Jurnal Ilmiah Setrum

Implementasi Algoritma SHA-3 Dan AES Sebagai Sistem Keamanan Pada Proses Pensinyalan *Mobile* IPv6

Supriyanto Praptodiyono[1], Muhammad Akbar Sidiq[1] , Fadil Muhammad[1]

[1]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Sultan Ageng Tirtayasa, Cilegon, Banten.

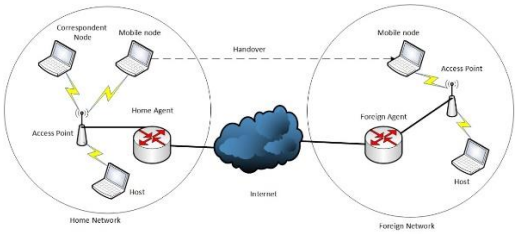
Informasi Artikel

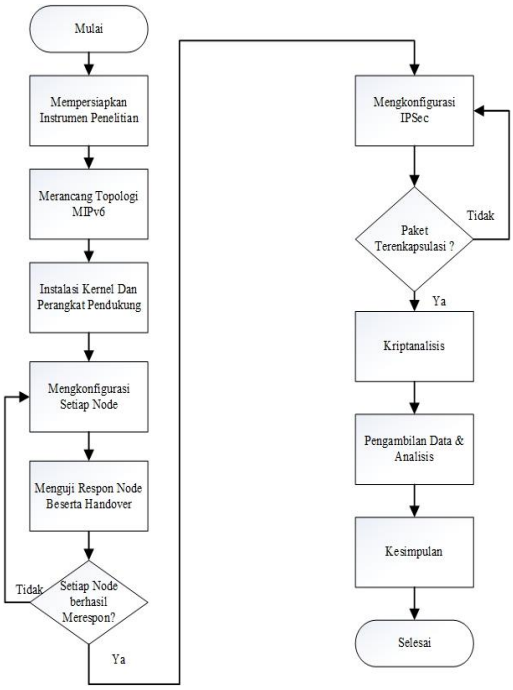
Naskah Diterima : 15 November 2021
Direvisi : 17 November 2021
Disetujui :17 November 2021

doi: 10.36055/setrum.v10i2.13075

***Korespodensi Penulis :**
fadil.muhammad@untirta.ac.id

Graphical abstract





Abstract

Based on statistical data, accessing the internet via mobile devices is one of the most popular where half of the world's web traffic uses a mobile account. Mobile IP technology can be used as a protocol to maintain connectivity even if the device changes connection channels from the network that is connected to the new network. However communication on MIPv6 (Mobile IPv6) is at risk of attack. The method to prevent attacks on the MIPv6 signaling process can use IPsec with the tunnel method using the ESP (Encapsulating Security Payload) protocol that supports encryption and authentication. The 3-DES encryption algorithm and the SHA-1 authentication algorithm are the most commonly used today. The 3-DES and SHA-1 algorithms are considered to have security holes, so an updated algorithm is needed. This study uses AES and SHA-3 as algorithms implemented in IPsec which is an update of 3-DES and SHA-1. Based on the research conducted, SHA-3 did not find any security holes of collision attack. AES also has a higher level of security compared to 3-DES against brute-force attacks with respectively an estimated cracking computation time is 2.7 x 10^25 years and 6.2 x 10^21 years.

Keywords: MIPv6, IPsec, AES, SHA-3, 3-DES, SHA-1

Abstrak

Berdasarkan data statistik, mengakses internet melalui perangkat *mobile* merupakan salah satu yang paling populer dimana setengah dari lalu lintas web di seluruh dunia menggunakan akun *mobile*. Teknologi *Mobile* IP dapat digunakan sebagai protokol untuk dapat menjaga konektifitas walaupun perangkat berpindah saluran koneksi dari jaringan yang terhubung ke jaringan yang baru. Namun komunikasi pada MIPv6 *(Mobile* IPv6) beresiko terhadap serangan. Metode untuk mencegah serangan pada proses pensinyalan MIPv6 dapat menggunakan IPsec dengan metode tunnel menggunakan protokol ESP (*Encapsulating Security Payload*) yang telah mendukung enkripsi dan autentikasi. Algoritma enkripsi 3-DES dan algoritma autentikasi SHA-1 merupakan yang paling umum digunakan hingga saat ini. Algoritma 3-DES dan SHA-1 dianggap telah memiliki celah keamanan sehingga diperlukan suatu algoritma pembaharuan. Penelitian ini menggunakan AES dan SHA-3 sebagai algoritma yang diimplementasikan pada IPsec yang merupakan pembaharuan dari 3-DES dan SHA-1. Berdasarkan penelitan yang dilakukan, SHA-3 tidak ditemukan celah keamanan *collision attack*. AES juga mempunyai tingkat keamanan yang lebih unggul dibandingkan dengan 3-DES terhadap *brute-force attack* dengan masing-masing estimasi waktu komputasi cracking sebesar 2.7 x 10^25 tahun dan 6.2 x 10^21 tahun.

