IMPLEMENTASI ALGORITMA BLUM-BLUM SHUB PADA ALGORITMA *ONE TIME PAD* (OTP) CIPHER DALAM PENGAMANAN PESAN

SKRIPSI

OLEH:
NOVI HARDIYANTIK
NIM. 19610013

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

IMPLEMENTASI ALGORITMA BLUM-BLUM SHUB PADA ALGORITMA *ONE TIME PAD* (OTP) CIPHER DALAM PENGAMANAN PESAN

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
Novi Hardiyantik
NIM. 19610013

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2023

IMPLEMENTASI ALGORITMA BLUM-BLUM SHUB PADA ALGORITMA *ONE TIME PAD* (OTP) CIPHER DALAM PENGAMANAN PESAN

SKRIPSI

Oleh
Novi Hardiyantik
NIM. 19610013

Telah Disetujui Untuk Diuji

Malang, 19 Desember 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si.	Ari Kusumastuti, M.Pd., M.Si.
NIP. 19900511 202321 1 029	NIP.19770521 200501 2 004

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005

IMPLEMENTASI ALGORITMA BLUM-BLUM SHUB PADA ALGORITMA *ONE TIME PAD* (OTP) CIPHER DALAM PENGAMANAN PESAN

SKRIPSI

Oleh:
Novi Hardiyantik
NIM. 19610013

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat.)

Tanggal 26 Desember 2023

Ketua Penguji	:Prof.Dr.H.Turmudzi, M.Si., Ph.D	.....
Anggota Penguji 1	:Muhammad Nafie Jauhari, M.Si.	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 3	: Ari Kusumastuti, M.Pd., M.Si.	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	:	Novi Hardiyantik
NIM	:	19610013
Program Studi	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	Implementasi Algoritma Blum-Blum Shub Pada Algoritma *One Time Pad Cipher* Dalam Pengaman Pesan.

Menyatakan dengan sebenar-benarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan dan pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 26 Desember 2023

Yang membuat pernyataan,

Novi Hardiyantik

NIM. 19610013

MOTO

"Sesungguhnya Allah Tidak Membebani Seseorang Melainkan Sesuai Dengan Kesanggupan."

(Al-Baqoroh : 44)

PERSEMBAHAN

Bismillahirrahmanirrahim, dengan mengucap syukur kepada Allah Swt. Skripsi ini peneliti persembahkan untuk ayahanda tercinta Baharudin yang tiada lelah berusaha menopang pendidikan anaknya, ibunda tercinta Sri Anik yang tiada henti mendo'akan anaknya, kaka tersayang Siti Istifadah, Abang tersayang Muladin Mulharam, Syahran Husin, adik tersayang Agus Tri Hardiyanto yang menjadi penyemangat, dan Teman tercinta Rafika, Kania, Lida, Aza, Dila, Riris, Hilda, Puan, Aniq, Miya, Fani, Fira yang selalu merayakan setiap momen serta menemani, membantu dan memberi dukungan peneliti.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan berkah, rahmat serta hidayah-Nya sehingga penulis masih diberikan nikmat kesehatan, kesabaran, dan kesempatan dalam pembuatan proposal skripsi yang berjudul "Implementasi Metode Algoritma Blum-Blum Shub pada Algoritma *One Time Pad* (OTP) Cipher dalam Pengamanan Pesan" dapat penulis lakukan dengan baik.

Sholawat dan salam selalu tercurahkan kepada Nabi Muhammad SAW yang telah menjadi panutan penulis agar menjadi pribadi yang cerdas dan berakhlak. Pada kesempatan kali ini, penulis ingin mengucapkan terima kasih kepada semua pihak yang telah mendukung, membantu, dan memotivasi dalam penyusunan proposal skripsi ini. Ucapan terima kasih dituliskan sebagai berikut:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. Hj. Sri Harini, M.Si., selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc., selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si., selaku dosen pembimbing I yang telah memberikan bimbingan, nasihat, do'a dan motivasi kepada penulis. Terimakasih atas semua waktu yang rela diberikan di sela-sela kesibukan Bapak.
5. Ari Kusumastuti, M.Pd., M.Si., selaku dosen pembimbing II yang telah memberikan bimbingan, nasihat, do'a dan motivasi kepada penulis. Terimakasih atas semua waktu yang rela diberikan di sela-sela kesibukan Ibu.
6. Prof. Dr. H. Turmudi, M.Si. Ph.D., selaku ketua penguji yang telah memberikan keritik, saran serta dukungan kepada penulis.
7. Mohammad Nafie Jauhari, M.Si., selaku anggota penguji yang telah memberikan keritik, saran serta dukungan kepada penulis.

8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
9. Ayahanda tercinta Baharudin, Ibunda tercinta Sri Anik, Kaka tercinta Siti Istifadah, Muladin Mulharam, Syahran Husin, Adik Tercinta Agus Tri Hardiyanto yang selalu mendoakan serta selalu mendukung penulis baik materi maupun nonmateri, tidak lupa nasehat-nasehat yang membangun bisa menjadi motivasi bagi penulis untuk menyelesaikan skripsi ini dengan baik.
10. Teman tercinta Rafika, Kania, Lida, Aza, Dila, Riris, Hilda, Puan, Aniq, Miya, Fani, Fira yang selalu merayakan setiap momen serta menemani, membantu dan memberikan dukungan kepeda penulis.
11. Sahabat saya Dicky Rega Firmansyah yang selalu memberikan dukungan serta semangat dalam penyususnan skripsi.
12. Seluruh teman-teman KKM Ngantang, PKL BPJS Pasuruan dan Matematika 2019 yang telah membarikan semangat serta bantuan kepada penulis.
13. Serta semua pihak yang selalu mendukung serta memberikan semangat dalam penyusunan skripsi ini.

Atas segala dukungan dan bantuan yang diberikan kepada penulis, semoga Allah SWT melimpahkan pahala yang berlipat ganda. Penulis menyadari bahwa dalam penulisan proposal masih terdapat banyak kekurangan didalamnya. Penulis mohon maaf apabila selama proses pembuatan proposal skripsi ini terdapat kesalahan. Selain itu, penulis berharap semoga proposal skripsi ini dapat bermanfaat bagi penulis dan para pembaca.

Malang, 26 Desember 2023

Penulis

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PENGAJUAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iv**
HALAMAN PENGESAHAN ..... **iv**
PERNYATAAN KEASLIAN TULISAN ..... **v**
MOTO ..... **vi**
PERSEMBAHAN ..... **vii**
KATA PENGANTAR ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR TABEL ..... **xii**
DAFTAR GAMBAR ..... **xiii**
ABSTRAK ..... **xv**
ABSTRACT ..... **xvi**
مستخلص البحث ..... **xvii**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 6
1.3 Tujuan Penelitian 7
1.4 Manfaat Penelitian 7
1.5 Batasan Masalah 8
1.6 Definisi Istilah 8
BAB II KAJIAN TEORI **10**
2.1 Kriptografi 10
2.1.1 Tujuan Kriptografi 11
2.1.2 Komponen Kriptografi 12
2.1.3 Jenis algoritma Kriptografi 13
2.1.4 Algoritma Kriptografi Modern 13
2.1.5 Algoritma Kriptografi Klasik 15
2.2 Teori Bilangan 16
2.2.1 Aritmatika Modulo 16
2.2.2 Kongruen 17
2.2.3 Balikan Modulo (Modulo Invers) 19
2.3 Algoritma One Time Pad Cipher 20
2.4 Algoritma Blum-Blum Shub 25
2.5 *Least Significant Bit* 27
2.6 Kajian Integritas Topik dengan Al-Quran dan Hadits 28
2.7 Kajian Topik Dengan Teori Pendukung 30
BAB III METODE PENELITIAN **32**
3.1 Jenis Penelitian 32
3.2 Pra Penelitian 32
3.3 Tahapan Penelitian 32
BAB IV HASIL DAN PEMBAHASAN **37**
4.1 Proses Pembentukan Kunci Menggunakan Algoritma Blum-Blum Shub 37

4.1.1 Algoritma Pembentukan Kunci menggunakan Algoritma Blum- Blum Shub 37
4.1.2 Simulasi dari Implementasi Kunci dengan Algoritma Blum-Blum Shub 38
4.2 Proses Enkripsi 41
4.2.1 Algoritma Enkripsi Algoritma *one time pad cipher* 42
4.2.2 Simulasi Enkripsi 42
4.3 Proses Dekripsi 43
4.3.1 Algoritma Dekripsi pada Algoritma *One Time Pad Cipher* 44
4.3.2 Simulasi Dekripsi 44
4.4 Kajian Integrasi Agama 45
BAB V PENUTUP 48
5.1 Kesimpulan 48
5.2 Saran 49
DAFTAR PUSTAKA 50
LAMPIRAN 52
RIWAYAT HIDUP 58

