effect yakni satu plaintext dengan 3 kunci yang berbeda dan 3 plaintext berbeda dengan satu key yang sama, masing-masing plaintext mempunyai panjang 9 karakter.

### 1.1.2 Lingkungan Pengujian

Lingkungan pengujian dalam applikasi kriptografi dengan menggunakan metode rijndael dilakukan dengan melakukan proses exhaustive attack untuk menghitung peluang dan waktu untuk memecahkan key, serta avalanche effect pada masing-masing data testing untuk memperoleh prosestase avalanche effect yang menandakan baik atau buruknya suatu metode kriptografi yakni mendekati angka 50%.

### 1.1.3 Hasil Pengujian

Pengujian yang pertama adalah exhaustive attack, terdapat kemungkinan terburuk dan kemungkinan terbaik. Kemungkinan terburuk adalah apabila key yang digunakan adalah pada batas maksimal kemungkinan yakni 16 karakter, dan kemungkinan terbaik adalah key menggunakan 1 karakter.

Karakter yang mungkin digunakan adalah karakter nomor 32 sampai dengan karakter nomor 126 menurut ASCII tabel pada lampiran 1. Total karakter yang digunakan adalah sebanyak 95, maka kemungkinan kunci yang bias dicoba terdapat pada tabel 4.4.

**Tabel 5.3** Kemungkinan key yang bisa dicoba pada rijndael

| Panjang | Karakter yang mungkin | Total |
|---|---|---|

| Plaintext | | |
|---|---|---|
| 1 | 95 | 95 |
| 2 | 95x95 | $90{,}25 \times 10^{2}$ |
| 3 | 95x95x95 | $85{,}74 \times 10^{4}$ |
| 4 | 95x95x95x95 | $81{,}45 \times 10^{6}$ |
| 5 | 95x95x95x95x95 | $77{,}38 \times 10^{8}$ |
| 6 | 95x95x95x95x95x95 | $73{,}51 \times 10^{10}$ |
| 7 | 95x95x95x95x95x95x95 | $69{,}83 \times 10^{12}$ |
| 8 | 95x95x95x95x95x95x95x95 | $66{,}34 \times 10^{14}$ |
| 9 | 95x95x95x95x95x95x95x95x95 | $63{,}02 \times 10^{16}$ |
| 10 | 95x95x95x95x95x95x95x95x95x95 | $59{,}87 \times 10^{18}$ |
| 11 | 95x95x95x95x95x95x95x95x95x95x95 | $56{,}88 \times 10^{20}$ |
| 12 | 95x95x95x95x95x95x95x95x95x95x95x95 | $54{,}04 \times 10^{22}$ |
| 13 | 95x95x95x95x95x95x95x95x95x95x95x95x95 | $51{,}33 \times 10^{24}$ |
| 14 | 95x95x95x95x95x95x95x95x95x95x95x95x95x95 | $48{,}77 \times 10^{26}$ |
| 15 | 95x95x95x95x95x95x95x95x95x95x95x95x95x95x95 | $46{,}33 \times 10^{28}$ |
| 16 | 95x95x95x95x95x95x95x95x95x95x95x95x95x95x95x95 | $44{,}01 \times 10^{30}$ |

Kunci yang digunakan pada algoritma rijndael ini adalah menggunakan kunci 128 bit, sehingga menurut Tabel 5.3 waktu yang digunakan untuk memecahkan jika lama waktu sebesar $10^{6}$ percobaan perdetik adalah $5.4 \times 10^{24}$ tahun dan apabila lama waktu percobaan sebesar $10^{12}$ percobaan perdetik maka lama yang dibutuhkan adalah $5.4 \times 10^{18}$ tahun.

Pengujian yang kedua adalah avalanche effect. Sekenario pertama adalah dengan menggunakan plaintext yang sama dengan key yang berbeda. Plaintext yang digunakan adalah “septyandi”, hasil pengujian dapat dilihat pada tabel 5.2

**Tabel 5.2** Avalanche effect untuk key yang berbeda

| **Key** | **Bit Berubah** | **Persentase (%)** |
|---|---|---|
| Ilkomers | 68/128 | 53,12 |
| Ilkomert | | |
| Brawijaya | 66/128 | 51,56 |
| Brawijayb | | |
| Kusuma | 74/128 | 57,81 |

| | | |
|---|---|---|
| Lusuma | | |
| Rata – rata | | 54,16 |

Skenario kedua pada avalanche effect adalah dengan menggunakan plaintext yang berbeda. Key yang digunakan adalah "ilkomers", hasil pengujian dapat dilihat pada tabel 5.4.

| Data uji .txt | Bit berubah | Presentase (%) |
|---|---|---|
| 1. Penjadwalan.txt | 64/128 | 63,28 |
| 2. uji.txt | 77/128 | 87.09 |
| 3. ambanglebar.txt | 40/128 | 42.97 |
| Rata-Rata | | 64.47 |

**Tabel 5.4** Avalanche effect untuk plaintext yang berbeda

| **Plaintext** | **Bit Berubah** | **Persentase (%)** |
|---|---|---|
| Septyandi<br>Septyandj | 74/128 | 57,81 |
| Computer<br>Computes | 58/128 | 45,31 |
| Malang<br>Nalang | 72/128 | 56,25 |
| Rata – rata | | 53,12 |

**Tabel 5.5** Avalanche untuk data uji yang berbeda

## 5.2 Analisa Hasil

Dari data hasil pengujian yang dilakukan pada subbab 4.4, maka pada exhaustive attack dalam kondisi terbaik terdapat pada panjang key 1 karakter dengan peluang pemecahan key sebanyak 95 percobaan, sedangkan kondisi terburuk terdapat pada panjang

key 16 karakter dengan peluang pemecahan key sebanyak 44,01 x $10^{30}$percobaan. Waktu yang diperlukan untuk memecahkan kunci rijndael sebesar 128 untukkecepatan sebesar $10^{6}$ percobaan perdetik adalah 5.4 x $10^{24}$ tahun dan apabila kecepatan percobaan sebesar $10^{12}$ percobaan perdetik maka lama yang dibutuhkan adalah 5.4 x $10^{18}$ tahun.

Pada tabel 5.4 hasil testing untuk avalanche effect untuk kondisi menggunakan key yang berbeda diperoleh avalance effect rata-rata sebesar 54,16%, sedangkan pada tabel 4.6 hasil testing untuk avalanche effect untuk kondisi dengan menggunakan *plaintext* yang berbeda didapatkan hasil rata-rata avalanche effect sebesar 53,12%.

Sedangkan pada tabel 5.5 hasil testing untuk avalanche untuk data uji pada file berekstensi .txt dapat rata rata sebesar 64.47% , jadi bisa di simpulkan semakin banyak *plaintext* semakin banyak presentase yang di hasilkan. Ini karena avalanche effect bekerja pada setiap 128 bit di dalam teks yang akan di enkripsi.