SATIN – Sains dan Teknologi Informasi
Journal Homepage : http://jurnal.sar.ac.id/index.php/satin

Penerapan Algoritma Hybrid RSA Terhadap Pembangkit Kunci Diffie Hellman untuk Sistem Keamanan

Romindo[1], Ferawaty[2]
[1]Politeknik Ganesha Medan, romindo4@gmail.com, Jl. Manunggal No.194, Helvetia, Kec. Sunggal, Deli Serdang, Indonesia
[2]Universitas Pelita Harapan, Ferawaty.fik@uph.edu, Lippo Plaza Medan, Lantai 5 - 7, Jl. Imam Bonjol No.6, Medan, Indonesia

Informasi Makalah

Submit : November 13, 2021
Revisi : November 29, 2021
Diterima : Desember 16, 2021

Kata Kunci :

Algoritma RSA
Diffie Hellman
Sistem Keamanan
Teknologi
Sistem Informasi

Abstrak

Dalam dunia kriptografi, kunci untuk mengenkripsi dan mendekripsi pesan rahasia adalah salah satu yang paling penting. Kunci tersebut menentukan apakah ciphertext dapat dibaca atau tidak. Rahasia kunci sebenarnya adalah sesuatu yang mungkin lebih esensial dan penting daripada rahasia ciphertext itu sendiri, dalam arti pesan ciphertext bisa dibocorkan tapi kuncinya tidak bisa diungkap. Tujuan penelitian ini membahas tentang implementasi sistem keamanan data dengan metode algoritma hybrid Rivest Shamir Adleman (RSA) pada pembangkit kunci Diffie Hellman. Kombinasi suatu algoritma kriptografi kunci publik ke dalam algoritma pertukaran kunci Diffie Hellman yang digunakan untuk algoritma kunci simetri merupakan hal yang menarik. Dalam hal ini, algoritma kriptografi kunci publik yang digunakan untuk memperkuat algoritma pertukaran kunci Diffie-Hellman adalah RSA. RSA digunakan dengan alasan tingkat keamanannya sangat tinggi dari sekian banyak kemungkinan kombinasi algoritma. Pada kombinasi algoritma RSA sangat bermanfaat dalam proses pertukaran kunci dan dengan kombinasi algoritma Diffie Hellman bisa memberikan hasil pada kombinasi kedua metode tersebut sehingga keamanan data jadi lebih terjaga dan memberi tingkat kesukaran pada kunci menjadi lebih rumit serta kompleks juga membuat kunci tersebut sulit untuk dipecahkan oleh penyadap dengan hasil perhitungan nilai kunci simetris yang didapatkan oleh Alice dengan nilai kunci simetris key x = yx mod q = 805599 mod 1444 = 961 dan Bob dengan nilai kunci simetris Key y = x4 mod q = 599805 mod 1444= 961.

Abstract

In the world of cryptography, the key to encrypt and decrypt secret messages is one of the most important. The key determines whether the ciphertext can be read or not. The secret of the key is

Romindo,
Email: romindo4@gmail.com.

actually something that may be more essential and important than the secret of the ciphertext itself, in the sense that the ciphertext message can be leaked but the key cannot be revealed. The purpose of this study is to discuss the implementation of a data security system using the Rivest Shamir Adleman (RSA) hybrid algorithm method on the Diffie Hellman key generator. The incorporation of the public key cryptography algorithm into the Diffie Hellman key exchange algorithm used for the symmetric key algorithm is an interesting thing. In this case, the public key cryptography algorithm used to strengthen the Diffie-Hellman key exchange algorithm is RSA. RSA is used because of the very high level of security from the many possible combinations of algorithms. The combination of the RSA algorithm is very useful in the key exchange process and with the combination of the Diffie Hellman algorithm it can provide a combination of both methods so that data security is more maintained and makes the difficulty level of the key more complicated and complicated also makes the key difficult for eavesdroppers to break. with the results of the calculation of the symmetric key value obtained by Alice with the symmetric key value of the key x = yx mod q = 805599 mod 1444 = 961 and Bob with the symmetric key value of the key y = x4 mod q = 599805 mod 1444 = 961.