DAFTAR TABEL

Tabel 2.1 Hasil Pembangkit Kunci dari Algoritma Blum-Blum Shub 27
Tabel 4.1 Konversi Plainteks ke dalam Bentuk Desimal..... 38
Tabel 4.2 Bilangan Acak xi 39
Tabel 4.3 Mengubah Plainteks Menjadi Bilangan Desimal..... 42
Tabel 4.4 Proses Enkripsi Menggunakan Algoritma OTP..... 43
Tabel 4.5 Mengubah Cipherteks Menjadi Bilangan Desimal..... 44
Tabel 4.6 Proses Dekripsi Menggunakan Algoritma OTP 45

DAFTAR GAMBAR

Gambar 2.1 Enkripsi daSn Dekripsi dalam Pengiriman Pesan 7
Gambar 2.2 Proses Skema Kriptografi Simetri 10
Gambar 2.3 Proses Skema Kriptografi Asimetri 10
Gambar 2.4 Flowchart Modifikasi *One Time Pad* Cipher 26
Gambar 2.5 Flowchart Enkripsi Hasil Modifikasi *One Time Pad* Cipher 27
Gambar 2.6 Flowchart Dekripsi Hasil Modifikasi *One Time Pad* Cipher 28

DAFTAR SIMBOL

x_i : Bilangan Acak

s : Nilai Umpan

z_i : Bilaingan Acak Baru

c_i : Indeks Karakter *Ciphertext*

p_i : Indeks Karakter *Plaintext*

ABSTRAK

Hardiyantik, Novi. 2023. **Implementasi Algoritma Blum-Blum Shub Pada Algoritma *One Time Pad Cipher* Dalam Pengaman Pesan**. Skripsi. Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing :(1) Muhammad Khudzaifah, M.Si. (2) Ari Kusumastuti, M. Pd., M. Si.

Kata kunci: Penerapan, Blum-Blum Shub,Algoritma*, One Time Pad Cipher*

Keamanan pesan menjadi syarat penting dalam pertukar informasi. Hal ini dikarenakan banyaknya kejahatan internet sehingga para pengguna merasa tidak aman setiap kali mengirimkan pesan. Oleh karena itu, diperoleh solusi yang bisa membantu agar pesan atau informasi yang diperlukan bersifat aman sampai ke tujuan sesuai dengan yang diinginkan. Secara teoritis Blum-Blum Shub termasuk cryptographically secure pseudorandom generator (CSPRNG) yang paling mudah dan paling efektif. Algoritma one time pad cipher merupakan sebuah metode penerapan algoritma kunci simetri atau proses enkripsi dan dakripsi menggunakan kunci yang acak. Penelitian ini membahas tentang penerapan algoritma Blum-Blum Shub pada algoritma one time pad cipher dalam pengaman pesan. Proses pertama dilakukan dengan pembentukan kunci menggunakan algoritma Blum-Blum Shub selanjutnya kunci acak tersebut digunakan untuk enkripsi dan dekripsi pada algoritma one time pad cipher. Bilangan acak yang di hasilkan oleh algoritma Blum-Blum Shub sebanyak jumlah posisi huruf pada plainteks. Maka dari itu, cipherteks yang di hasilkan dari hasil penerapan algoritma Blum-Blum Shub pada algoritma one time pad cipher dapat digunakan untuk mengamankan pesan.

ABSTRACT

Hardiyantik, Novi. 2023. **Implementation of the Blum-Blum Shub Algorithm in the One Time Pad Cipher Algorithm in Message Security**. Thesis Department of Mathematics, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors:(I) Muhammad Khudzaifah, M.Si. (II) Ari Kusumastuti, M. Pd., M. Si.

Keywords: Implementation, Blum-Blum Shub, Algorithm, *One Time Pad Cipher*

Message security is an important requirement in the exchange of information. This is because there are so many internet crimes that users feel unsafe every time they send messages. Therefore, a solution is needed that can help so that the message or information needed is safe to the destination as desired. Theoretically, Blum-Blum Shub includes the easiest and most effective cryptographically secure pseudorandom generator (CSPRNG). The one time pad cipher algorithm is a method of applying symmetry key algorithms or the process of encryption and encryption using random keys. This study discusses the application of the Blum-Blum Shub algorithm to the one time pad cipher algorithm in message security. The first process is carried out by forming a key using the Blum-Blum Shub algorithm, then the random key is used for encryption and decryption on the one time pad cipher algorithm. Random numbers generated by the Blum-Blum Shub algorithm to the one time pad cipher algorithm can be used to secure messages.

مستخلص البحث

هارديانتيك، نوفي. ٢٠٢٣.**تنفيذ خوارزمية *Blum-Blum Shub* في خوارزمية تشفير *One Time Pad* في أمان الرسائل.** قسم الرياضيات، كلية العلوم والتكنولوجيا، الجامعة الإسلامية نيجري مولانا مالك إبراهيم مالانج. المستشارون: (١) محمد خذيفة، اماجستير. (٢) آري كوسوماستوتي ،الماجستير ،

الكلمات المفتاحية: التنفيذ، *Blum-Blum Shub*، الخوارزمية، تشفير لوحة زمنية واحدة

يعد أمان الرسائل مطلبًا مهمًا في تبادل المعلومات. وذلك لأن هناك الكثير من جرائم الإنترنت التي يشعر المستخدمون فيها بعدم الأمان في كل مرة يرسلون فيها رسالة. لذلك، هناك حاجة إلى حل يمكن أن يساعد في ضمان وصول الرسالة أو المعلومات المطلوبة بأمان إلى وجهتها المطلوبة. يناقش هذا البحث تطبيق خوارزمية *Blum-Blum Shub* في خوارزمية التشفير ذات لوحة المرة الواحدة في أمن الرسائل. تتم عملية التنفيذ باستخدام أرقام عشوائية تم إنشاؤها بواسطة خوارزمية *blum-blum shub* وتستخدم هذه الأرقام العشوائية للتشفير وفك التشفير في خوارزمية تشفير لوحة المرة الواحدة. الأرقام العشوائية التي تم إنشاؤها بواسطة خوارزمية *Blum-Blum Shub* تعادل عدد مواضع الحروف في النص العادي. وبالتالي فإن عملية التشفير تنتج مفتاحًا عشوائيًا للغاية. لذلك، فإن النص المشفر الناتج عن تنفيذ خوارزمية *blum-blum shub* في خوارزمية تشفير لوحة المرة الواحدة يكون أكثر صعوبة ويصعب حله عن طريق تحليل التشفير.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang bersifat pribadi dan rahasia. Kriptografi membuat data atau pesan menjadi kode-kode terlebih dahulu oleh pengirim. Proses ini dikenal dengan enkripsi. Enkripsi diartikan sebagi proses diubahnya data atau pesan yang hendak di kirim sehingga bentuk chiper tidak dikenali oleh pihak ke tiga. Setelah data atau pesan itu sampai kepada penerima, maka penerima melakukan dekripsi yang merupakan kebalikan dari enkripsi. Dekripsi diartikan sebagai proses mengubah data atau pesan kembali ke bentuk semula sehingga data atau pesan dapat tersampaikan dan dimengerti oleh penerima. Data atau pesan asli dinamakan plaintext sedangkan sesudah dikodekan dinamakan *Chipertext*. Proses enkripsi dan dekripsi memerlukan kunci dalam mekanismenya dan biasanya berupa string atau deretan bilangan.(Amin, 2016)

Fungsi utama ilmu kriptografi yaitu untuk memberikan keamanan pada suatu sistem dalam mengirimkan pesan agar pesan tersebut tidak dapat diretas oleh kriptanalis. Keamanan pesan atau informasi menjadi syarat yang harus dipenuhi oleh semua pihak yang terlibat dalam sistem tersebut. Kemajuan teknologi juga memberikan kemudahan kepada setiap pihak dalam bertukar pesan atau informasi. Kebutuhan akan informasi dan komunikasi merupakan hal yang tidak kalah pentingnya dari kebutuhan sandang dan pangan manusia meskipun, peranan informasi dalam beberapa dekade kurang mendapat perhatian. Pertukaran informasi tersebut juga memberikan dampak positif dan negatif. Dampak positif dari

kemajuan teknologi dalam bertukar pesan atau informasi ini seperti penyebaran informasi yang sangat luas dan cepat dari berbagai bidang memberikan perubahan yang amat cepat dalam kehidupan manusia. Hal ini juga menimbulkan dampak negatif yang bisa terjadi dikarenakan kurangnya keamanan yang digunakan dan mencegah *cryptanalysis*. Dengan adanya kejahatan-kejahatan internet ini para pengguna merasa semakin tidak aman setiap kali mengirimkan pesan. Maka diperlukan solusi yang bisa membantu agar pesan atau informasi yang dipertukarkan bersifat aman dan sampai ketujuan sesuai dengan yang diinginkan. Sebagaimana sesuai dengan konsep amanah bahwa merahasiakan pesan seseorang itu termasuk menjaga amanah dimana hanya penerima pesan tersebut lah yang boleh mengetahuinya. Dalam surah Al- Zalzalah ayat 7-8 yang artinya:

"Siapa yang mengerjakan kebaikan seberat zarah, dia akan melihat (balasan)-nya (7). Siapa yang mengerjakan kejahatan seberat zarah, dia akan melihat (balasan)-nya. (Q.S. Al-Zalzalah: 7-8)

Imam Jalaluddin As-Suyuti dalam kitabnya(Amiruddin, 2021), Lubabun Nuqul menyebutkan riwayat Ibnu Abi Hatim dari Said bin Jubair tentang asbabun nuzul surat az-Zalzalah ayat 7 dan 8 sebagai berikut:

Artinya, "Ibnu Abi Hatim meriwayatkan dari Said bin Jubair (Aly, 2019), dia berkata, "Ketika turun ayat 8 surat Al-Insan: *"Dan mereka memberikan makanan yang disukainya"*, kaum Muslimin mengira bahwa mereka tidak akan diberi pahala bila memberikan sesuatu yang sedikit. Sedangkan yang lainnya mengira bahwa mereka tidak dicela karena melakukan dosa kecil, dusta, melihat (yang haram), menggunjing dan yang memyerupainya. Mereka mengatakan bahwa Allah hanya akan memberikan siksaan pada dosa-dosa besar. Karena itu kemudian Allah swt menurunkan ayat 7 dan 8 surat Al-Zalzalah: "*Maka barangsiapa mengerjakan kebaikan seberat zarrah, niscaya dia akan melihat (balasan)nya, dan barangsiapa mengerjakan kejahatan seberat zarrah, niscaya dia akan melihat (baIasan)nya"*.

Ketika turun surah Al-Zalzalah ayat 7 dan 8 maka kaum muslimin beranggapan bahwa seseorang tidak akan diberi pahala atas amalan yang kecil

sedikit, mereka enggan memberi sebiji kurma, sepotong roti dan kenari, karna mereka menolak si miskin itu dan mereka mengatakan: ini bukan apa-apa, kami hanya diberi pahala atas pemberian yang kami sayangi, ada juga yang beranggapan mereka tidak dituntut terhadap dosa kecil, seperti dusta, melihat yang haram atau menggunjing orang, mereka mengatakan Allah hanya mengancam terhadap dosa-dosa yang besar. Maka ayat ini Allah menggemarkan mereka untuk beramal meskipun sedikit dari kebaikan yang mungkin kelak menjadi besar dan banyak, demikian pula mengancam dari perbuatan kejahatan yang kecil sedikit kemungkinan tertumpuk sehingga menjadi banyak dan basar.

Syekh Nawawi Banten (wafat 1316 H) menafsirkan ayat 7 dengan makna: "*Siapa yang mengerjakan kebaikan seberat zarrah, yakni seberat semut kecil dia akan melihatnya."* Kemudian ia menyebutkan perkataan Imam Ahmad bin Ka'ab Al-Qurazhi, sebagai berikut:

Artinya, "Ahmad bin Ka'ab Al-Qurazhi berkata: "*Siapa yang mengerjakan kebaikan seberat zarrah sedangkan dia seorang kafir, maka dia akan melihat balasanya di dunia, hingga di akhirat ia tidak mendapatkan apapun di sana; dan siapa dari seorang mukmin yang mengerjakan keburukan seberat zarrah, dia akan melihat hukumannya di dunia pada dirinya, harta, keluarga dan anaknya, sehingga ia keluar dari dunia dengan tidak ada keburukannya di sisi Allah swt."* (Al-Bantani,2017)

Kemudian beliau menjelaskan ayat 8: *"Siapa yang mengerjakan kejahatan seberat zarrah yakni seberat semut paling kecil, ia akan melihatnya."* Beliau menyebutkan perkataan Ibnu Abbas sebagai berikut: Artinya, *"Tidaklah seorang mukmin dan kafir yang melakukan kebaikan atau kejelekan kecuali Allah akan memperlihatkan kepadanya. Namun, orang mukmin akan diberi ampun dan diberi pahala atas kebaikannya. Sedangkan orang kafir kebaikannya akan ditolak dan disiksa sebab kejelekannya."* (Al-Bantani,2017)

Dari penjelasan di atas dapat disimpulkan bahwa orang kafir akan disiksa sebab kekafirannya, sedangkan kebaikannya hanya akan bermanfaat baginya selama di dunia saja, seperti menolak kejahatan atau bahaya dari dirinya. Adapun

di akhirat, kebaikannya tersebut tidak akan bermanfaat dan tidak akan dapat membebaskannya dari siksaan kekafiran, ini yang menjadikannya kekal di neraka.

Seiring dengan perkembangan zaman, kriptografi sudah menjadi sebuah bahan objek penelitian yang dilakukan oleh banyak orang, dari berbagai cara dengan menggabungkan beberapa metode kriptografi hingga menciptakan metode kriptografi yang baru. Menggabungkan dua buah cipher itu merupakan salah satu cara membuat sebuah kriptografi yang lebih aman atau biasa juga cara tersebut dinamakan dengan super enkripsi. Hal itu dilakukan agar bisa mendapatkan cipher yang lebih kuat sehingga tidak mudah untuk dipecahkan, dan juga untuk mengatasi penggunaan cipher tunggal yang secara komparatif sangatlah lemah.

Salah satu dari algoritma kriptografi yang dapat digunakan adalah *one time pad. One time pad* memiliki keunggulan dalam melakukan proses enkripsi dan dekripsi yaitu setiap karakter dalamkunci digunakan untuk mengenkripsi dan mendekripsi setiap karakter dalam plainteks. Hal ini membuat kriptanalis kesulitan dalam menemukan plainteks asli jika kunci yang digunakan adalah kunci yang acak.

Algoritma *one time pad* cipher diciptakan oleh Mayor J. Maugboune dan Gilbert Vernam pada tahun 1917. Algoritma *one time pad* cipher juga bisa disebut dengan algoritma Unbreakable Cipher. Hal ini dikarenakan sifat dari algoritma ini kunci harus berupa barisan nilai yang seluruhnya acak sempurna (*truly random*) dan juga panjang dari kunci algoritma ini haruslah sama dengan panjang plainteks nya.(Harahap & Khairina, 2018)

Dari sifat-sifat yang ada pada algoritma *one time pad* ini menyebabkan beberapa plainteks yang sama belum tentu bisa dienkripsi menjadi cipherteks yang

sama pula. Maksudnya adalah kriptanalis akan mendapatkan hasil bahwa sebuah cipherteks yang didekripsinya mungkin menghasilkan beberapa plainteks berbeda namun memiliki makna. Hal ini akan membingungkannya dalam menentukan plainteks mana yang benar. *Unbreakable* Cipher dikatakan memiliki tingkat kerahasiaan yang sempurna (*perfect secrecy*).

Kunci kriptografi algoritma *One Time Pad* berisi barisan acak yang ketika disandikan akan menghasilkan plaintext dengan barisan yang sepenuhnya acak. *One time pad* harus menggunakan kunci yang random untuk meningkatkan keamanan dari algoritma *one time pad* cipher.

Metode kriptografi yang menjadi objek penelitian ini adalah kriptografi simetris yaitu *one time pad* cipher. *One time pad* Cipher dipilih karena proses dekripsi satu karakter setiap kali, sedangkan proses enkripsi menggunakan cara *stream* cipher dimana cipher tersebut berasal dari proses pembangkit kunci dari Blum-Blum Shub dan nantinya bilangan acak yang di hasilkan dari blum-blum shub tersebut akan digunakan untuk menggantikan nilai pergeseran pada proses enkripsi aloritma *one time pad* cipher. Algoritma Blum-Blum Shub dipilih karena keamanan Blum-Blum Shub terletak pada sulitnya memfaktorkan n dan menghasilkan bilangan yang tidak mudah diprediksi.