Kata Kunci: MIPv6, IPsec, AES, SHA-3, 3-DES, SHA-1

1. PENDAHULUAN

Pengguna internet memiliki perkembangan yang cukup pesat dalam beberapa tahun terakhir. Statistik dunia internet [1] menunjukkan bahwa pertumbuhan pengguna internet dari tahun 2000 sampai

akhir tahun 2020 mencapai 1,300 %. Jumlah pengguna internet pada bulan Desember 2020 diestimasikan mencapai 5,053,911,722 pengguna dari jumlah seluruh penduduk dunia yang diestimasikan berjumlah 7,875,765,584 orang. Jumlah pengguna internet tersebut adalah sekitar 64.2 % dari populasi dunia. Pesatnya pertumbuhan pengguna internet selama beberapa tahun tersebut menyebabkan masalah terkait ketersediaan masalah alamat IP (*Internet Protocol*) [2]. Standar alamat IP yang sebelumnya adalah IPv4 (*Internet Protocol Version* 4) dikembangkan lagi oleh IETF (*Internet Engineering Task Force*) untuk menyelesaikan masalah terkait ketesediaan alamat IP dengan menambahkan beberapa fitur baru, standar tersebut kemudian diberi nama IPv6 (*Internet Protocol Version* 6) [3].

Terdapat beberapa cara agar seseorang dapat mengakses internet, yaitu melalui perangkat desktop atau melalui perangkat *mobile*. Mengakses internet melalui perangkat *mobile* merupakan salah satu yang paling populer digunakan dalam beberapa tahun terakhir. Berdasarkan data statistik [4], sekitar setengah dari lalu lintas web di seluruh dunia menggunakan akun *mobile*. Perangkat *mobile* menyumbang sekitar 51,53 % lalu lintas web secara global pada kuartal kedua di tahun 2020, data tersebut belum termasuk penggunaan tablet. Riset yang dilakukan oleh perusahaan internet bernama SimilarWeb juga menunjukkan bahwa lalu lintas web yang berasal dari perangkat *mobile* meningkat 30,6 % sejak tahun 2017 hingga 2019 [5]. Lalu lintas web dari perangkat desktop justru mengalami penurunan sekitar 3,3 % untuk periode yang sama. Adapun alasan dari meningkatnya penggunaan perangkat *mobile* adalah karena mempunyai sifat yang fleksibel yaitu dapat mengakses internet dimana saja dan kapan saja [6]. Perangkat *mobile* ketika berpindah konektifitas dari satu titik ke titik yang lain dapat kehilangan koneksi untuk sementara waktu sehingga tidak dapat mengirim atau menerima paket [7]. Oleh karena itu, *mobile* IP digunakan sebagai protokol untuk dapat menjaga konektifitas walaupun berpindah saluran koneksi dari jaringan yang terhubung ke jaringan yang baru.

Komunikasi pada jaringan nirkabel termasuk pada MIPv6 (*Mobile* IPv6) beresiko terhadap serangan. Metode untuk mencegah serangan pada proses pensinyalan MIPv6 dapat menggunakan IPsec dengan metode *tunnel* menggunakan protokol ESP (*Encapsulating Security Payload*) yang telah mendukung enkripsi dan autentikasi [8]. IPSec menerapkan teknik kriptografi untuk menjamin keamanan dalam komunikasi melalui jaringan komputer. Adapun pengkajian tentang bagaimana memecahkan mekanisme pada kriptografi disebut dengan kriptanalisis [9]. Salah satu serangan yang dapat dilakukan pada kriptanalisis adalah *bruce force attack* yang digunakan untuk memecahkan cipher dengan menggunakan semua kunci yang mungkin hingga menemukan satu kunci yang benar [10]. Kriptanalisis pada algoritma autentikasi umumnya dilakukan dengan mencoba menemukan dua buah pesan dengan masukan berbeda namun memiliki nilai *hash* yang sama, hal tersebut disebut dengan *collision attack*. Terdapat beberapa metode enkripsi dan autentikasi yang dapat digunakan dimana 3-DES (*Triple Data Encryption Standard*) dan SHA-1 (*Secure Hash Algoritm* 1) merupakan yang paling umum digunakan hingga saat ini [9][10]. Algoritma 3-DES dan SHA-1 dianggap telah memiliki celah keamanan sehingga NIST mengeluarkan algoritma pembaharuan berupa AES (*Advanced Encryption Standard*) dan SHA-3 (*Secure Hash Algoritm* 3).

Beberapa penelitian terkait implementasi algoritma AES dan SHA-3 pada jaringan MIPv6 telah dilakukan diantaranya adalah pada [11]. Namun, penelitian pada [11] hanya membahas bagaimana performa jaringan MIPv6 ketika menggunakan metode enkripsi AES dan tidak dilakukan pengujian terhadap serangan untuk mengetahui tingkat keamanan sistem yang telah dibuat. Penelitian yang dilakukan pada [12] telah dilakukan pengujian untuk mengetahui keamanan pada jaringan MIPv6. Namun, penelitian [12] hanya membahas bagaimana pengaruh SHA-3 sebagai algoritma autentikasi dan tidak dilakukan penelitian terkait algoritma enkripsi yang digunakan. Oleh karena itu, penelitian ini menggabungkan metode autentikasi dan enkripsi dengan mengimplementasikan algoritma SHA-3 dan AES untuk mengetahui keefektifisannya terhadap keamanan jaringan MIPv6.

