BAB V

PENUTUP

5.1 Kesimpulan

Penlitian dan percobaan yang telah dilakukan menghasilkan kesimpulan sebagai berikut:

1. Dari Analisa Hasil P dan Q

   A. Hasil *p* dan *q* yang dibangkitkan berukuran 2 *bit* sampai 17 bit, pembangkitan yang diketahui hanya waktu dalam 1 jam yaitu pada jam 16:51:05GMT+8 sampai dengan 17:46:01 GMT+8.

   B. Hasil proses kombinasi berdasarkan infomasi peranti waktu diuji keberhasilan program dengan *monitoring* pengecualian sehingga menghasilkan tidak ada *feedback* berupa pengecualian di seluruh pemrosesan.

2. Dari Analisa Hasil Entropi Enkripsi, didapat teks 1 = 4.035569614562073, teks 2 = 4.257107430057822, teks 3 = 3.77391380004984 dan teks 4 = 4.421087076196203. Enkripsi dilakukan dengan bantuan RSA (*Rivest Shamir Adleman*) yang proses didalamnya menghadirkan p dan q berdasarkan informasi peranti. Hasil seluruh teks memiliki nilai entropi yang ekuivalen dengan hasil entrop enkripsi rsa yang proses didalamnya (*p* dan *q*) ditentukan default.

5.2 Saran

Adapun saran pada penelitian ini sebagai berikut:

1. Efek *Avalanche*, dapat ditambahkan yang digunakan untuk menilai seberapa signifikan perubahan yang terjadi pada cipherteks karena adanya perubahan kecil, baik pada pesan maupun pada kunci. AE dihitung menggunakan Persamaan 8. AE dikatakan baik jika perubahan bit yang terjadi berkisar antara 45 % hingga 60 % (Sugiyanto & Hapsari, 2017). Semakin banyak bit yang berubah mengindikasikan bahwa algoritme enkripsi tersebut semakin sulit untuk dipecahkan.

$$AE = \frac{Jumlah\ bit\ yangberubah}{Jumlah\ bit\ cipherteks}\ 100\%$$

2. Eksperimen berdasarkan informasi peranti waktu dapat digunakan pada hasil enkripsi untuk modifikasi, dimana *block ciphertext* tertentu diputar atau dipindah berdasarkan nilai informasi peranti dan dikembalikan dengan menyimpan nilai informasi peranti ke dalam memory sementara atau dengan rumus tertentu.
3. Informasi peranti bisa menggunakan informasi selain waktu jam menit dan detik untuk kemudahan lainya tergantung pada peranti yang diterapkan.
4. Gunakan metode lain sebagai bantuan untuk menjadikan hasil p dan q menjadi kunci enkripsi.

DATAR PUSTAKA

Cahyo Dhea Arokhman Yusufi. (2020). *Heuristic - For Mathematical Olympiad Approach*. Math Heuristic. https://books.google.co.id/books?id=OJriDwAAQBAJ&pg=PA18&lpg=PA18&dq=6k+%2B+1+selalu+prima+?&source=bl&ots=aWNDfVbx9w&sig=ACfU3U3JQyCKsvq5_G4JUSbp8WKZhr_7Tw&hl=en&sa=X&ved=2ahUKEwiW9eXuhr_qAhUkheYKHfrHAJ4Q6AEwCnoECAoQAQ#v=snippet&q=prima&f=false

Chiewchanchairat, K., Bumroongsri, P., & Kheawhom, S. (2016). Improving fermat factorization algorithm by dividing modulus into three forms. *KKU Engineering Journal*, *40*(March), 131–138. https://doi.org/10.14456/kkuenj.2015.1

FAQ - Kotlin Programming Language. (n.d.). Diambil 15 Agustus 2020, dari https://kotlinlang.org/docs/reference/faq.html

Ferreira, J. W. P. (2017). The Pattern of Prime Numbers. *Applied Mathematics*, *08*(02), 180–192. https://doi.org/10.4236/am.2017.82015

Firmansyah, F. F. (2015). *Kajian matematis dan penggunaan bilangan prima pada algoritma kriptografi RSA (Rivest, Shamir, dan Adleman) dan algoritma kriptografi Elgamal [skripsi]*.

Harahap, M. K. (2019). *Membangkitkan Bilangan Prima Marsenne dengan metode Bilangan Prima Probabilistik Solovay – Strassen*. *1*(Oktober).

Kumari, J., Singh, S., & Saxena, A. (2015). *An Exception Monitoring Using Java*.

3(2), 12–18.

Meštrović, R. (2018). *Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.--2017) and another new proof*. http://arxiv.org/abs/1202.3670

Muchlis, B. S., Budiman, M. A., & Rachmawati, D. (2017). Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. *SinkrOn*, *2*(2), 49–64. http://jurnal.polgan.ac.id/index.php/sinkron/article/view/75

Nisha, S., & Farik, M. (2017). RSA Public Key Cryptography Algorithm A Review. *International Journal of Scientific & Technology Research*, *06*(07), 187–191.

Prime Numbers - GeeksforGeeks. (n.d.). Diambil 15 Agustus 2020, dari https://www.geeksforgeeks.org/prime-numbers/?ref=lbp

Rihartanto, R., Ningsih, R. K., Gaffar, A. F. O., & Utomo, D. S. B. (2020). Implementation of vigenere cipher 128 and square rotation in securing text messages. *Jurnal Teknologi dan Sistem Komputer*, *8*(3), 201–209. https://doi.org/10.14710/jtsiskom.2020.13476

Sari, R. H. (2017). Apakah Integrasi Islam dapat Membudayakan Literasi Matematika ? *Seminar Matematika dan Pendidikan Matematika UNY*, 655–662.

Sciences, T. (2016). *Dirichlet ' s Theorem Related Prime Gap*. *10*, 305–310.

Serdano, A., Zarlis, M., Sawaluddin, & Hartama, D. (2019). Pengamanan Pesan Menggunakna Algoritma Hill Cipher Dalam Keamanan Komputer. *Jurnal*

Mahajana Informasi, *2*, 1–5.

Sugiyanto, S., & Hapsari, R. K. (2017). Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere. *Jurnal ULTIMATICS*, *8*(2), 131–138. https://doi.org/10.31937/ti.v8i2.528

Sylfania, D. Y., Juniawan, F. P., Laurentinus, L., & Pradana, H. A. (2019). SMS Security Improvement using RSA in Complaints Application on Regional Head Election's Fraud. *Jurnal Teknologi dan Sistem Komputer*, *7*(3), 116–120. https://doi.org/10.14710/jtsiskom.7.3.2019.116-120

TH, A., & MB, B. (2017). The Unique Natural Number Set and Distributed Prime Numbers. *Journal of Applied & Computational Mathematics*, *06*(04). https://doi.org/10.4172/2168-9679.1000368

Wulansari, D., Alamsyah, Setyawan, F. A., & Susanto, H. (2016). Mengukur Kecepatan Enkripsi dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security. *Seminar Nasional Ilmu Komputer (SNIK 2016)*, *Snik*, 85–91.

Zulfikar, M. I., Abdillah, G., Komarudin, A., Informatika, J., & Sains, F. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). *Seminar Nasional Aplikasi Teknologi Informasi (SNATi) 2019*, *2*(1), 19–26.