KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)
Volume 6, Nomor 1, November 2022
DOI: 10.30865/komik.v6i1.5775
ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 819-823

Pembangkitan Kunci pada Algoritma Hill Cipher menggunakan Teknik Distribusi Angka Diffie-Hellman

Andysah Putera Utama Siahaan

Fakultas Sains dan Teknologi, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: andiesiahaan@gmail.com

Abstrak-Pengiriman data perlu dilakukan dengan baik dan aman karena menyangkut informasi penting yang dimiliki oleh seseorang, perusahaan atau pihak tertentu. Pengiriman pesan sering menggunakan password atau kata kunci agar proses pengiriman berjalan dengan baik. Penerima pesan harus memiliki password tersebut untuk dapat membuka pesan tersebut setelah diterima. Pertukaran kunci mengakibatkan kunci tersebut dapat diketahui oleh pihak yang tidak bertanggung jawab. Proses pembangkitan kunci menggunakan algoritma Diffie-Hellman merupakan teknik yang baik agar dapat menghindari pertukaran kunci antara pengirim dan penerima. Penelitian ini menggunakan algoritma Hill Cipher dalam menguji pembangkitan sebanyak empat buah kunci yang akan ditempatkan pada matriks kunci 2 x 2. Hasilnya setiap kunci yang akan dibangkitkan akan menggunakan teknik Diffie-Hellman dalam menentukan nilai yang akan dimasukkan ke dalam matriks kunci Hill Cipher. Penggunaan teknik ini sangat baik dilakukan dalam memberikan kunci algoritma Hill Cipher kepada penerima pesan agar dapat membuka pesan yang dikirim oleh pengirim.

Kata Kunci: Hill Cipher, Diffie-Hellman, Distribusi, Enkripsi, Dekripsi

Abstract - Sending data needs to be done properly and safely because it involves important information owned by a person, company or certain party. Sending messages often uses passwords or keywords so that the sending process goes well. The recipient of the message must have the password to be able to open the message after it is received. The key exchange causes the key to be known by irresponsible parties. The key generation process using the Diffie-Hellman algorithm is a good technique to avoid key exchange between sender and receiver. This study uses the Hill Cipher algorithm to test the generation of four keys which will be placed in a 2 x 2 key matrix. As a result, each key that will be generated will use the Diffie-Hellman technique in determining the value to be entered into the Hill Cipher key matrix. The use of this technique is very well done in providing the Hill Cipher algorithm key to the recipient of the message so that it can open the message sent by the sender.

Keyword: Hill Cipher, Diffie-Hellman, Distribution, Encryption, Decryption

1. PENDAHULUAN

Informasi merupakan suatu pesan yang akan disebarluaskan atau dikirimkan kepada orang tertentu. Informasi dapat berupa data penting dari suatu perusahaan atau data yang memiliki kandungan informasi rahasia yang tidak boleh diketahui oleh orang lain. Pengiriman informasi membutuhkan keamanan yang baik. Keamanan ini sangat penting untuk dipertimbangkan. Dalam melakukan pengiriman data, ada tiga bagian yang terlibat yaitu pengirim, penerima dan pencuri pesan. Pencuri pesan tidak selamanya melakukan pencurian terhadap data yang akan dikirimkan tetapi bisa saja pengirim dan penerima pesan bernasib sial pada saat melakukan pertukaran informasi. Kebutuhan keamanan dikarenakan pengiriman data dilakukan melalui jaringan internet. Pengiriman data yang tidak memiliki keamanan akan menyebabkan kerugian bagi pengirim dan penerima pesan.

Pengiriman data dapat dilakukan dengan memanfaatkan teknik kriptografi [1]. Penelitian ini menggunakan algoritma klasik yaitu algoritma Hill Cipher dengan matriks 2 x 2. Enkripsi Hill Cipher membutuhkan empat angka yang akan ditempatkan pada matriks 2 x 2. Kerentanan algoritma Hill Cipher adalah kunci yang dikirim ke penerima akan berpotensi dicuri oleh orang lain sehingga pengiriman kunci secara langsung tidak menjadi solusi yang baik.

Penulis menyarankan kunci tersebut sebaiknya dikirim menggunakan suatu cara. Empat buah angka yang ada pada matriks 2 x 2 akan dibangkitkan menggunakan teknik Diffie-Hellman agar angka tersebut tidak dapat diketahui oleh orang lain. Diffie-Hellman akan melakukan pencarian angka berdasarkan pemangkatan modular $A = G^X \bmod N$ [2]. Teknik yang dilakukan oleh algoritma Diffie-Hellman adalah seperti teknik Three-pass Protocol. Three-pass Protocol melakukan proses enkripsi dan dekripsi tanpa harus bertukar kunci antara pengirim dan penerima [3], dimana teknik Diffie-Hellman akan melakukan pertukaran sebagian angka dengan menggunakan pemangkatan modular secara matematika dalam mendapatkan kunci rahasia yang tidak akan diketahui oleh orang lain.