Keyword: RSA Algorithm, Diffie Hellman, Security System, Technology, Information Systems

1. Pendahuluan

Komunikasi adalah hal utama yang dilakukan oleh setiap orang, komunikasi juga sangat berpengaruh bagi kelangsungan hidup orang tersebut, sebab komunikasi adalah sarana utama bagi seseorang untuk mengenal serta beradaptasi dalam lingkungan hidup (Jamaludin & Romindo, 2020b). Manusia hidup berkumpul dan tidak dapat hidup hanya seorang diri saja, oleh karena itu hal yang sering dilakukan orang dahulu kala adalah dengan tulisan dimana sebuah tulisan berfungsi sebagai penyampaian pesan yang dibuat untuk mempermudah seseorang dalam berkomunikasi dengan kumpulan yang lainnya. Penulisan pun mengalami perkembangan dari zaman dahulu kala hingga zaman sekarang, pada zaman dahulu orang-orang menggunakan simbol, gambar, yang ditulis pada batu, dinding goa dan lain-lain.

Penulisan tersebut berupa, pesan untuk orang banyak, pesan untuk kelompok, pesan untuk satu orang saja, dan pesan rahasia yang bersifat pribadi hanya untuk orang-orang yang berkuasa atau memiliki peran penting dalam kepemimpinan. Kini semakin berkembanganya cara tiap-tiap orang dalam melakukan pengiriman pesan semakin berkembang juga cara untuk merahasiakan pesan tersebut supaya isi pesan tidak mudah diketahui oleh orang lain. Dari sinilah awal mula penemuan suatu ilmu baru dalam pengiriman pesan rahasia yang dinamakan dengan ilmu kriptografi. Semakin berkembangnya zaman semakin banyak pula penemuan baru dalam kehidupan manusia untuk berkomunikasi satu dengan lainnya, lalu di ciptakan sebuah komputer yang menjadi awal mula perkembangan zaman hingga ke masa moderen saat ini.

Untuk itu hal menjaga keamanan data merupakan aspek penting dalam pengiriman informasi ke berbagai macam orang yang telah menjadi rutinitas dalam kegiatan harian tiap-tiap orang, misalnya dalam penggunaan internet untuk mengirim data via *email*, untuk transaksi jual beli online, penggunaan media sosial, menggunakan kartu kredit atau debit dan lain-lain (Mesran & Nasution, 2020). Dengan melakukan rutinitas kegiatan tersebut data diri orang tersebut sudah tersimpan dan dapat digunakan oleh pihak-pihak lain yang telah bersangkutan dengan orang tersebut. Dengan mengantisipasi terjadinya hal yang merugikan berbagai pihak kemajuan teknologi memberikan

inovasi dengan merancang suatu kode agar menjaga keamanan data operasional pada jaringan publik tersebut agar pesan yang dikirim tetap dalam kondisi rahasia dan aman, karena jaringan publik rentan akan penyadapan data atau terdapat sistem peretas oleh pihak lain. Layanan keamanan data tersebut menerapkan sistem keamanan pada data yang telah ditetapkan, dimana terjadinya proses implementasi yang menghasilkan kata sandi khusus, penerapan tersebut dikenal dengan metode kriptografi.

Kriptografi merupakan sebuah teknik penyandian untuk memberikan keamanan extra dalam pengiriman data atau pesan khusus yang berdasarkan pada teknik perhitungan matematika (Hariati et al., 2018). Proses pada kriptografi itu sendiri merupakan proses untuk menjaga dan memberi perlindungan pada data yang memiliki informasi khusus. Ilmu kriptografi dilakukan dengan cara subtitusi (pergantian huruf) dan transposisi (perpindahan posisi) yang menghasilkan kode - kode rahasia dengan makna yang sulit terpecahkan oleh orang lain (Surbakti, 2019). Teknik enkripsi adalah proses awal pengacakkan data "naskah asli" (plaintext) hasil dari teknik enkripsi adalah sistem subtitusi atau data asli sudah menjadi "naskah acak" (ciphertext) menjadi data yang tidak mudah dipahami orang lain, yang dapat membuka data asli (pesan asli) hanya orang yang memiliki kunci dekripsi (Saragi et al., 2020). Teknik deskripsi yang merupakan teknik kebalikkan dari proses enkripsi atau pengembalian naskah asli, dimana proses pengembalian naskah acak harus di deskripsi dengan kunci yang sesuai dengan kunci enkripsi untuk mendapatkan pesan asli. Kriptografi tidak hanya bermanfaat untuk penyembunyian data tetapi merupakan kumpulan teknik yang menyediakan keamanan pada data tersebut.