Secara teoritis Blum-Blum Shub termasuk *cryptographically secure pseudorandom generator* (CSPRNG) yang paling mudah dan paling efektif. Blum-Blum Shub(Sianturi, 2020) dibuat pada tahun 1986 oleh Lenore Blum, Manuel Blum, dan Michael Shub. Blum-Blum Shub memiliki bentuk persamaan:

$$X_{n+1} = X_n^2 \ \boldsymbol{mod}\ m$$

Dengan *m* merupakan hasil perkalian dua buah bilangan prima besar p dan q. Dua buah bilangan prima p dan q harus kongruen terhadap 3 mod 4 dan *Greatest Common Divisor* (GCD) harus kecil, karena agar membuat siklus menjadi besar. Generator ini sering digunakan untuk aplikasi kriptografi, karena generator ini tidak begitu cepat.(Parry et al., 1986)

Pada penelitian ini Algoritma Blum-Blum Shub digunakan dalam menentukan implementasi untuk membangkitkan setiap kunci yang akan di gunakan oleh *one time pad chiper*. Untuk menghasilkan implementasi tersebut yang di mulai dengan menentukan *plaintext* dan *ciphertext* untuk mengkonvensi huruf *plaintext* yang di gunakan untuk mengetahui kunci yang digunakan untuk mengenkripsi dan dekripsi setiap kunci yang digunakan. Sehingga pada penelitian ini dilakukan pengimplementasian dari algoritma Blum-Blum Shub ke algoritma *one time pad* cipher.

Berdasarkan uraian yang telah dikemukankan di atas, peneliti tertarik mengkaji lebih dalam penelitian yang berjudul "Implementasi Algoritma Blum-Blum Shub pada Algoritma *One Time Pad* Cipher dalam pengamanan pesan".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah penelitian ini sebagai berikut:

1. Bagaimana proses pembentukan kunci menggunakan algoritma Blum-Blum Shub?
2. Bagaimana *ciphertext* yang dihasilkan dari pesan menggunakan algoritma *one time pad cipher* dengan kunci dari algoritma blum-blum shub?

3. Bagaimana *plaintext* yang dihasilkan dari pesan menggunakan algoritma *one time pad cipher* dengan kunci dari algoritma blum-blum shub?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini sebagai berikut :

1. Untuk mengetahui hasil dari pembentukan kunci menggunakan algoritma Blum- Blum Shub.
2. Untuk mengetahui proses enkripsi implementasi algoritma Blum-Blum Shub pada algoritma *one time pad* cipher dalam pengamanan pesan.
3. Untuk ngetahui proses dekripsi implementasi algoritma Blum-Blum Shub pada algoritma o*ne time pad* cipher dalam pengamanan pesan.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian, peneliti dapat memberikan manfaat kepada siapapun pembaca dan penulis antara lain:

1. Bagi penulis

   Mengetahui cara mengamankan pesan menggunakan Algoritma Blum-Blum Shub yang di implementasikan dengan algoritma *one time pad* Cipher.
2. Bagi Pembaca dan peneliti selanjutnya
   a. Dapat menambah wawasan tenang ilmu kriptografi khususnya *one time pad* Cipher yang di implementasikan dengan algoritma Blum-Blum Shub.
   b. Mengetahui Keamanan pesan dengan menggunakan *one time pad* Cipher yang implementasikan dengan algoritma Blum-Blum Shub.

c. Sebagai referensi bagi peneliti selanjutnya dalam memodifikasi *one time pad* cipher menggunakan algoritma Blum-Blum Shub.

3. Bagi Institusi

a. Sebagai media pembelajaran bagi para mahasiswa khususnya mata kuliah kriptografi.

b. Mengimplementasikan materi khususnya mata kuliah Kriptografi dalam dunia teknologi.

1.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

1. Pengkodean karakter menggunakan table ASCII.
2. Pengurutan posisi suatu pesan dimulai dari 1 hingga jumlah huruf pada pesan.
3. Pengurutan indeks karakter pesan dimulai dari 0 hingga 255.

1.6 Definisi Istilah

Beberapa istilah yang digunakan sebagai berikut:

1. Pesan adalah informasi berupa teks.
2. *Plaintext* adalah teks jelas atau pesan asli yang dapat dipahami.
3. *Ciphertext* adalah suatu pesan yang telah melalui proses enkripsi dan tidak memiliki arti (makna).
4. Enkripsi adalah proses suatu pesan asli yang diubah dengan algoritma tertentu sehingga menjadi kode rahasia yang tidak dimengerti
5. Dekripsi adalah pesan atau kode rahasia yang tidak dapat terbaca diubah menjadi pesan yang dapat dibaca dengan menggunakan algoritma tertentu.

6. Cipher adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi.
7. Bit adalah satuab terkecil dalam system angka biner.

BAB II

KAJIAN TEORI

2.1 Kriptografi

Kriptografi (*cryptography*) yaitu gabungan dari kata *" crypto"* yang artinya *"hidden"* (tersembunyi/rahasia) dan *"graphy"* yang mengacu pada *"writing"* (tulisan), sehingga kriptografi merupakan tulisan yang terahasiakan dan umumnya mengacu pada bagian enkripsi untuk membangun sebuah sistem untuk mengirimkan rahasia. (Amin, 2016)

Kriptografi merupakan ilmu dan seni yang mempelajari bagaimana memproteksi pesan yang akan disampaikan menjadi lebih aman dengan sistem mengubah pesan menjadi bentuk yang tidak dapat diketahui. *Plaintext* merupakan teks yang asli dan dapat dibaca serta dapat diketahui maknanya. *Ciphertext* merupakan teks yang tidak dapat dibaca dan tidak dapat diketahui maknanya. Terdapat dua proses utama pada kriptografi yaitu sebagai berikut :

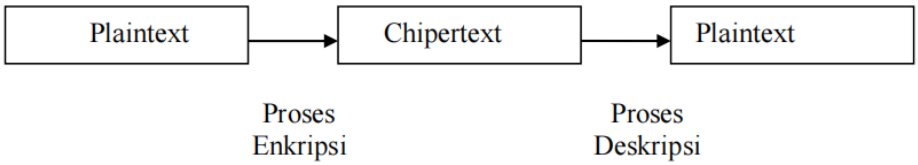
1. Enkripsi

   Enkripsi merupakan proses pengubahan *plaintext* dengan menggunakan kunci yang telah ditentukan menjadi ciphertext. Proses diubahnya data atau pesan yang hendak dikirim menjadi bentuk yang hampir tidak dikenali oleh pihak ketiga.

2. Dekripsi

   Dekripsi merupakan proses pengembalian ciphertext dengan menggunakan kunci yang sama pada enkripsi menjadi *plaintext*. Proses mengubah data atau pesan kembali kebentuk semula sehingga data atau pesan dapat

tersampaikan dan dimengerti oleh penerima. Pada Gambar 2.1 merupakan skema proses enkripsi dan dekripsi yang digunakan dalam pengiriman pesan.



Gambar 2.1 Enkripsi dan Dekripsi dalam Pengiriman Pesan

2.1.1 Tujuan Kriptografi

Menurut (Setyaningsih, 2015) beberapa dari tujuan kriptografi adalah sebagai berikut:

1. Kerahasiaan (*confidentiality*) yaitu layanan perlindungan agar pesan yang dikirim tidak dapat dibaca oleh pihak-pihak yang tidak bertanggungjawab. Secara umum *confidentiality* dilakukan dengan aturan membuat suatu algoritma matematis tertentu yang dapat mengubah data hingga sulit ntuk dimengerti.
2. Integritas data (*data integrity*) merupakan layanan yang dapat mendeteksi adanya pesan masih dikatakan asli atau belum pernah dimanipulasi selama masa pengiriman.
3. Otentikasi (*authentication*) adalah layanan penerima pesan yang dapat memastikan keaslian pengirimannya. Penyerang tidak dapat berpura-pura sebagai orang lain.
4. Penyangkalan (*Non-repudiation*) adalah layanan yang dapat mencegah pembuktian bahwa pengirim tidak dapat menyangkal bahwa pengirim telah

mengirim pesan, dan penerima juga tidak dapat menyangkal bahwa penerima telah menerima pesan.

2.1.2 Komponen Kriptografi

Di dalam kriptografi, akan sering ditemukan berbagai istilah atau terminologi. Berikut adalah beberapa istilah yang penting untuk diketahui.

1. *Plaintext* dan *Ciphertext.*

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (*plaintext*) atau teks-jelas (*cleartext*). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (*ciphertext*) atau kriptogram (*cryptogram*). Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca.

2. Pengirim dan Penerima

   Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas di sini dapat berupa orang, mesin (komputer), kartu kredit, dan sebagainya.