2. METODOLOGI PENELITIAN

2.1Kriptografi

Kriptografi adalah pembelajaran seputar cara atau tentang teknik mengirimkan informasi atau melakukan komunikasi secara aman yang tidak diketahui oleh orang lain selain pengirim dan penerima pesan. Pesan yang dikirimkan hanya dapat isinya oleh penerima. Istilah kriptografi berasal dari kata Yunani “kryptos”, yang artinya tersembunyi. Proses kriptografi adalah enkripsi dimana proses tersebut melakukan pengacakan teks biasa menjadi ciphertext dan kemudian akan dikembalikan lagi pada saat proses dekripsi. Proses kriptografi dapat dilakukan melalui berbagai media dalam menyamarkan informasi yaitu ke dalam gambar, file atau suara.

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 819-823

Kriptografi juga dapat diartikan sebagai teknik transformasi pesan dalam bentuk simbol atau karakter yang berada di tabel ASCII agar pesan tersebut tidak dapat diketahui atau dipahami oleh orang lain yang berhasil mendapatkan pesan tersebut. Kriptografi terdiri dari dua bagian proses yaitu enkripsi dan dekripsi [4].

2.2Hill Cipher

Hill cipher adalah algoritma kriptografi yang bersifat substitusi poligrafik berdasarkan aljabar linier. Hill cipher menggunakan operasi modulo untuk melakukan proses enkripsi dan dekripsi tergantung dengan pembatasan jumlah karakter yang digunakan. Algoritma Hill Cipher sering digunakan untuk penggunaan modulo 26 sesuai dengan jumlah abjad dari A hingga Z. Setiap huruf akan digantikan menjadi index 0 hingga 25. Dalam melakukan enkripsi, setiap blok n huruf akan dibentuk dalam matriks persegi 2 x 2 atau 3 x 3 atau n × n dan kemudian akan dikalikan dengan nilai setiap kunci yang sudah dibangkitkan. Untuk mendekripsi pesan, setiap blok dikalikan dengan kebalikan dari matriks yang digunakan untuk enkripsi [3],[5].

Hill Cipher menggunakan kunci yang memiliki nilai determinan ganjil karena nilai determinan yang bernilai genap tidak dapat membentuk kunci inverse yang akan digunakan pada proses dekripsi[6],[7]. Hasil determinan tersebut akan menentukan kunci inverse. Kunci inverse merupakan kunci yang digunakan oleh algoritma Hill Cipher pada proses dekripsi[8].

2.3Diffie-Hellman

Diffie-Hellman adalah teknik perhitungan matematika dalam melakukan pertukaran angka terhadap dua buah aktor yang bertindak sebagai pengirim dan penerima tanpa harus saling memberikan informasi lengkap seputar angka yang dihasilkan kepada masing-masing pengirim dan penerima[9]. Kedua pengirim dan penerima akan melakukan suatu perhitungan matematika yang hasilnya ada yang bersifat public dan privat. Nilai yang bersifat publik akan dikembalikan kepada pengirim atau penerima untuk melakukan pencarian nilai berikutnya. Perhitungan terakhir akan mendapatkan nilai yang sama antara pengirim dan penerima. Nilai inilah yang akan digunakan sebagai kunci pada proses enkripsi dan dekripsi [10].

Pertukaran kunci Diffie–Hellman adalah metode pembangkitan dan pertukaran kunci yang digunakan untuk teknik kriptografi secara aman melalui jaringan publik atau internet. Teknik ini merupakan salah satu protokol kunci publik pertama yang disusun oleh Ralph Merkle dan dinamai Whitfield Diffie dan Martin Hellman [11].