2. METODE PENELITIAN

2.1 Metode Penelitian

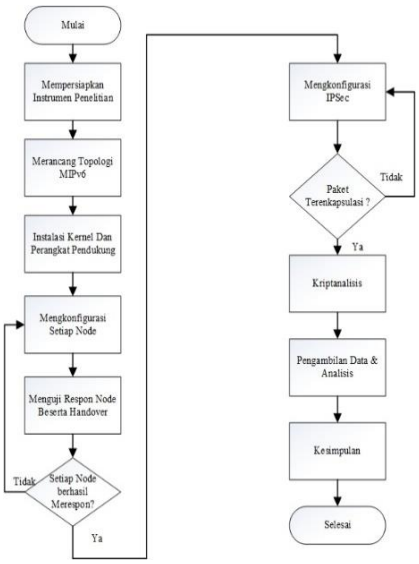
Proses penelitian terbagi menjadi beberapa tahap yang dilakukan berdasarkan urutan dalam melakukan penelitian:

a) Identifikasi masalah yaitu dengan merumuskan latar belakang hingga tujuan dalam penelitian ini.

b) Studi literatur, yaitu mengumpulkan data-data dari buku referensi dan jurnal-jurnal sesuai dengan topik penelitian yang dilakukan yaitu tentang MIPv6, IPSec, kriptografi dan algoritma yang akan digunakan
c) Perancangan dan pengujian, yaitu dengan merancang jaringan MIPv6 serta melakukan pengujian ping antar node dan proses handover. Selain itu dilakukan juga pengujian *brute-force attack* untuk algoritma enkripsi dan pengujian *collision attack* untuk algoritma autentikasi yang digunakan.

2.2 Diagram Alir Penelitian

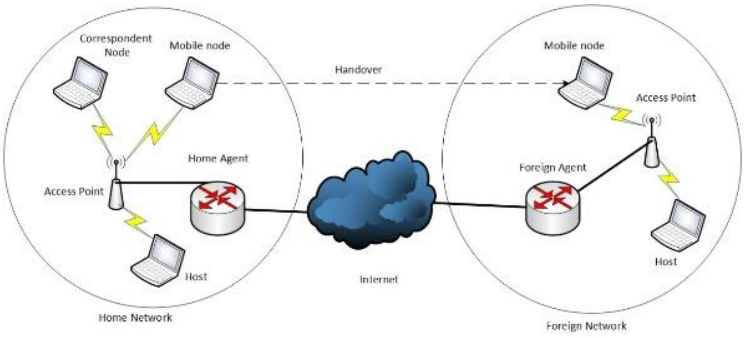
Secara sederhana proses penelitian terkait implementasi algoritma SHA-3 dan AES sebagai sistem keamanan pada proses pensinyalan mobile IPv6 dapat dijelaskan melalui diagram alir pada Gambar 1.



Gambar 1. Diagram Alir Penelitian

2.3 Perancangan Penelitian

Perancangan jaringan MIPv6 pada penelitian menggunakan beberapa perangkat PC, *access point* dan beberapa perangkat pendukung lainnya sebagai *node* untuk membangun topologi yang akan dibuat. Bentuk dari topologi jaringan *mobile* IPv6 adalah pada penelitian ini adalah seperti pada Gambar 2.



Gambar 2. Topologi Jaringan MIPv6

Gambar 2 menunjukkan bahwa topologi jaringan MIPv6 yang dibangun pada penelitian ini menggunakan dua jaringan yang berbeda yaitu *home network* dan *foreign network. Home network* pada topologi jaringan yang dibangun terdapat beberapa komponen didalamnya yaitu 1 buah *home agent*, 1 buah *access point*, 1 buah *correspondent node*, 1 perangkat *host* lain, dan 1 buah *mobile node* yang

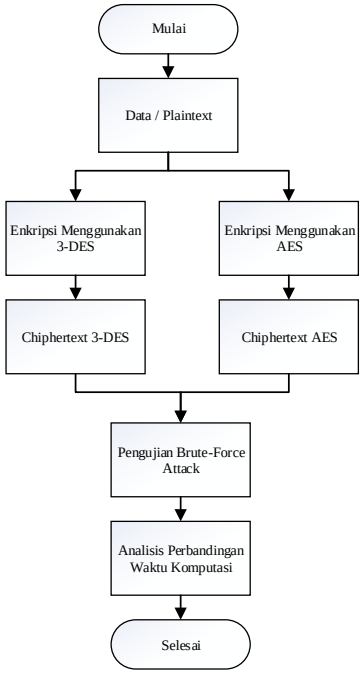
mana *mobile node* tersebut akan melakukan mobilitas atau *handover* kedalam *foreign network*. Komponen yang terdapat pada *foreign network* adalah 1 buah *home agent*, 1 buah *access point*, dan 1 perangkat *host* lain. Kedua jaringan tersebut terhubung dalam *subnetting* dan konfigurasi MIPv6.