3. Enkripsi dan dekripsi

   Enkripsi (*encryption*) merupakan proses menyandikan plainteks menjadi cipherteks. Sedangkan, proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi (*decryption*).

4. Kriptanalis dan Kriptologi

   Kriptanalis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks, tanpa memerlukan kunci yang digunakan.

Pelakunya disebut dengan *cryptanalyst*. Kriptanalis berusaha memecahkan cipherteks tersebut untuk menemukan *plaintext* atau *key*. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalis.

2.1.3 Jenis algoritma Kriptografi

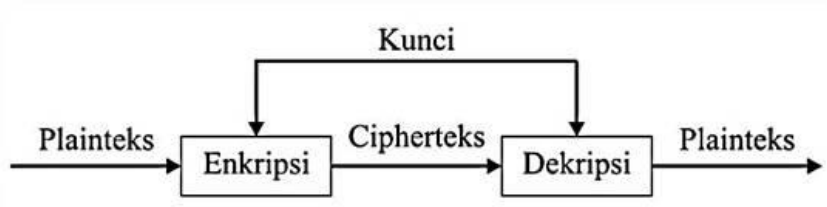
Berdasarkan perkembangannya, kriptografi terbagi atas dua jeis yaitu kriptografi modern dan kriptografi klasik. Kriptografi modern terbagi menjadi dua jenis yaitu simetris dan asimetris. Kriptografi klasik terbagi menjadi dua jenis yaitu substitusi dan transposisi.

2.1.4 Algoritma Kriptografi Modern

Secara umum ada dua jenis kriptografi berdasarkan kuncinya, yaitu: algoritma simetris dan algoritma asimetris.

1. Algoritma Simetris

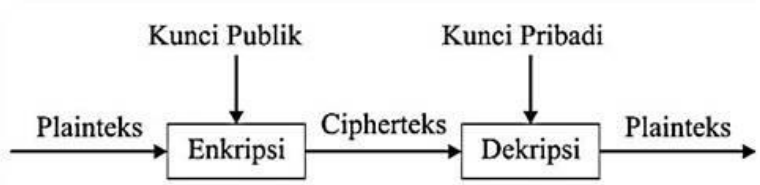
   Algoritma simetris adalah algoritma yang mempergunakan kunci yang sama dalam proses enkripsi dan dekripsinya. Aplikasi kriptografi simetri yang utama adalah melindungi kerahasiaan data yang dikirim melalui saluran tidak aman dan melindungi kerahasiaan data yang disimpan pada media yang tidak aman. Kelemahan dari sistem ini adalah baik pengirim maupun penerima pesan harus memiliki kunci yang sama, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahukan kunci kepada penerima pesan (Munir, 2006). Contoh algoritma kriptografi simetris adalah DES, *Beaufort Cipher, Twofish, AES (Rijndael), Blowfish, GOST*, dan lain-lain.



Gambar 2.1 Proses Skema Kriptografi Simetri

2. Algoritma Asimetris

Algoritma Asimetris adalah algoritma kriptografi yang mempergunakan kunci yang berbeda pada enkripsi dan dekripsinya. Pada kriptografi asimetris kunci untuk enkripsi tidak rahasia dan dapat diketahui siapapun (diumumkan ke publik), sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan (karena itu rahasia). Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan (*receiver*). Hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri (Munir, 2006). Algoritma yang termasuk dalam algoritma asimetri adalahRSA, RSA-CRT, Elgamal, DSA, dsb. Skema kriptografi asimetri dapat dilihat pada gambar di bawah ini.



Gambar 2.2 Proses Skema Kriptografi Asimetri

Algoritma simetris dan asimetris memiliki keunggulan tersendiri dari masing-masing konsep kerjanya. Pada algoritma simetris, kecepatan

operasi enkripsi dan dekripsi lebih tinggi dan ukuran kuncinya juga relatif pendek bila dibandingkan dengan algoritma asimetris. Namun algoritma asimetris memiliki manajemen kunci yang lebih baik. Tidak seperti algoritma simetris yang harus sering mengubah kunci setiap kali melaksanakan komunikasi, pasangan kunci privat dan kunci publik pada algoritma asimetris tidak perlu diubah dalam jangka waktu yang sangat lama (Bakir & Hozairi, 2018).

2.1.5 Algoritma Kriptografi Klasik

Kriptografi klasik adalah algoritma yang sudah digunakan pada sejak zaman dahulu sebelum ditemukannya komputer. Kriptografi klasik dilakukan dengan cara mengacak huruf pada plaintext. Pada dasarnya kriptografi klasik dapat dikelompokkan menjadi dua macam cipher, yaitu sebagai berikut:

1. Cipher Substitusi

   Cipher Substitusi adalah algoritma kriptografi yang mengubah sebuah karakter pada *plaintext* dengan sebuah karakter *ciphertext* (Setyaningsih, 2015). Cipher substitusi mempunyai berbagai macam algoritma yang berbeda-beda seperti *Vigenere* Cipher, *Caesar* Cipher, *One Time Pad* Cipher dan *Playfair* Cipher.

2. Cipher Transposisi

   Cipher Transposisi adalah mengubah urutan huruf *plaintext* atau melakukan transpose terhadap rangkaian karakter (Setyaningsih, 2015). Ciphertransposisi mempunyai berbagai macam algoritma yang berbeda-beda seperti *Rail Fence* Cipher, *Myszkowski Transposition*, *Route Cipher, Columnar Transposition.*

2.2 Teori Bilangan

Teori bilangan (*number theory*) merupakan teori yang paling umum untuk memahami algoritma kriptografi. Bilangan yang dimaksudkan adalah bilangan bulat (*integer*).

2.2.1 Aritmatika Modulo

Aritmatika modulo menjadi dasar dan memainkan peran penting dalam komputasi bilangan bulat. Aritmatika digunakan pada operasi aritmatika dengan tujuan agar menghasilkan nilai integer pada ruang lingkup yang sama (Munir,2010). Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi a *mod* m (dibaca "*a modulo m*") memberikan sisa jika a dibagi dengan m. Notasi $a \; mod$ m $=$ r sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$ Bilangan m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0,1,2, \ldots, m-1\}$.

Contoh 2.1.

Beberapa hasil operasi dengan oprator modulo:

1. $23 \; mod \; 5 = 3 \qquad (23 = 5.4 + 3)$
2. $27 \; mod \; 3 = 0 \qquad (27 = 3.9 + 0)$
3. $6 \; mod \; 8 = 6 \qquad (6 = 8.0 + 6)$
4. $0 \; mod \; 12 = 0 \qquad (0 = 12.0 + 0)$
5. $-41 \; mod \; 9 = 4 \qquad (-41 = 9(-5) + 4)$
6. $-39 \; mod \; 13 = 0 \qquad (-39 = 13(-3) + 0)$

Penjelasan (v): Karena a negatif, bagi $|a|$ dengan m mendapatkan sisa r'. Maka a mod $m = m - r'$ bila r' $\neq$ 0 . Jadi $|-41| mod \; 9 = 5$, sehingga $-41 \; mod \; 9 = 9 - 5 = 4$.

2.2.2 Kongruen

Ditentukan p, q, m adalah bilangan-bilangan bulat dan $\neq 0$, p disebut kongruen dengan q modulo m, ditulis $p \equiv q(mod\, m)$, jika dan hanya jika $m|p-q$, Misalnya $38\ mod\ 5 = 3\ dan\ 13\ mod\ 5 = 3$,maka kita katakan $38 \equiv 13\ (mod\ 5)$(baca: 38 kongruen dengan 13 dalam modulo 5). Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b(mod\, m)$ jika m habis membagi $a-b$. Jika a tidak kongruen dengan b dalam modulus m, maka ditulis $a \equiv /b(mod\, m)$.

Contoh 2.2.

$17 \equiv 2(mod\ 3)$ (3 habis membagi $17-2=15$)

$-7 \equiv 15(mod\ 11)$ (11 habis membagi $-7-15=-22$)

$12 \equiv /2(mod\ 7)$ (7 tidak habis membagi $12-2=10$)

$-7 \equiv /15(mod\ 3)$ (3 tidak habis membagi $-7-15=-22$)

Contoh 2.3.

$17 \equiv 2\ (mod\ 3)$ dapat ditulis sebagai $17 = 2 + 5 \cdot 3$

$-7 \equiv 15\ (mod\ 11)$ dapat ditulis sebagai $-7 = 15 + (-2)11$

Berdasarkan definisi aritmatika modulo, kita dapat menuliskan $a\ mod\ m = r$ sebagai $a \equiv r(mod\, m)$

Contoh 2.4.