Pada tahun 2016 penelitian oleh Ashari Arief dan Ragil Saputra dari jurusan Ilmu Komputer, FSM Universitas Diponegoro Semarang (Arief & Saputra, 2016). Penelitian ini membahas tentang kemajuan teknologi yang bersifat instant messaging dengan banyaknya dampak negatif berupa penyadapan atau mudah diretas oleh pihak lain. Menggunakan algoritma RSA untuk menerapkan proses penyandian sehingga menghasilkan data yang telah di enkripsi serta memiliki beberapa banyak kunci sesuai dengan data atau pesan pada kunci dekripsi yang bersifat kunci publik, pada proses dekripsi algoritma RSA sering terjadi kendala karena ukuran kunci dekripsi yang relatif lebih dari kapasitas sehingga membuat proses pengembalian ke naskah asli menjadi lebih lambat. Untuk mempercapat proses maka RSA dapat dimodifikasi dengan menggukan algoritma *Chinese Remainder Theorem* (CRT), sering disebut juga dengan algoritma RSA-CRT. Dengan kombinasi dari algoritma kriptografi RSA-CRT pada aplikasi instant messaging mengasilkan proses dekripsi RSA-CRT dua kali lebih cepat dibandingkan proses dekripsi RSA.

Pada tahun 2018 penelitian oleh Ahmad Ihsanudin dan Achmad Solichin dari Program Studi Teknik Informatika, Falkutas Teknoligi Informasi Universitas Budi Luhur (Ihsanudin & Solichin, 2018). Penelitian ini membahas tentang algoritma *Data Encryption Standart* (DES) dan Vernam Cipher dengan pembangkitan kunci algoritma Diffie Hellman. Proses enkripsi dilakukan pada pendaftaran mahasiswa yang dimasukkan dalam aplikasi sebelum dikirimkan ke sever. Ketika data sampai di server data kemudian didekripsi dan disimpan ke data base server, sehingga menghasilkan data yang sulit di pengerti (*Ciphertext*). Hasil ini kemudian di implementasikan pada sebuah program aplikasi berbasis android dengan bahasa pemrograman Java, dimana dapat membantu keamanan data pada saat proses pendaftaran mahasiswa dengan mudah serta mengurangiadanya resiko pencurian dan penyalahgunaan data.

Penelitian yang pernah dilakukan oleh Febri Dwinata Yonathan, dkk. Penelitian ini membahas tentang Kombinasi algoritma enkripsi dan kompresi menciptakan dokumen yang tidak dapat dibaca oleh pihak ketiga yang tidak berwenang, menghasilkan dokumen yang lebih kecil, menghasilkan lebih banyak ruang penyimpanan dan waktu penyelesaian yang lebih cepat. Berdasarkan hasil pengujian, lamanya proses encoding dan decoding dipengaruhi oleh ukuran data dokumen. Ukuran data setiap dokumen terenkripsi meningkat, seperti pada contoh di mana ukuran asli dokumen terenkripsi adalah antara 657 dan 7.500 byte setelah enkripsi. Algoritma kompresi Huffman mengurangi ukuran, seperti pada contoh dokumen yang ukuran awalnya 4.080 byte setelah dikompresi menjadi 2.629 byte (Yonathan et al., 2021).

Penelitian pada 2020 yang dilakukan oleh Luthfiatun Nisa, dkk. Penelitian ini membahas tentang Kombinasi algoritma Diffie-Hellman dan ElGamal untuk melindungi pesan teks dan gambar. Kombinasi kedua algoritma ini melibatkan empat proses: pertukaran kunci, pembuatan kunci, enkripsi dan dekripsi. Menurut hasil pencarian, untuk 10 file teks dengan ukuran mulai dari 10 Kb hingga 100 Kb, waktu encoding rata-rata adalah 119,9 ms, decoding adalah248,3 ms,dan bitrate 600,96 Kbps. Sedangkan untuk file gambarberukuran 100 x 100 piksel, tingkat reduksinya adalah1000 x 1000 piksel, waktu pengkodean rata-rata adalah 2623,4 ms, waktu dekode adalah 39,5milidetik, dan nilai kesalahannya adalah Mean Square Error (MSE) adalah 213,95, 27,67%., Peak Signal to Noise Ratio (PSNR) dengan sebesar 173,27.dB dengan tingkat kenaikan sebesar 1,9 %. Selain itu, menurut hasil uji Avalanche, bit shift rateuntuk file teks adalah 85,18ndan8,6% untuk filegambar (Nisa et al., 2020).