Setiap *node* yang telah dirancang sedemikian rupa menjadi sebuah topologi jaringan kemudian dikonfigurasi pada masing-masing *node* tersebut agar dapat saling terhubung dan berkomunikasi berdasarkan prinsip MIPv6. Selain itu dilakukan konfigurasi IPSec untuk mengamankan pesan pada proses pensinyalan MIPv6. IPsec yang telah dikonfigurasi selanjutnya dilakukan pengecekan terhadap pesan BU dan BA yang telah berhasil terkirim apakah sudah berhasil terenkapsulasi oleh IPsec. Pengecekan dapat dilakukan melalui tampilan *interface* wireshark bahwa pesan BU dan BU telah teridentifikasi sebagai ESP.

Pengujian yang dilakukan selanjutnya adalah mengukur tingkat keamanan algoritma yang digunakan. AES dan SHA-3 yang diimplementasikan pada penelitian ini dibandingkan dengan algoritma sebelumnya yaitu 3-DES dan SHA-1. Pengujian tingkat keamanan algoritma dijelaskan pada subbab berikut.

2.3.1 Pengujian *Brute-Force Attack*

Brute-Force merupakan suatu metode yang digunakan untuk memecahkan *chiphertex*t. *Brute-force* dapat dikatakan sebagai usaha untuk mendekripsi suatu teks yang telah terenkripsi sebelumya dengan mencoba semua kemungkinan kunci yang ada. Pengujian *brute-force attack* pada penelitian ini dilakukan untuk mengetahui seberapa lama waktu komputasi yang dibutuhkan untuk mendekripsikan suatu pesan yang telah terenkripsi. Pengujian *brute-force attack* pada penelitian ini adalah seperti pada Gambar 3.

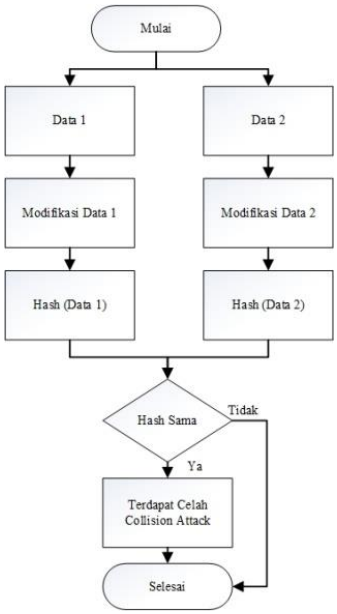


Gambar 3 Pengujian *Brute-Force Attack*

Gambar 3. memperlihatkan pengujian *brute-force attac*k yang dilakukan pada penelitian ini. Pengujian dilakukan dengan membandingkan waktu komputasi antara dua algoritma yaitu 3-DES dan AES. Pengujian dilakukan menggunaan bantuan perangkat lunak cryptool.

2.3.2 Pengujian *Collision-Attack*

Collision Attack merupakan celah keamanan yang terdapat pada suatu fungsi *hash* dimana dengan masukan data yang berbeda akan menghasilkan *hash* yang sama. Data dengan masukan yang berbeda idealnya akan menghasilkan nilai *hash* yang juga berbeda. Pengujian *collision attac*k pada penelitian ini adalah seperti pada Gambar 4.



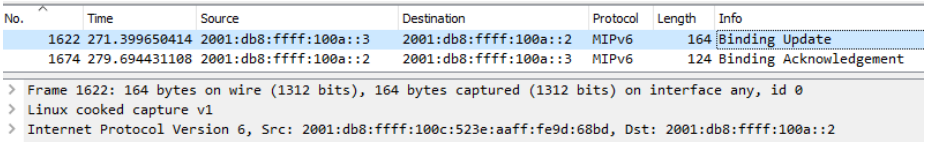
Gambar 1 Pengujian *Collision Attack*

Gambar 4 memperlihatkan bahwa pengujian dilakukan dengan mempersiapkan dua buah data dengan masukan yang berbeda. Duah buah data tersebut kemudian dimodifikasi menggunakan sha1-collider. *Output* dari kedua data tersebut kemudian di *hash function* menggunakan SHA-1 dan SHA-3. Kedua data apabila mempunyai nilai *hash* yang sama maka dapat dikatakan mempunyai celah keamanan *collision attack*.