Beberapa hasil operasi dengan operator modulo berikut:

1. $23\ mod\ 5 = 3$ dapat ditulis sebagai $23 \equiv 3(mod\ 5)$
2. $27\ mod\ 3 = 0$ dapat ditulis sebagai $27 \equiv 0(mod\ 3)$
3. $6\ mod\ 8 = 6$ dapat ditulis sebagai $6 \equiv 6(mod\ 8)$
4. $0\ mod\ 12 = 0$ dapat dituliskan sebagai $0 \equiv 0(mod\ 12)$

5. $-41\ mod\ 9\ = 4$ dapat dituliskan sebagai $-41 \equiv 4\ (mod\ 9)$

6. $39\ mod\ 13\ = 0$ dapat dituliskan sebagai $-39 \equiv 0(mod\ 13)$

Teorema 2.1

Misalkan m adalah bilangan bulat positif.

1. Jika $a\ \equiv b(mod\ m)$ dan c adalah sembarang bilangan bulat maka

   a. $(a + c) \equiv (b + c)(mod\ m)$

   b. $ac \equiv bc(mod\ m)$

   c. $ap\ \equiv bp\ (mod\ m)$ untuk suatu bilangan bulat tak negative p.

2. Jika $a\ \equiv b(mod\ m)$ dan $c \equiv d(mod\ m)$, maka

   a. $(a + b) \equiv (b + d)(mod\ m)$

   b. $ac \equiv bd(mod\ m)$

Bukti (hanya untuk 1 (b) dan 2(a) saja):

1(b) $a \equiv b\ (mod\ m)$ berarti:

$\Leftrightarrow a = b + km$

$\Leftrightarrow a - b = km$

$\Leftrightarrow (a - b)c = ckm$

$\Leftrightarrow ac = bc + km$

$\Leftrightarrow ac \equiv bc(mod\ m)$

2(i) $a \equiv b(mod\ m) \Leftrightarrow a = b + k_1 m$

$c\ \equiv (mod\ m)\ \Leftrightarrow c = d +\ k_2 m$

$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$

$\Leftrightarrow (a + c) = (b + d) + km(k = k_1 + k_2)$

$\Leftrightarrow (a + c) = (b + d)(mod\ m)$

Contoh 2.5.

Misalkan $17 \equiv 2(mod\ 3) dan\ 10 \equiv 4(mod\ 3)$, maka menurut Teorema 2.1:

$$17 + 5 = 2 + 5(mod\ 3) \quad \Leftrightarrow \quad 22 = 7(mod\ 3)$$

$$17.5 = 5.2(mod\ 3) \quad \Leftrightarrow \quad 85 = 10(mod\ 3)$$

$$17 + 10 = 2 + 4(mod\ 3) \quad \Leftrightarrow \quad 27 = 6(mod\ 3)$$

$$17.10 = 2.4(mod\ 3) \quad \Leftrightarrow \quad 170 = 8(mod\ 3)$$

Perhatikan bahwa teorema 2.1 tidak memasukkan operasi pembagian pada aritmatika modulo karena jika kedua ruas dibagi dengan bilangan bulat, maka kekongruenan tidak selalu dipenuhi. Misalnya:

1. $10 \equiv 4(mod\ 3)$ dapat dibagi dengan 2 karena 10/2=5 dan 4/2=2, dan $5 \equiv 2(mod\ 3)$
2. $14 \equiv 8(mod\ 6)$ tidak dapat dibagi dengan 2, karena 14/2=7 dan 8/2=4, tetapi $7 \equiv /4(mod\ 6)$.

2.2.3 Balikan Modulo (Modulo Invers)

Jika a dan m relatif prima dan $m > 1$, maka kita dapat menemukan balikan (invers) dari $a\ modulo\ m$. Balikan dari a modulo m adalah bilangan bulat a sedemikian sehingga

$$aa \equiv 1(mod\ m).$$

Bukti:

Dari definisi relatif prima diketahui bahwa FPB $(a, m) = 1$, dan menurut persamaan (2) terdapat bilangan bulat $p\ dan\ q$ sedemikian sehingga

$$pa + qm = 1$$

Yang mengimplikasikan bahwa

$$pa + qm \equiv 1(mod\ m)$$

Karena $qm \equiv 0(mod\ m), maka$

$$pa \equiv 1(mod\ m)$$

Kekongruenan yang terakhir ini berarti bahwa p adalah balikan dari $a\ modulo\ m$. Pembuktian di atas juga menceritakan bahwa untuk mencari balikan modulo dari $a\ modulo\ m$, kita harus membuat kombinasi lanjar dari $a\ dan\ m$ sama dengan 1. Koefisien a dari kombinasi lanjar tersebut merupakan balikan dari $a\ modulo\ m$.2.2.2 Aritmatika Modulo dan Kriptografi Aritmatika modulo cocok digunakan untuk kriptografi karena dua alasan:

1. Oleh karena nilai-nilai aritmatika modulo berada dalam himpunan berhingga (0 sampai modulus m-1), maka kita tidak perlu khawatir hasil perhitungan berada di luar himpunan.
2. Karena kita bekerja dengan bilangan bulat, maka tidak khawatir kehilangan informasi akibat pembulatan (*round off*) sebagaimana pada operasi bilangan rill.

2.3 Algoritma One Time Pad Cipher

Algoritma *One Time Pad* Cipher adalah sebuah metode yang menerapkan algoritma kunci simetris atau proses enkripsi dan dekripsi menggunakan kunci yang acak. Kerahasiaan kunci merupakan faktor utama dalam penentuan keamanan atau pesan yang dikirimkan. Algoritma *One Time Pad* Cipher diciptakan oleh Mayor J. Maugboune dan Gilbert Vernam pada tahun 1917. Algoritma *One Time Pad* Cipher juga bisa disebut dengan algoritma Unbreakable Cipher. Hal ini dikarenakan sifat dari algoritma ini kunci harus berupa barisan nilai yang seluruhnya acak sempurna (*truly random*) dan juga panjang dari kunci algoritma ini haruslah sama dengan panjang plainteks nya.(Harahap & Khairina, 2018) Dari sifat-sifat yang ada pada

algoritma *One Time Pad* ini menyebabkan beberapa plainteks yang sama belum tentu bisa dienkripsi menjadi cipherteks yang sama pula. Maksudnya adalah kriptanalis akan mendapatkan hasil bahwa sebuah cipherteks yang didekripsinya mungkin menghasilkan beberapa plainteks berbeda namun memiliki makna. Hal ini akan membingungkannya dalam menentukan plainteks mana yang benar. *Unbreakable* Cipher dikatakan memiliki tingkat kerahasiaan yang sempurna (*perfect secrecy*). Satu-satunya algoritma kriptografi sempurna aman dan tidak dapat dipecahkan adalah *One Time Pad* Cipher.

Algoritma *One Time Pad* adalah stream cipher yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Algoritma ini merupakan perbaikan dari *Vernamcipher* untuk menghasilkan keamanan yang sempurna. Cipher ini termasuk ke dalam kelompok algoritma kriptografi simetri. *One Time Pad* (*pad* = kertas *bloknot*) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Satu buah *One Time Pad* adalah sebuah pita (*tape*) yang berisi barisan karakter-karakter kunci. Satu pad hanya digunakan sekali (*one time*) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain. Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada *plaintext* dengan satu karakter pada kunci. Oleh karena itu, panjang kunci harus sama dengan panjang *plaintext.* Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 (menggunakan kode ASCII) dari satu bit *ciphertext* dengan satu bit kunci.

Contoh penerapan:

1. Karakter pembentuk *plaintext* dan *ciphertext* yang digunakan adalah seluruh abjad romawi yaitu 26 huruf (A-Z) dengan nomer *index* karakter 0-25, maka nilai modulus yang digunakan modulo 26.
2. Dilakukan proses enkripsi dengan operasi matematika penjumlahan, sementara untuk dekripsi menggunakan operasi matematikapenjumlahan, sementara untuk dekripsi menggunakan operasi matematika pengurangan. Penggunaan *One Time Pad* berikut yang digunakan yaitu menggunakan table ASCII, berikut merupakan table ASCII.