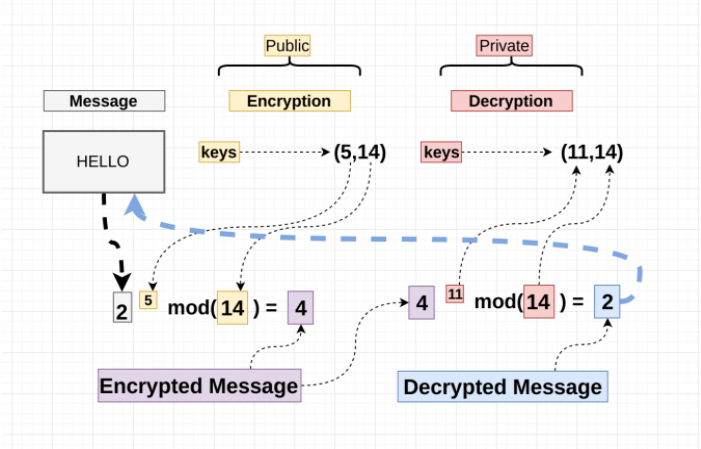
Pada penelitian ini menggunakan metode algoritma *Rivest Shamir Adleman* (RSA) dengan alasan tingkat keamanannya yang tinggi dan dapat di implementasikan pada sistem kriptografi kunci publik pada algoritma *Diffie Hellman* yang merupakan pembangkit kunci sandi dengan cara bertukar kunci publik antara pengirim dan penerima sehingga menghasilkan kunci rahasia. Berdasarkan latar belakang diatas, maka peneliti tertarik untuk melakukan.

2. Metode Penelitian

2.1 Rivest Shamir Adleman (RSA)

Algoritma RSA adalah algoritma asimetris yang menggunakan metode kunci publik dimana kunci tersebut harus sepasang, yaitu satu kunci untuk enkripsi bersifat *public* dan satu kunci lagi untuk proses dekripsi bersifat *private* (Jamaludin & Romindo, 2020a). Algoritma ini diterapkan untuk mengenkripsi kunci asli (plainkey) menjadi kunci enkripsi (chiperkey). Ketika kunci diambil dari algoritma simetris (enigma) untuk menghasilkan skema asosiasi yang menjamin integritas dan kerahasiaanpesan (Prasetyo et al., 2018). Konsep dasar enkripsi dan dekripsi RSA merupakan bilangan prima serta aritmetika modulo. Kunci publik merupakan bilangan prima pada kunci tersebut tidak dirahasiakan, kunci publik tersebut merupakan kunci dasar yang berada pada proses enkripsi. Kunci dekripsi bersifat rahasia atau kunci milik pribadi, untuk memperoleh kunci tersebut harus dengan cara memfaktorkan bilangan bulat menjadi bilangan prima dimana akan melalui proses yang sangat merumitkan dalam menemukan kunci yang sebenarnya. Metode pemfaktoran dengan pohon faktor cukup memakan waktu lama sebab semakin besar bilangan tersebut maka akan semakin sulit untuk difaktorkan dan akan memperkuat metode kriptografi pada algoritma RSA (Gunawan, 2018). Oleh sebab itu ketentuan dalam algoritma RSA harus dengan bilang prima besar untuk memperoleh hasil keamanan yang optimal, seperti pada gambar 1.

SATIN – Sains dan Teknologi Informasi
Vol. 7, No. 2, Desember 2021, pp. 92-101
ISSN: 2527-9114, DOI: 10.33372/stn.v7i2.783



Gambar 1. Proses enkripsi dan dekripsi algoritma rsa (Yalisa et al., 2019)

Pembangkitan Kunci pada Algoritma RSA. Rumus utama pada proses enkripsi atau dekripsi algoritma RSA, lihat rumus 1 dan 2 (Gunawan, 2017).

$E_e (m) = c = m^e \bmod n,$ (1)

$D_d (c) = m = c^d \bmod n,$ (2)

dimana E_e (m) merupakan fungsi enkripsi terhadap *plaintext* m, Dan D_d (c) merupakan fungsi dekripsi terhadap *chipertext* c.

Terdapat Nilai (d, e, n) dimana yang merupakan pasangan kunci publik (e,n) dan kunci private (d) yang diperoleh dengan menggunakan aturan pembangkitan kunci sebagai berikut:

a. Pilih dua buah bilangan prima sembarang, p dan q.
b. Hitung n = p.q (sebaiknya p≠q, sebab jika p=q maka,

n =p^2sehingga p dapat diperoleh dengan mudah dengan menarik akar pangkat dua dari n).

a. Hitung ϕ(n) = (p-1)(q-1).
b. Pilih kunci publik e, yang relatif prima terhadap ϕ(n).
c. Pembangkitan kunci privat dengan menggunakanpersamaan e.d ≡ 1(mod ϕ(n)) yang ekivalen dengan e.d = 1+ kϕ(n), sehingga secara sederhana d dapat dihitung, seperi pada rumus 3 (Achmad et al., 2017).