3. HASIL DAN PEMBAHASAN

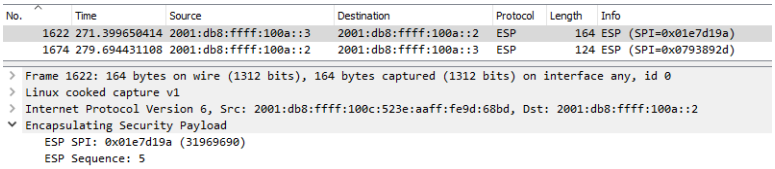
3.1 Implementasi SHA-3 Dan AES Pada Pensinyalan MIPv6

Proses pensinyalan MIPv6 yang dilakukan pada penelitian ini telah diimplementasikan oleh IPSec dengan AES sebagai algoritma enkripsi dan SHA-3 sebagai algoritma autentikasinya. Proses pensinyalan pada penelitian ini menggunakan pesan BU (*binding update*) dan pesan BA (*binding acknowledgment*). MN ketika melakukan proses *handover* kedalam *foreign link* maka akan mendapatkan CoA. MN perlu memberitahukan CoA tersebut kepada HA melalui pesan BU agar komunikasi yang berasal dari maupun ke MN dapat diatur. HA kemudian melakukan pesan balasan berupa BA untuk mengkonfirmasi bahwa HA telah menerima pesan BU dari MN. Pensinyalan MIPv6 sebelum dan sesudah diimplementasikan IPSec akan terlihat perbedaannya seperti pada Gambar berikut.



Gambar 5 Pensinyalan Sebelum Implementasi IPSec

Gambar 5 memperlihatkan tampilan trafik jaringan yang sedang digunakan melalui perangkat lunak wireshark. Tampilan wireshark memperlihatkan beberapa kolom informasi mengenai rafik yang berhasil ditangkap. Kolom tersebut antara lain memuat informasi yang beberapa diantaranya adalah IP *address* dari perangkat *source* dan *destination*, serta jenis protokol yang sedang digunakan. Gambar 5 menunjukkan bahwa IPSec belum diimplementasikan, protokol yang terbaca pada tampilan wireshark adalah MIPv6. Protokol tersebut akan berubah menjadi ESP ketika IPSec telah diimplementasikan seperti pada gambar 6 berikut.



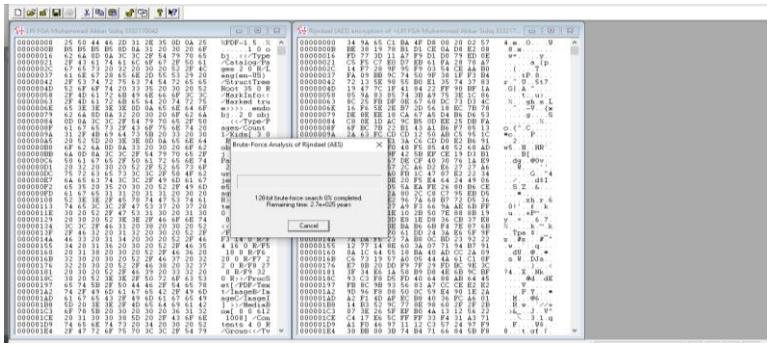
Gambar 6 Pensinyalan Setelah Implementasi IPSec

Gambar 6 menunjukkan bahwa proses pensinyalan telah berhasil terenkapsulasi oleh IPSec dimana protokol yang digunakan adalah ESP. Informasi yang terdapat pada pesan pensinyalan tidak dapat diketahui karena telah terenkapsulasi oleh ESP header.

3.2 Pengujian Brute-Force Attack

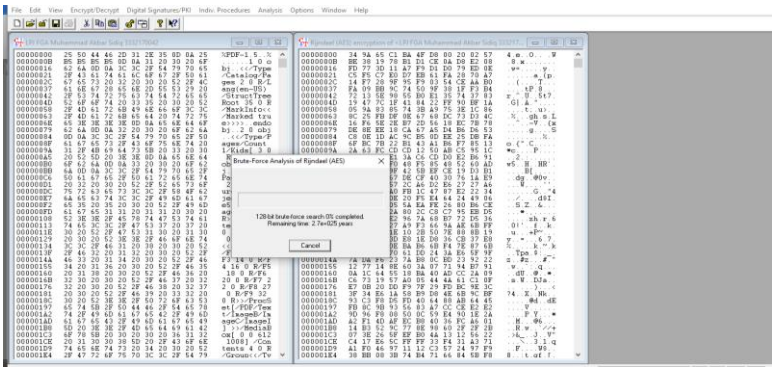
Penetrasi serangan yang dapat dilakukan pada kriptanalisis sangat beragam. Salah satu serangan yang dapat dilakukan pada kriptanalisis adalah *bruce force attack*. Penetrasi serangan pada *brute-force attack* bertujuan untuk memecahkan *cipher* dengan menggunakan semua kunci yang mungkin hingga menemukan satu kunci yang benar. Misalkan terdapat algoritma enkripsi dengan kunci yang digunakan sebesar 128 bit, maka akan dicoba semua kunci yang mungkin yaitu sebanyak 2^{128} kali hingga mendapatkan kunci yang tepat.