Tabel 1. Teknik pengiriman angka Diffie-Hellman

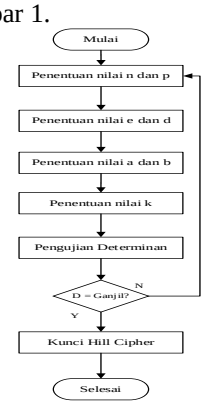
Pengirim	Penerima
n	p
e	d
$a = p^e \bmod n$	$b = p^d \bmod n$
$k = b^e \bmod n$	$k = a^d \bmod n$

Pengiriman angka menggunakan teknik Diffie-Hellman dapat dilihat pada tabel 1. Pengirim menentukan nilai N, penerima menentukan nilai P sebagai angka yang bersifat publik yang kemudian akan saling dipertukarkan. Pengirim menentukan nilai E dan penerima menentukan nilai D yang bersifat privat. Nilai E dan D hanya berada pada pengirim dan penerima. Pengirim dan penerima akan menentukan nilai A dan B berdasarkan perhitungan modulo eksponensial. Perhitungan akhir dari modulo eksponensial akan menghasilkan nilai K dimana angka ini akan bernilai sama pada pengirim dan penerima.

Penelitian ini memiliki beberapa bagian yang dilakukan untuk mendapatkan hasil. Ada beberapa bagian penting yang akan dijelaskan yang berhubungan dengan tahapan penelitian[12].

2.4 Tahapan Penelitian

Dalam proses penentuan kunci yang akan digunakan pada algoritma Hill Cipher, ada beberapa langkah yang harus dilakukan yang secara jelas dijelaskan pada gambar 1.



Gambar 1. Tahapan penelitian

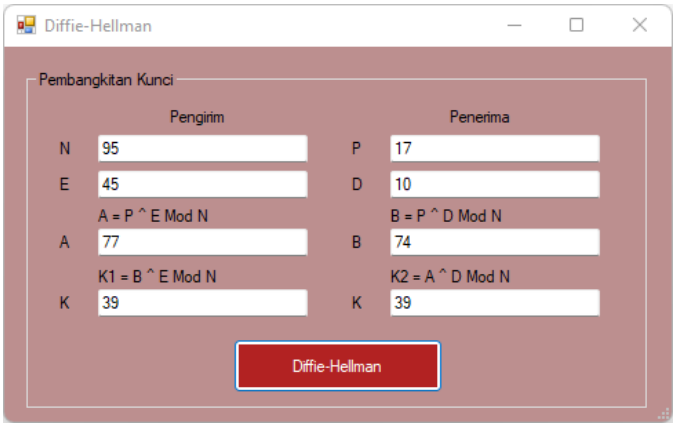
ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 819-823

Tahapan pertama yang dilakukan adalah menentukan dua angka n dan p secara acak yang bersifat publik dan akan dipertukarkan dengan batasan tertentu, misalnya dibatasi dengan 255 sesuai dengan nilai tertinggi pada tabel ASCII. Angka e dan d merupakan angka rahasia yang tidak boleh diberikan kepada penerima atau pengirim. Penentuan angka a dan b diperoleh melalui perhitungan matematika berdasarkan angka n, p, e dan d. Hasilnya akan saling dipertukarkan antara pengirim dan penerima untuk mendapatkan angka k yang merupakan angka yang akan digunakan pada matriks persegi Hill Cipher 2 x 2. Proses ini dilakukan sebanyak empat kali karena jumlah angka yang terdapat pada matriks tersebut adalah berjumlah empat buah. Matriks yang sudah dipenuhi dengan angka akan dilakukan pengujian determinan. Nilai determinan diperoleh dari rumus $D = (k1 * k4) - (k2 * k3)$. Hasil perhitungan determinan bernilai ganjil yang hanya dapat digunakan pada algoritma Hill Cipher karena memiliki kunci inverse yang akan digunakan pada proses dekripsi pesan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Bagian ini merupakan hasil yang dicapai dalam menentukan kunci Hill Cipher menggunakan teknik Diffie-Hellman. Penentuan nilai kunci yang diperoleh menggunakan teknik Diffie-Hellman akan dilakukan dengan bantuan program aplikasi Microsoft Visual Basic 2010.



Gambar 2. Hasil perhitungan Diffie-Hellman

Hasil perhitungan dapat dilihat melalui gambar 2. Pengirim membangkitkan angka acak N = 95 bersifat publik dan E = 45 bersifat privat. Penerima membangkitkan angka acak juga dengan komposisi P = 17 bersifat publik dan D = 10 bersifat privat. Nilai N akan diberikan ke penerima dan nilai P akan diberikan ke pengirim sehingga pengirim dapat menghitung A = 14^{45} mod 95, hasilnya adalah 77 dan penerima menghitung nilai B = 17^{10} mod 95, hasilnya adalah 74. Nilai A akan diberikan ke penerima dan nilai B akan diberikan ke pengirim. Pengirim dapat menghitung nilai K = 74^{45} mod 95, hasilnya adalah 39 dan penerima dapat menghitung nilai K = 77^{10} mod 95, hasilnya adalah 39 juga. Angka 39 ini akan dimasukkan ke dalam matriks 2 x 2 Hill Cipher. Proses ini akan diulang sebanyak empat kali dan kemudian kunci Hill Cipher tersebut akan ditentukan nilai determinan apakah sudah bernilai ganjil.