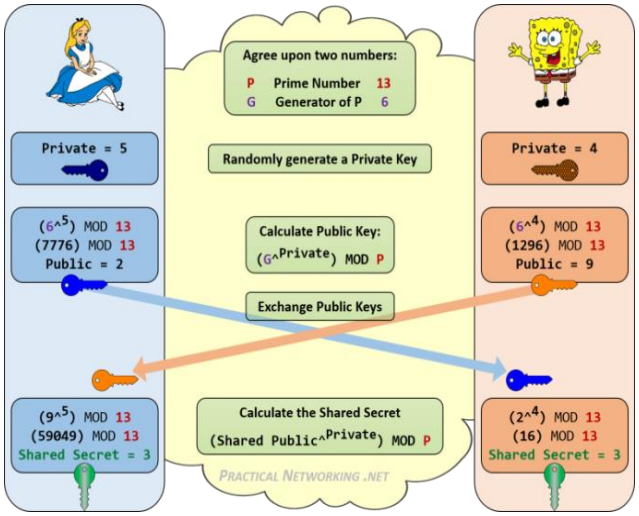
$(d = \frac{1+k\varphi(n)}{e})$ (3)

Setelah perhitungan selesai, maka hasil nilai dari (d) merupakan kunci dekripsi.

2.2 Algoritma Diffie Hellman

Algoritma *Diffie Hellman* merupakan algoritma yang pada prosesnya tidak memfokuskan terhadap teknik enkripsi dan dekripsi suatu data, tetapi titik fokus utama terdapat pada metode matematika dalam menghasilkan kunci rahasia(Yuniati & Sidiq, 2020). Hasil kunci rahasia tersebut dapat tersebar dan diketahui orang lain, tetapi tak perlu dikhawatirkan karena kunci tersebut hanya dapat digunakan dan didekripsikan oleh pemilik dan penerima data tersebut. Pada dasarnya algoritma ini merupakan konsep perhitungan matematika dasar dan aritmatika modulus. Fungsi unggul dari algoritma *Diffie Hellman* ini merupakan protokol pertukaran kunci internet serta sebagai pusat arsitektur IP *security*, jadi metode yang ada pada algoritma *Diffie Hellman* sangat aman dimana pengguna dapat membangkitkan kunci khusus meskipun dalam berkirim pesan mereka berada pada ruang lingkup publik yang bebas diketahui banyak orang (Alam & Pasaribu, 2019), sebagaimana dapat terlihat pada gambar 2.

SATIN – Sains dan Teknologi Informasi
Vol. 7, No. 2, Desember 2021, pp. 92-101
ISSN: 2527-9114, DOI: 10.33372/stn.v7i2.783



Gambar 2. Proses pertukaran kunci pada algoritma *diffie hellman* (Yalisa et al., 2019)

Langkah-langkah Pertukaran Kunci (Yalisa et al., 2019):

a. Pada algoritma Diffie Hellman terdapat sistemParamater (p) yang merupakan bilangan prima besar dan parameter q (generator) adalah bilangan integer yang tidak melebihi nilai pada p.
b. Terdapat proses pertukaran kunci yang dilakukan antara J dan C, konsep pertukaran kunci tersebut memiliki metode utama perhitungan matematika pada proses rumus 4 dan 5.

   $J = q^a \bmod p$ (4)

   $C = q^b \bmod p$ (5)
c. Algoritma Diffie Hellman memiliki kelebihan dimana proses pertukaran kunci tidak hanya untuk 2 orang penggunamelainkan dapat digunakan untuk beberapa orang. Dalam proses pertukaran kunci harus memenuhi 2 prinsip utama yang harus dilakukan dalam metode tersebut yaitu :
   1. Memiliki bilangan p dan q yang sudah disepakati oleh semua pihak.
   2. Semua pihak harus melakukan pertukaran data sesuai dengan kebutuhan yang diperlukan oleh setiap anggota lainnya sehingga semua data secara merata dapat di proses, $q^{abc....n}$
d. Prosespertukaran proses kunci:
   1. Memilih bilangan prima (p) kemudian bilangan (q) yang akan digunakan sebagai basis atau generator, bilangan tersebut dapat diketahui oleh publik.
   2. Pilih bilangan acak pada pengirim (j) yang tidak dapat diketahui oleh orang lain.
   3. Pilih bilangan acak pada penerima (c) yang tidak diketahui oleh orang lain.
   4. Pengirim menghitung ($J = q^a \bmod p$) bilangan yang terdapat pada J merupakan kunci publik.
   5. Penerima menghitung ($C = q^b \bmod p$) bilang yang terdapat pada B merupakan kunci publik.
   6. Terjadi proses pertukaran bilangan J dan C terhadap pengirim dan penerima.
   7. Kemudian pengirim menghitung (Key $J = C^a \bmod p$).
   8. Kemudian penerima menghitung (Key $C = J^b \bmod p$).
   9. Hasil dari perhitungan J dan C merupakan kunci private yang hanya di ketahui oleh pengirim dan penerima data tersebut.