Pengujian *brute-force attack* pada penelitian ini menggunakan bantuan aplikasi *cryptool.* Proses kriptanalisis menggunakan penetrasi serangan *brute force* pada penelitian ini adalah dengan membandingkan dua algoritma enkripsi yang berbeda yaitu AES dan 3-DES. Pengujian dengan serangan *brute-force* dilakukan terhadap file berekstensi .pdf yang telah disiapkan sebelumnya dengan ukuran file sebesar 492 kb. File tersebut dienkripsi terlebih dahulu menggunakan algoritma AES dan 3-DES. Langkah selanjutnya adalah melakukan pengujian serangan *brute-force* pada algoritma AES seperti pada gambar 7 berikut.



Gambar 7 Proses Komputasi Untuk *Cracking* AES.

Gambar 7 memperlihatkan proses komputasi untuk melakukan *cracking* pada berkas yang telah dienkripsi algoritma AES. Penyerang diasumsikan tidak mengetahui keseluruhan nilai kunci yang digunakan. Gambar 7 menunjukkan bahwa untuk melakukan *cracking* pad aberkas yang telah dienkripsi algoritma AES diperlukan waktu komputasi dengan estimasi 2.7e+025 *years* atau sekitar 2.7 x 10^25 tahun. Percobaan berikutnya yaitu melakukan serangan *brute-force* dengan algoritma yang berbeda. Algoritma yang dipilih yaitu 3-DES yang merupakan algoritma pendahulu dari AES, selain itu 3-DES merupakan salah satu algoritma yang paling banyak digunakan hingga saat ini. Gambar 8 berikut merupakan proses komputasi untuk *cracking* berkas yang telah dienkrpsi oleh algoritma 3-DES



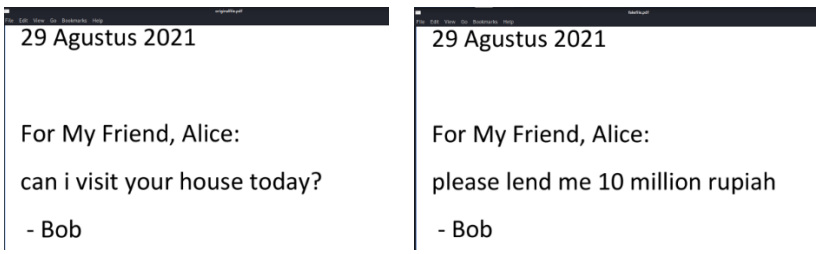
Gambar 8 Proses Komputasi Untuk *Cracking* 3-DES.

Pengujian serangan *brute-force* pada 3-DES dilakukan terhadap file yang sama seperti pada pengujian AES. Penyerang juga diasumsikan tidak mengetahui keseluruhan nilai kunci yang digunakan. Gambar 8 menunjukkan bahwa untuk melakukan *cracking* berkas yang telah dienkripsi oleh 3-DES diperlukan waktu komputasi dengan estimasi 6.2e+021 *years* atau sekitar 6.2 x 10^21 tahun. Data tersebut menunjukkan bahwa untuk meng-*crack* file yang telah dienkripsi oleh AES membutuhkan waktu yang lebih lama dibandingkan dengan file yang di enkripsi oleh 3-DES. Hal tersebut menunjukkan bahwa keamanan enkripsi pada AES lebih kuat dibandingkan dengan 3-DES. Berdasarkan kedua data yang diperoleh, kemampuan komputasi yang ada saat ini dapat dikatakan mustahil untuk dapat meng-*crack* keamanan pada algoritma AES maupun 3-DES. Namun, jika penyerang dapat mengetahui beberapa celah bit kunci maka keamanan pada 3-DES lebih rentan untuk di tembus kerana memiliki waktu komputasi yang lebih sedikit daripada AES.

3.3 Pengujian *Collision Attack*

Collision attack merupakan celah keamanan yang dapat terjadi pada *hash function*. Fungsi *hash* atau *hash function* idealnya akan menghasilkan *hash* yang berbeda ketika di-*input*-kan data yang berbeda. Namun dalam beberapa kasus fungsi *hash*, ketika data yang di-*input*-kan berbeda akan menghasilkan *hash* yang sama. Kondisi yang demikian dapat dikatakan bahwa fungsi *hash* memiliki celah keamanan *collision attack*. Percobaan penetrasi *collision attack* pada penelitian ini menggunakan bantuan *software* sha1-collider. Perangkat lunak tersebut merupakan *tool* berbasis python yang berfungsi untuk memodifikasi data yang nantinya digunakan untuk menguji celah keamanan *collision attack* pada fungsi *hash*. Adapun fungsi *hash* yang digunakan pada penelitian ini adalah SHA-1 dan SHA-3.

Langkah pertama yang harus dipersiapkan dalam pengujian ini adalah menyiapkan dua buah data dengan isi yang berbeda. Data yang digunakan adalah dua file berekstensi .pdf untuk memudahkan pengujian yang dilakukan. Adapun kedua file tersebut adalah seperti pada Gambar berikut ini.