Aturan enkripsi yang digunakan pada algoritma *One Time Pad* Cipher sangatlah persis dengan aturan enkripsi pada algoritma *Vignere* Cipher. Pengirim pesan menggunakan setiap karakter kunci untuk mengenkripsikan satu karakter plainteks. Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci *One Time Pad*. Berikut persamaan dari enkripsi *One Time Pad* yaitu:

$$C_i = (P_i + K_i) mod\ 26 \quad (1)$$

Yang dalam hal ini, pi adalah plainteks ke-i, k_i adalah huruf kunci ke-i dan c_i adalah huruf cipherteks ke-i Perhatikan bahwa panjang kunci sama dengan panjang plainteks, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama enkripsi. Setelah pengirim mengenkripsi pesan dengan kunci, i menghancurkan kunci tersebut (makanya disebut satu kali pakai atau *One Time Pad*). Penerima pesan menggunakan kunci yang sama untuk mendeskripsikan karakter-karakter cipherteks menjadi karakter-karakter dan persamaan dekripsi dari *One Time Pad* yaitu:

$$C_i = (P_i + K_i) mod\ 26 \quad (2)$$

Keterangan persamaan:

C_i = Pergeseran karakter pada cipherteks (*Ciphertext*),

P_i = Pergeseran karakter pada plainteks *(Plaintext*),

K_i = Kunci dalam bentuk desimal yang dihasilkan dari table konversi.

Dimana P_i adalah rangkaian *plaintext*, K_i adalah kunci, C_i adalah *ciphertext* yang diperoleh dan n adalah jumlah karakter yang digunakan. Kunci yang digunakan pada algoritma *One Time Pad* diambil secara acak dan harus memiliki panjang karakter yang sama dengan plaintext (Maulana & Ibrahim, 2020).

Contoh 2.6

Pesan asli yang akan dikirimkan adalah "ONEPAD" dengan kunci "TBFRGM" dengan asumsi A = 0, B = 1, …, Z = 25 yang berarti nilai modulo nya adalah 26. Maka proses enkripsi pesan sebagai berikut:

$$O + T(mod\ 26) = 14 + 19\ (mod\ 26) = 7 = H$$

$$N + B(mod\ 26) = 13 + 1\ (mod\ 26) = 14 = O$$

$$E + F(mod\ 26) = 4 + 5\ (mod\ 26) = 9 = J$$

$$P + R(mod\ 26) = 15 + 17\ (mod\ 26) = 6 = G$$

$$A + G(mod\ 26) = 0 + 6\ (mod\ 26) = 6 = G$$

$$D + M(mod\ 26) = 3 + 12\ (mod\ 26) = 15 = P$$

Sehingga, didapatkan ciphertext "HOJGGP". Sedangkan untuk proses dekripsi pesan sebagai berikut:

$$H - T(mod\ 26) = 33 - 19(mod\ 26) = 14 = O$$

$$O - B(mod\ 26) = 14 - 1(mod\ 26) = 13 = N$$

$$J - F(mod\ 26) = 9 - 5(mod\ 26) = 4 = E$$

$$G - R(mod\ 26) = 32 - 17(mod\ 26) = 15 = P$$

$$G - G(mod\ 26) = 6 - 6\ (mod\ 26) = 0 = A$$

$$P - M(mod\ 26) = 15 - 12(mod\ 26) = 3 = D$$

Sehingga, didapatkan plaintext "ONEPAD'' Mendekripsikan suatu chipertext dengan menggunakan kunci yang berbeda akan menghasilkan plaintext yang berbeda pula, misalnya dari chiperteks diatas kita ambil kunci yang berbeda yakni "POYUSC", maka proses dekripsinya sebagai berikut:

$$H - P(mod\ 26) = 33 - 15(mod\ 26) = 18 = S$$

$$O - O(mod\ 26) = 14 - 14(mod\ 26) = 0 = A$$

$$J - Y(mod\ 26) = 35 - 24(mod\ 26) = 11 = L$$

$$G - U(mod\ 26) = 32 - 20(mod\ 26) = 12 = M$$

$$G - S(mod\ 26) = 32 - 18(mod\ 26) = 14 = O$$

$$P - C(mod\ 26) = 15 - 2(mod\ 26) = 13 = N$$

Didapatkan plaintext "SALMON", plaintext tersebut memiliki makna, sehingga hal ini dapat memicu kebingungan kriptanalis dalam menentukan plaintext mana yang benar. Hal inilah yang menjadi salah satu kelebihan dari

algoritma OTP. Contoh OTP dalam kehidupan sehari hari antara lain yaitu untuk verifikasi nomer telpon, pemulihan akun dan konfirmasi pembayaran.

2.4 Algoritma Blum-Blum Shub

Secara teoritis algoritma Blum-Blum Shub (BBS) termasuk *cryptographically secure pseudorandom generator* (CSPRNG) yang paling mudah dan paling efektif. Blum-Blum Shub(Sianturi, 2020) dibuat pada tahun 1986 oleh Lenore Blum, Manuel Blum, dan Michael Shub. Blum-Blum Shub memiliki bentuk persamaan:

$$X_{n+1} = X_n^2 \ \boldsymbol{mod}\ m$$

Dengan *m* merupakan hasil perkalian dua buah bilangan prima besar p dan q, serta output-nya dalam *Least Significant Bit* dari x_n dimana hal yang sama sebagai parity dari x_n. Dua buah bilangan prima p dan q harus kongruen terhadap 3 mod 4 dan *Greatest Common Divisor* (GCD) harus kecil. Generator ini sering digunakan untuk aplikasi kriptografi, karena generator ini tidak begitu cepat.(Parry et al., 1986)

Untuk membangkitkan bilangan acak dengan Blum-Blum Shub, algoritmanya adalah sebagai berikut (Munir, 2019):

1. Pilih dua buah bilangan prima rahasia p dan q, yang masing-masing kongruen dengan 3 (mod 4) (semakin besar bilangan prima tersebut maka semakin sulit dipecahkan oleh kriptanalis).
2. Kalikan keduanya menjadi $n = pq$. Bilangan n disebut bilangan bulat Blum-Blum Shub.
3. Pilih bilangan bulat acak lain s sebagai umpan dengan syarat:
   a. $2 \leq s < n$

b. s dan n adalah bilangan yang relatif prima.

Kemudian hitung $x_0 = s^2 (mod\ n)$

Barisan bit acak dihasilkan dengan melakukan iterasi berikut sepanjang yang diinginkan:

a. Hitung $x_i = x_{(i-1)^2} (mod\ n)$

b. $z_i = LSB(Least\ Significant\ Bit)$ dari x_i

Barisan bit acak yang dihasilkan adalah $z_1, z_2, z_3, ...$

Bilangan acak tidak harus satu *least significant bit* tetapi bisa juga j buah bit (j adalah bilangan bulat positif yang tidak melebihi ($log_2(log_2\ n)$) . Nilai n disebut kunci publik dimana kunci tersebut dapat diumumkan kepada publik. Blum-Blum Shub tidak dapat diprediksi dari arah manapun, artinya jika diberikan barisan bit kriptanalis tidak dapat memprediksi barisan bit sebelumnya dan barisan bit sesudahnya.(Nguyen & Lee, 2016)

Contoh 2.7

Misalkan nilai $p = 11$ dan $q = 19$ sehingga nilai $n = pq = 209$.menghitung nilai $x_0 = s^2\ mod\ n$. Nilai s yang di pilih yaitu $s = 3$ jadi nilai $x_0 = 3^2 mod\ 209 = 9$ Sehingga membentuk bilangan acak dari $x_i = x_{(i-1)^2}$ jadi,

$$x_1 = 9^2\ mod\ 209 = 81$$

$$x_2 = 81^2 mod\ 209 = 82$$

$$x_3 = 82^2 mod\ 209 = 36$$

$$x_4 = 36^2 mod\ 209 = 42$$

$$x_5 = 42^2 mod\ 209 = 92$$

$$x_6 = 92^2 mod\ 209 = 104$$

$$x_7 = 104^2 mod\ 209 = 157$$

$$x_8 = 157^2 mod\ 209 = \ 196$$

Terdapat kunci hasil pembangkitan kunci menggunakan algoritma Blum-Blum Shub di atas

Tabel 2.1 Hasil Pembangkit Kunci dari algoritma Blum-Blum Shub

Kunci biner	Bilangan acak	Hasil gabungan LSB	Decimal	Karakter
x_1	81	10100010	162	¢
x_2	82	10100100	164	¤
x_3	36	10010000	144	
x_4	42	10101000	168	¨
x_5	92	10111000	184	¸
x_6	104	11010000	208	Ð
x_7	157	10011101	157	
x_8	196	11000100	196	Ä