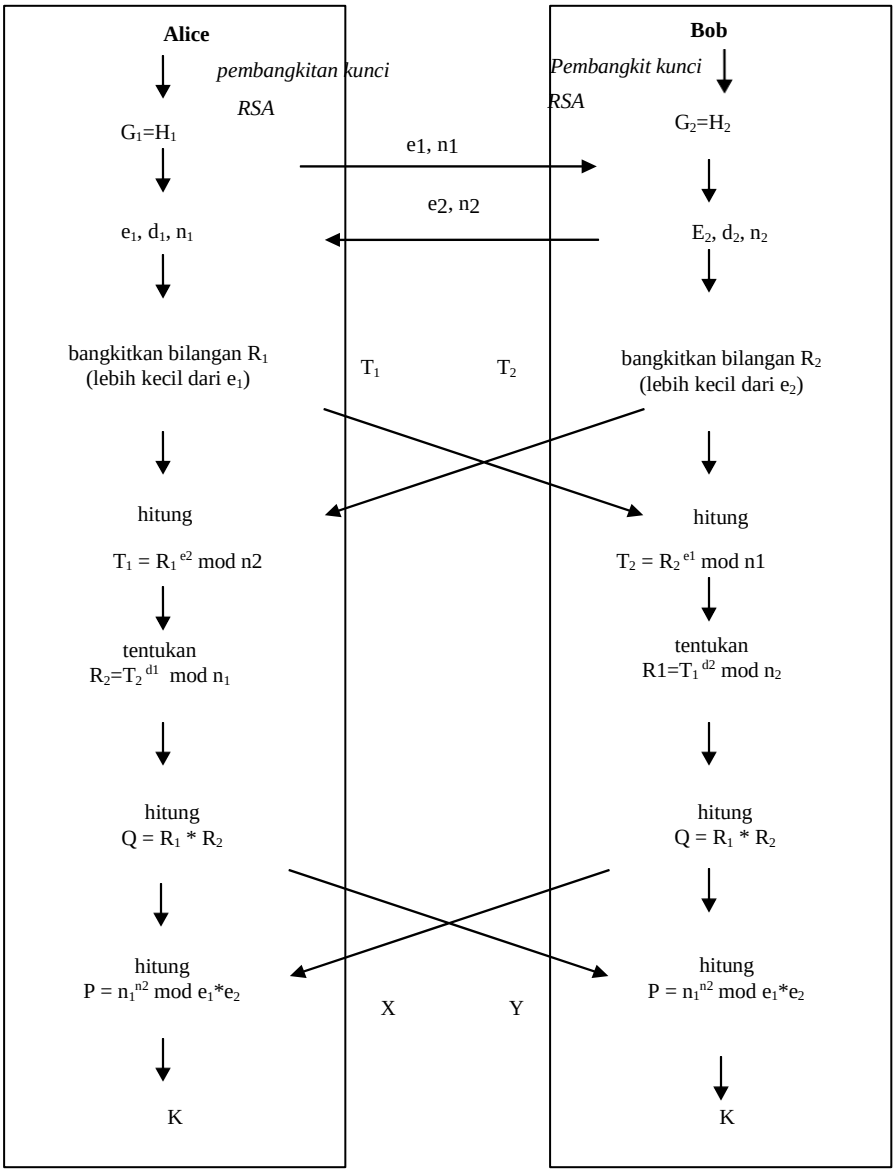
2.3 Langkah-langkah algoritma hybrid: Deffie- Helman dan RSA.

Misal ada penyadap katakan si Jhon di perjalanan transmisi pesan tersebut. Jhon hanya bisa mendapat informasi nilai e, n, X

SATIN – Sains dan Teknologi Informasi
Vol. 7, No. 2, Desember 2021, pp. 92-101
ISSN: 2527-9114, DOI: 10.33372/stn.v7i2.783

dan Y yang bukan merupakan kunci untuk memecahkan pesan tersebut. Ada kesulitan pada perhitungan logaritma diskrit untuk mendapat nilai K tanpa mengetahui nilai P dan Q yang tidak dipublikasikan.Dengan demikian Alice dan Bob dapat mengirim kunci yang disandikan (bukan kunci sebenarnya) dengan tingkat keamanan berlipat (Suhandinata et al., 2019).