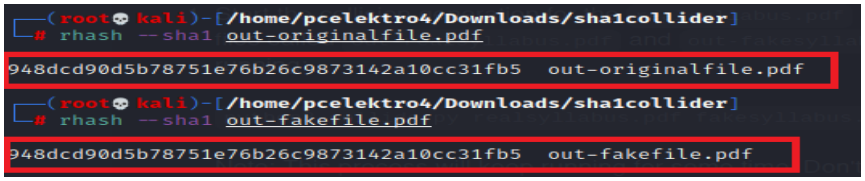


(a) (b)

Gambar 9 File Pengujian *Collision attack*

Gambar 9 menunjukkan file yang digunakan untuk melakukan pengujian *collision attack*. File tersebut memperlihatkan dua pesan dengan isi yang berbeda. File (a) diberi nama originalfile.pdf sedangkan file (b) diberi nama fakefile.pdf. File tersebut kemudian dimodifikasi menggunakan sha1-collider. Kedua file yang telah dimodifikasi mengalami perubahan nama menjadi out-originalfile.pdf untuk file (a) dan out-fakefile.pdf untuk file (b). File yang telah dimodifikasi

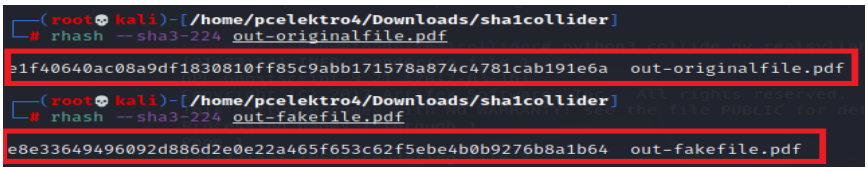
kemudian dilihat nilai *hash* nya menggunakan *hash function* yang berbeda yaitu SHA-1 dan SHA-3. Hal tersebut dilakukan untuk mengetahui apakah *hash function* tersebut mempunyai celah keamanan berupa *collision attack*. Berikut ini merupakan nilai *hash* dari kedua file menggunakan algoritma SHA-1 yang telah dimodifikasi.



Gambar 10 Nilai *Hash* File Menggunakan SHA-1

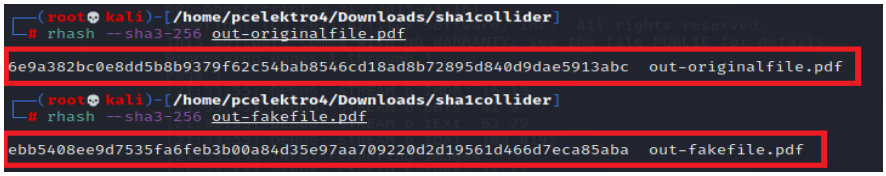
Gambar 10 memperlihatkan nilai *hash* dari kedua file ketika di *hash function* menggunakan SHA-1 dengan panjang *hash* yang dihasilkan sebesar 160-bit. Gambar 10 menunjukkan bahwa setelah proses modifikasi melaui sha1-collider, file antara out-originalfile.pdf dengan out-fakefile.pdf mempunyai nilai *hash* yang sama. Hal tersebut menunjukkan bahwa pada SHA-1 terdapat celah keamanan *collision attack*. Dua file yang mempunyai masukan berbeda idealnya akan mempunyai nilai *hash* yang juga berbeda. Namun dalam pengujian yang telah dilakukan pada penelitian ini, kedua file tersebut mempunyai nilai *hash* yang sama.

Percobaan selanjutnya adalah dengan mendapatkan nilai *hash* dari kedua file menggunakan SHA-3 dengan variasi bit yang digunakan adalah 224-bit, 256-bit, 384-bit, dan 512-bit. Adapun nilai *hash* yang diperoleh dari kedua file menggunakan SHA-3 yang telah dimodifikasi adalah seperti gambar berikut.