Berikut ini akan dilakukan pengujian terhadap empat angka yang dibangkitkan menggunakan teknik Diffie-Hellman.

Pengirim
N = 28
E = 195
A = P ^ E Mod N
= 228 ^ 195 Mod 28
= 8
K = B ^ E Mod N
= 4 ^ 195 Mod 28
= 8

Penerima
P = 228
D = 28
B = P ^ D Mod N
= 228 ^ 28 Mod 28
= 4
K = A ^ D Mod N
= 8 ^ 28 Mod 28
= 8

Pengirim
N = 72
E = 124
A = P ^ E Mod N
= 14 ^ 124 Mod 72
= 40
K = B ^ E Mod N
= 56 ^ 124 Mod 72
= 16

Penerima
P = 14
D = 161
B = P ^ D Mod N
= 14 ^ 161 Mod 72
= 56
K = A ^ D Mod N
= 40 ^ 161 Mod 72
= 16

Pengirim
N = 59
E = 210
A = P ^ E Mod N
= 88 ^ 210 Mod 59
= 53
K = B ^ E Mod N
= 21 ^ 210 Mod 59
= 25

Penerima
P = 88

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 819-823

D = 77
B = P ^ D Mod N
= 88 ^ 77 Mod 59
= 21
K = A ^ D Mod N
= 53 ^ 77 Mod 59
= 25

Pengirim
N = 226
E = 39
A = P ^ E Mod N
= 212 ^ 39 Mod 226
= 166
K = B ^ E Mod N
= 198 ^ 39 Mod 226
= 64

Penerima
P = 212
D = 206
B = P ^ D Mod N
= 212 ^ 206 Mod 226
= 198
K = A ^ D Mod N
= 166 ^ 206 Mod 226
= 64

Hasil pembangkitan kunci menggunakan teknik Diffie-Hellman menghasilkan kunci K = $\begin{bmatrix} 8 & 16 \\ 25 & 64 \end{bmatrix}$. Determinan yang diperoleh adalah D = $(8 * 24) - (16 * 25) = 112$. Determinan yang dihasilkan tidak bernilai ganjil sehingga tidak dapat digunakan pada algoritma Hill Cipher. Percobaan berikutnya akan diulang sehingga mendapatkan determinan yang sesuai.

Pengirim
N = 55
E = 21
A = P ^ E Mod N
= 125 ^ 21 Mod 55
= 15
K = B ^ E Mod N
= 45 ^ 21 Mod 55
= 45

Penerima
P = 125
D = 45
B = P ^ D Mod N
= 125 ^ 45 Mod 55
= 45
K = A ^ D Mod N
= 15 ^ 45 Mod 55
= 45

Pengirim
N = 239
E = 126
A = P ^ E Mod N
= 192 ^ 126 Mod 239
= 166
K = B ^ E Mod N
= 91 ^ 126 Mod 239
= 22

Penerima
P = 192
D = 72
B = P ^ D Mod N
= 192 ^ 72 Mod 239
= 91
K = A ^ D Mod N
= 166 ^ 72 Mod 239
= 22

Pengirim
N = 69
E = 45
A = P ^ E Mod N
= 134 ^ 45 Mod 69
= 65
K = B ^ E Mod N
= 38 ^ 45 Mod 69
= 38

Penerima
P = 134
D = 183
B = P ^ D Mod N
= 134 ^ 183 Mod 69
= 38
K = A ^ D Mod N
= 65 ^ 183 Mod 69
= 38

Pengirim
N = 236
E = 207
A = P ^ E Mod N
= 213 ^ 207 Mod 236
= 181
K = B ^ E Mod N
= 137 ^ 207 Mod 236
= 49

Penerima
P = 213
D = 163
B = P ^ D Mod N
= 213 ^ 163 Mod 236
= 137
K = A ^ D Mod N
= 181 ^ 163 Mod 236
= 49

Pembangkitan kunci menggunakan teknik Diffie-Hellman pada percobaan berikutnya menghasilkan kunci $K = \begin{bmatrix} 35 & 22 \\ 38 & 49 \end{bmatrix}$. Pencarian determinan dilakukan berdasarkan kunci yang telah dibangkitkan sehingga diperoleh $D = (35 * 49) - (22 * 38) = 233$. Determinan yang dihasilkan sudah sesuai karena bernilai ganjil sehingga dapat digunakan untuk proses dekripsi algoritma Hill Cipher karena memiliki kunci inverse yang benar. Kunci Inverse yang dihasilkan adalah $Ki = \begin{bmatrix} 153 & 250 \\ 106 & 245 \end{bmatrix}$