Skema pada gambar 3 memperlihatkan lebih jelas algoritma pertukaran kunci Diffie-Hellman setelah diimbuhkan RSA. Di akhir perhitungan, Alice dan Bob telah memiliki kunci rahasia yang sama.



Gambar 3. Algoritma pertukaran kunci diffie-hellman

3. Hasil dan Pembahasan

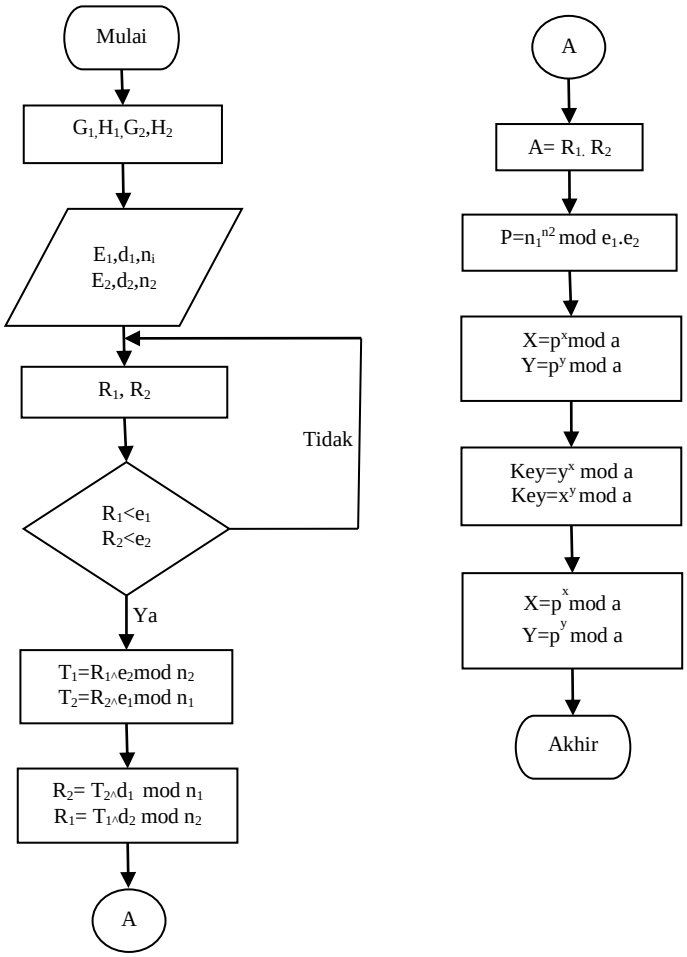
Analisis pembangkit kunci algoritma kriptografi Diffie Hellman dengan algoritma RSA.

a. Alice memiliki kunci public dan kunci private G1 = 47 dan H1 = 71
   Dan bob memiliki kunci public dan kunci private G2 = 53 dan H2 =97
b. Setelah kunci dikerjakan Alice memiliki e1 = 79, n1= 71 dan d1 =1019
   Bob memiliki e2 = 84, n2 = 79 dan d2 = 2114

SATIN – Sains dan Teknologi Informasi
Vol. 7, No. 2, Desember 2021, pp. 92-101
ISSN: 2527-9114, DOI: 10.33372/stn.v7i2.783

c. Alice membangkitkanbilangan R1<71 misalnya 69
   Bob membangkitkan bilangan R2<76 misalnya 75
d. Kemudian Alice dan Bob mengenkripsikan masing-masing bilangan dengan mengirim hasilnya
   T1 = 6984 mod 79 = 18
   T2 = 7579 mod 71 = 15
e. Alice dekripsi T2 →R2
   Bob dekripsi T1 →R1
   R2 = 181015 mod 71 → 38
   R1 = 152114 mod 70 → 38
f. Masing-masing menghitung nilai
   Q =R1*R2 = 38*38 = 1444
   P = n1n2 mod (e1*e2)= 7179 mod (79*84) = 71
g. Alice membangkitkan nilai x = 113 dan Bob nilai y =366
h. Alice → x = px mod q = proses Diffie Hellman
   Bob → y = py mod q = proses Diffie Hellman
   X= 71113 mod 1444 = 599
   Y = 71366 mod 1444 = 805
i. Hasil perhitungan nilai kunci simetris dari pengirim pesan yang bernama Alice.
   Key x = yx mod q = 805599 mod 1444 = 961
   Bob menghitung nilai kunci simetris
   Key y = x4 mod q = 599805 mod 1444= 961

Proses perhitungan pembangkit kunci algoritma kriptografi diffie hellman dengan algoritma RSA digambarkan dalam bentuk flowchart, perhatikan gambar 4.