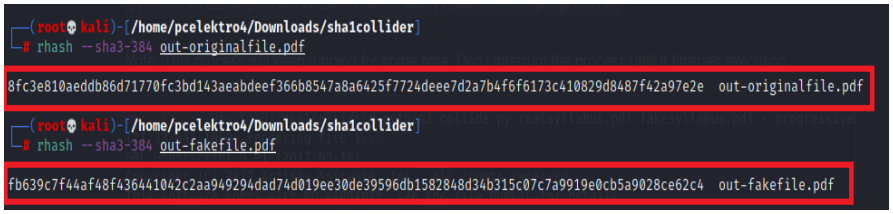


Gambar 11 Nilai *Hash* File Menggunakan SHA3-224

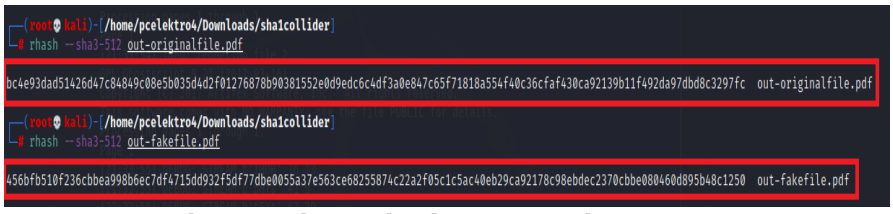
4



Gambar 12 Nilai *Hash* File Menggunakan SHA3-256



Gambar 13 Nilai *Hash* File Menggunakan SHA3-384



Gambar 14 Nilai *Hash* File Menggunakan SHA3-512

Gambar 11 sampai Gambar 14 memperlihatkan nilai *hash* dari kedua file ketika di *hash function* menggunakan SHA-3. Variasi panjang *hash* yang dihasilkan adalah sebesar 224-bit pada Gambar 11, 256-bit pada Gambar 12, 384-bit pada Gambar 13, dan 512-bit pada Gambar 14. Gambar 11 sampai Gambar 14 menunjukkan bahwa setelah di *hash function* menggunakan SHA-3, file antara out-originalfile.pdf dengan out-fakefile.pdf mempunyai nilai *hash* yang berbeda. Hal tersebut menunjukkan bahwa berdasarkan penelitian yang telah dilakukan, SHA-3 tidak memiliki celah keamanan *collision attack* berapapun variasi bit yang dimilikinya. Semaikin besar nilai variasi bit yang dimiliki maka semakin panjang juga nilai *hash* yang dihasilkan. Percobaan yang telah dilakukan pada penelitian ini menunjukkan bahwa SHA-3 memiliki tingkat keamanan yang lebih baik dibandingkan dengan SHA-1.

4. KESIMPULAN

4.1 Kesimpulan

Berdasarkan pengujian yang telah dilakukan pada penelitian ini, dapat diperoleh beberapa kesimpulan sebagai berikut.

a) IPsec dapat digunakan untuk mengamankan pesan pensinyalan pada jaringan MIPv6
b) AES mempunyai tingkat keamanan yang lebih tinggi terhadap *brute force attack* dibandingkan dengan 3-DES.
c) SHA-3 tidak memiliki celah keamanan *collision attack* sedangkan celah keamanan *collision attack* ditemukan pada SHA-1.
d) AES dan SHA-3 merupakan algoritma yang lebih baik dibandingkan 3-DES dan SHA-1 berdasarkan tingkat keamanannya.

4.2 Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dilakukan pada penelitian selanjutnya. Pengamanan jaringan MIPv6 melalui implementasi IPSec dapat menggunakan algoritma enkripsi dan autentikasi yang lain. Selain itu, pengujian ketahanan dan kehandalan pada algoritma yang digunakan dapat menggunakan penetrasi serangan yang berbeda dari yang telah dilakukan dalam penelitian ini.

REFERENSI

[1] Miniwatts Marketing Group, "World Internet Usage And Population Statistics," *Internet World Stats*, 2020. https://www.internetworldstats.com/stats.htm

[2] S. Praptodiyono, R. K. Murugesan, I. H. Hasbullah, C. Y. Wey, M. M. Kadhum, and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration," in *Proceedings of the 2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology, ICACOMIT 2015*, 2016, pp. 31–36. doi: 10.1109/ICACOMIT.2015.7440150.

[3] S. Deering and H. R., "RFC8200: Internet Protocol, Version 6 (IPv6) Specification," 2017.

[4] J. Clement, "Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 3rd quarter 2020," *Statista.com*, 2020. https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/

[5] SimilarWeb. LTD, "2020 State of Digital Report," 2020. [Online]. Available: https://www.similarweb.com/corp/reports/2020-digital-trends-lp/

[6] S. Busanelli, M. Martal, G. Ferrari, G. Spigoni, and N. Iotti, "Vertical Handover between WiFi and UMTS Networks : Experimental Performance Analysis," *IJEIC*, vol. 2, no. 1, pp. 75–96, 2011, [Online]. Available: http://www.sersc.org/journals/IJEIC/vol2_Is1/7.pdf

[7] S. Praptodiyono, T. Firmansyah, M. Alaydrus, M. I. Santoso, A. Osman, and R. Abdullah, "Mobile IPv6 Vertical Handover Specifications, Threats, and Mitigation Methods: A Survey," *Security and Communication Networks*, vol. 2020. 2020. doi: 10.1155/2020/5429630.

[8] A. Alhofiki, "Analisis Handover Pada Heterogeneous Network Menggunakan Objek Bergerak Dengan Parameter Handover Trigger," 2017.

[9] W. Y. Azhar, S. Supriyadi, and Y. Yanitasari, "Kriptanalisis Hill Cipher Terhadap Known Plaintext Attack Menggunakan Metode Determinan Matriks Berbasis Android," *Simetris : Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, vol. 8, no. 2, 2017, doi: 10.24176/simet.v8i2.1535.

[10] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 1, no. 1, 2016, doi: 10.30743/infotekjar.v1i1.48.

[11] D. Barita, "Peningkatan Kinerja Sistem Keamanan Pada Proses Pensinyalan Dalam Vertical Handover Mipv6," 2019.

[12] R. Aprilia, "Analisis Performansi Keccak Message Authentication Code Sebagai Metode Autentikasi Pesan Pensinyalan Mobile Ipv6," 2019.