3.2 Pembahasan

Bagian ini merupakan pembahasan seputar apa yang sudah dilakukan pada pengujian teknik Diffie-Hellman dalam menentukan kunci matriks persegi 2 x 2 pada algoritma Hill Cipher. Pembangkitan kunci menggunakan teknik Diffie-Hellman tidak selamanya menghasilkan determinan yang sesuai atau bernilai ganjil. Apabila determinan yang dihasilkan adalah salah, maka pencarian angka yang dilakukan oleh teknik Diffie-Hellman akan diulang sebanyak empat kali lagi dan melakukan proses validasi determinan kembali, tetapi karena penentuan nilai determinan hanya memiliki syarat bahwa nilai tersebut harus ganjil, maka tidaklah susah untuk mendapatkan nilai tersebut sehingga proses pencarian menggunakan teknik Diffie-Hellman tidak membutuhkan waktu yang lama.

4. KESIMPULAN

Teknik Diffie-Hellman dapat digunakan dalam melakukan pembangkitan kunci matriks persegi 2 x 2 pada algoritma Hill Cipher. Kelemahan Diffie-Hellman adalah tidak dapat langsung menentukan kunci yang memiliki determinan yang

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 819-823

sesuai pada algoritma Hill Cipher tetapi hal ini tidak terlalu menjadi permasalahan yang berat karena proses pembangkitan kunci ini sangat cepat untuk dilakukan. Proses yang tidak menghasilkan kunci akan diulang kembali sehingga dalam beberapa saat, Diffie-Hellman dapat menghasilkan kunci yang bernilai determinan ganjil.

REFERENCES

[1] D. Kurnia, H. Dafitri, A. P. U. Siahaan, Sugianto, and Mardiana, "RSA 32-bit Implementation Technique," Int. J. Recent Trends Eng. Res., vol. 3, no. 7, pp. 279–284, Jul. 2017, doi: 10.23883/IJRTER.2017.3359.UXAIW.

[2] A. Kamsyakawuni, Fanani, A. Husnan, and A. Riski, "Pengamanan Citra dengan Algoritma Diffie-Hellman dan Algoritma Simplified Data Encryption Standard (S-DES)," J. Ilm. Mat. dan Pendidik. Mat., vol. 10, no. 2, pp. 63–80, 2018.

[3] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," Int. J. Sci. Res., vol. 5, no. 7, pp. 1149–1152, 2016.

[4] A. I. Permana, T. Tulus, and Z. Situmorang, "Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY," 2020, doi: 10.4108/eai.3-8-2019.2290723.

[5] V. S. Ginting, "Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa," J. Teknol. Inf., vol. 4, no. 2, pp. 241–246, 2020, doi: 10.36294/jurti.v4i2.1365.

[6] A. Serdano, M. Zarlis, Sawaluddin, and D. Hartama, "Pengamanan Pesan Menggunakan Algoritma Hill Cipher Dalam Keamanan Komputer," J. Mahajana Inf., vol. 4, no. 2, pp. 1–5, 2019.

[7] Y. W. Hasibuan, R. B. Veronica, J. Matematika, U. N. Semarang, K. S. Gunungpati, and I. Artikel, "How to Cite," vol. 11, no. 1, pp. 54–68, 2022.

[8] A. Manaor, H. Pardede, H. Manurung, and D. Filina, "Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi," J. Tek. Inform. Kaputama, vol. 1, no. 1, pp. 26–33, 2017.

[9] A. Wahyuni, "Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid : Diffie-Hellman dan RSA," Maj. Ilm. Inform., vol. 2, no. 2, pp. 15–23, 2011.

[10] Purwadi, H. Jaya, and A. Calam, "Aplikasi Kriptografi Asimetris dengan Metode Diffie-Hellman dan Algoritma ElGamal untuk Keamanan Teks," J. Ilm. Saintikom, vol. 13, no. 3, pp. 183–196, 2014.

[11] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Inf. Theory., vol. 22, no. 6, pp. 644–654, 1976.

[12] Abdul Halim Hasugian, "Implementasi Algoritma Hill Cipher Dalam Penyandian Data," Pelita Inform. Budi Darma, vol. IV, no. 2, pp. 115–122, 2013.