Gambar 4. Flowchart algoritm hybrid rsa dan diffie hellman

4. Simpulan

Dari sekian banyak kemungkinan kombinasi algoritma, kombinasi algoritma RSA sangat bermanfaat dalam memperkuat algoritma dalam proses pertukaran kunci Diffie-Hellman bisa menjadi contoh bagaimana peningkatan keamanan itu terjadi. Pertukaran kunci menjadi lebih kompleks dan lebih sulit untuk dipecahkan oleh para penyadap dengan hasil perhitungan nilai kunci simetris yang didapatkan oleh Alice dengan nilai kunci simetris key x = yx mod q = 805599 mod 1444 = 961 dan Bob dengan nilai kunci simetris key y = x4 mod q = 599805 mod 1444 = 961.

5. Referensi

Achmad, F., Novriyenni, N., Yani, M., & Akim, M. H. P. (2017). Analisis Hybrid Cryptosystem Algoritma Algoritma. *Jurnal Teknik Informatika Kaputama (JTIK)*, *1*(2), 36–44.

Alam, H., & Pasaribu, K. M. (2019). *Rancang Bangun Aplikasi Penyandian Data Text Menggunakan Algoritma Diffie-Hellman Dan Algoritma Rc4*. 1–7.

Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics*, *3*(1), 46–54. https://doi.org/10.15294/sji.v3i1.6115

Gunawan, I. (2017). Pengamanan Acakan Biss Menggunakan Algoritma RSA. *Jurasik (Jurnal Riset Sistem Informasi Dan Teknik Informatika)*, *2*(1), 58. https://doi.org/10.30645/jurasik.v2i1.19

Gunawan, I. (2018). Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *2*(2), 124–129. https://doi.org/10.30743/infotekjar.v2i2.266

Hariati, A., Hardiyanti, K., & Putri, W. E. (2018). Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks. *Sinkron*, *2*(2), 13–17.

Ihsanudin, A., & Solichin, A. (2018). *Penerapan Algoritma DES, Vernam Cipher dan Diffie-Hellman untuk Mengamankan Data Pendaftaran Mahasiswa Baru pada*. *1*(1), 60–67.

Jamaludin, J., & Romindo, R. (2020a). *Hybrid Cryptosystem Analysis by Using The Combination of Vigenere Cipher and RSA for Text Security*. *1*(1), 89–100. https://doi.org/10.31098/ic-smart.v1i1.31

Jamaludin, J., & Romindo, R. (2020b). Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security. *International Journal of Information System & Technology*, *4*(1), 471–481.

Mesran, M., & Nasution, S. D. (2020). Peningkatan Keamanan Kriptografi Caesar Cipher dengan Menerapkan Algoritma Kompresi "Stout Codes." *JURNAL RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1209–1215.

Nisa, L., Indriyani, T., & Ruswiansari, M. (2020). Aplikasi Enkripsi Citra dan Teks Menggunakan Algoritma Diffie-Hellman dan ElGamal. *Jurnal Teknologi Dan Manajemen*, *1*(1), 8–17.

Prasetyo, Y., Triandi, B., & Hardianto, H. (2018). Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA. *It (Informatic …*, *6*(1), 46–55.

Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 114. https://doi.org/10.30865/json.v1i2.1745

Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi, S. (2019).

Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *6*(1), 1–10. https://doi.org/10.33330/jurteksi.v6i1.395

Surbakti, S. D. B. (2019). Implementasi Algoritma Playfair Cipher pada Penyandian Data. *Jurnal Teknik Informatika Unika St. Thomas*, *04*(02), 125–132.

Yalisa, N., Arhami, M., & Azhar, A. (2019). Algoritma Elgamal dengan Pertukaran Kunci Diffie Hellman pada Aplikasi Keamanan Citra Sidik Jari Berbasis Android. *Prosiding Seminar Nasional …*, *2*(1), 1–7.

Yonathan, F. D., Nasution, H., & Priyanto, H. (2021). *Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan*. *7*(2), 181–195.

Yuniati, T., & Sidiq, M. F. (2020). Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1058–1069. https://doi.org/10.29207/resti.v4i6.2502