2.5 Least *Significant Bit*

LSB (*Least Significant Bit)* adalah bagian data dari sebagian data biner yang mempunyai nilai paling kecil dan letak posisinya nilai paling kecil dan letak posisinya pada barisan bit paling kanan. Pada berkas file gambar yang berektensi *bitmap* 24-bit dan setiap *pixel* tersusun dari tiga warna merah, hijau dan biru (RGB).(Bakir & Hozairi, 2018) Masing-masing susunan terdapat bilangan 8bit yang dimulai dari 0 sampai 255 yaitu menggunakan bilangan biner 00000000 sampai 11111111. Setiap *pixel* pada berkas gambar *bitmap* 24 bit dapat kita lakukan penyisipan 3bit data. Metode ini menyembunyikan pesan rahasia dengan cara menambahkan bit- bit pesan yang akan disembunyikan ke akhir file citra penampung (Gunawan, 2018) Proses penyisipan pesan dengan metode Least Significant Bit dapat dituliskan dalam algoritma sebagai berikut:

1. Inputkan pesan yang akan disisipkan
2. Ubah pesan menjadi kode-kode desimal.

3. Inputkan citra grayscale yang akan disisipi pesan.
4. Dapatkan nilai derajat keabuan masingmasing piksel.
5. Tambahkan kode desimal pesan sebagai nilai derajat keabuan citra.
6. Petakan menjadi citra baru

2.6 Kajian Integritas Topik dengan Al-Quran dan Hadits

Pada BAB I subbab 1.1 telah dijelaskan mengenai ayat Al-Qur'an yang berkaitan dengan pengmanan pesan yaitu tentang amanah pada QS. Al- Zalzalah 7-8 beserta dengan tafsir nya. Pada subbab ini akan dijelaskan kaitan dari algoritma yang di jelaskan dengan kajian ataupun surah yang di bahas.

Algoritma blum-blum shub merupakan algoritma suatu sebuah pembangkit bilangan acak semu (*pseudo random generator*) yang aman secara kriptografi. BBS menggunakan fungsi yang berpacu pada dua buah bilangan prima rahasia, yang masing-masing dari bilangan tersebut kongruen dengan 3 modulo 4. Sehingga pada algoritma ini mempunyai beberapa tahapan untuk mencari bilangan acak baru antara lain memulai dengan mencari bilangan acak baru, setelah itu mencari nilai bilangan acak tersebut sehingga menghasilan kunci baru. Pada tahapan ini dapat di perumpamakan seperti surah al-zalzalah ayat 7 dan 8 yang memiliki arti:

"Siapa yang mengerjakan kebaikan seberat zarah, dia akan melihat (balasan)-nya (7). Siapa yang mengerjakan kejahatan seberat zarah, dia akan melihat (balasan)-nya." (Q.S. Al-Zalzalah: 7-8)

Sehingga melalui ayat ini, Allah SWT coba jelaskan perlakuan adil-Nya terhadap seluruh manusia. Di mana masing-masing amal meski sedikit atau kecil yang mereka kerjakan sungguh akan menerima ganjarannya. Seperti halnya, seorang yang menganggap perbuatan baiknya tak seberapa, tapi di mata Allah SWT hal sekecil itu tetap memberikan pahala bagi si pelaku. Begitu pula dengan orang

yang meremehkan segelintir aksi kejinya, di mata-Nya itu tetaplah dosa yang mampu memasukkan pelaku ke neraka.

Pada hadits lain riwayat Abu Hurairah, Rasul SAW juga coba terangkan perihal amal yang dilakukan dengan ikhlas mengharap ridha Allah SWT akan memberi balasan meski dianggap sederhana. Tafsir Ibnu Katsir Jilid 15(Ghoffar, 2000), berikut sabda Nabi SAW:

"Kuda itu untuk tiga orang. Bagi seseorang kuda itu akan menjadi pahala, bagi seorang lagi akan menjadi satar (penutup), dan bagi seorang yang lainnya akan menjadi dosa.

Adapun orang yang mendapatkan pahala adalah orang yang mengikat kuda itu di jalan Allah SWT, lalu dia membiarkannya di tempat penggembalaan atau taman dalam waktu yang lama, maka apa terjadi selama masa penggembalaannya di tempat penggembalaan dan taman itu, maka itu akan menjadi kebaikan baginya.

Dan jika dia menghentikan masa penggembalaannya lalu kuda itu melangkah satu atau dua langkah, maka jejak kaki dan juga kotorannya akan menjadi kebaikan baginya. Dan jika kuda itu menyeberangi sungai lalu ia minum air dari sungai tersebut, maka yang demikian itu menjadi kebaikan baginya, dan kuda itu pun bagi orang tersebut adalah pahala.

Dan orang yang mengikat kuda itu karena untuk memperkaya diri dan demi kehormatan diri tetapi dia tidak lupa hak Allah SWT dalam pemeliharaannya, maka kuda itu akan menjadi satar baginya. Serta orang yang mengikatnya karena perasaan bangga dan riya, maka ia hanya akan menjadi dosa baginya." (HR Muslim)(Materi et al., n.d.)

Dalam ayat dan hadits tersebut dapat dilihat bagaimana proses untuk mendapatkan pahala dari allah kita dapat melihat berapa tahapan tahapan seperti pada algoritma blum-blum shub bahwa ada tahapan-tahapan untuk mencari kunci acak lalu menenkripsi dan dekripsi suatu bilangan acak tersebut menggunakan metode OTP untuk bisa membaca kunci yang sudah di ubah di algoritma blum-blum shub dengan mendekripsi pesan.

Ayat yang di bahas seperti perumpamaan manusia tidak tahu apa yang di lakukan memiliki ganjaran walaupun itu sekecil atom. Sama hal nya kita tidak tau bagai mana algoritma ini bekerja untuk meyelesakan kunci acak tersebut hingga bisa terbaca. Maka dari itu kita dapat mengetahui bagimana tahapan allah memberi ganjaran untuk setiap hambanya.

2.7 Kajian Topik Dengan Teori Pendukung

Penelitian ini disusun menggunakan beberapa teori pendukung, seperti *One Time Pad Cipher* yang termasuk kedalam kriptografi simetris. *One Time Pad Cipher* adalah sebuah metode yang menggunakan algoritma kunci simetris atau proses enkripsi dan dekripsi menggunakan kunci yang acak. Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasi masing-masing karakter pada *plaintext* dengan satu karakter pada kunci. Oleh karena itu, panjang kunci harus sama dengan panjang *plaintext.* Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26(menggunakan kode ASCII) dari satu bit *ciphertext* dengan satu bit kunci.

Tetapi sebelum mengenkripsi dan dekripsi dengan menggunakan *Onetime Pad Cipher* kita perlu mencari bilangan acak dengan menggunakan algoritma blum-blum shub dimana pada algoritma ini membangkitkan bilangan acak dengan algoritma blum-blum shub. Pada blum-blum shub bilangan acak tidak harus satu

Least Significant Bit tetapi bisa juga *j* buah bit (*j* adalah bilangan bilat positif yang tidak melebihi ($\log_2(\log_2 n)$). Blum-blum shub tidak dapat diprediksi dari arah manapun, artinya jika diberikan barisan bit kriptanalis tidak dapat memprediksi barisan bit sebelumnya dan barisan bit sesudahnya.

Dalam penelitian ini algoritma blum-blum shub digunakan untuk mengimplementasikan kunci-kunci yang akan digunakan untuk mengenkripsi dan mendekripsi algoritma one time pad cipher sehingga keterhubungan antar algoritma dibutuhkan dalam penyelesaian penelitian ini. Dalam algoritma blum- blum terdapat berberapa tahapan untuk mengubah kunci yang di gunakan oleh one time pad cipher.

Berdasarkan uraian diatas, kajian topik dengan teori pendukung saling berhubungan untuk memudahkan penelitian. Teori pendukung juga sebagai bekal untuk menuju ke pembahasan penelitian. Oleh sebab itu, maka pada kajian teori penduung implementasi algoritma *One Time Pad Cipher* dengan algoritma blum-blum shub dalam pengamanan pesan dapat membantu penelitian selanjutnya.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kualitatif yaitu penelitian yang menghasilkan penemuan-penemuan yang tidak dapat diperoleh dengan menggunakan prosedur-prosedur statistik atau cara-cara lain dari kuantifikasi (pengukuran). Penelitian kualitatif antara lain bertujuan untuk memperoleh pemahaman yang lebih mendalam dengan mengembangkan teori. Penelitian ini menggunakan studi literatur yang berkaitan dengan apa yang diteliti, seperti buku, skripsi dan artikel jurnal.

3.2 Pra Penelitian

Proses pra penelitian ini diawali dengan mencari referensi penelitian mengenai kelemahan algoritma Blum-Blum Shub dan algoritma *one time pad cipher* peneliti mencari sumber penelitian dari jurnal, artikel, buku yang relevan serta semacamnya. Kemudian, peneliti menganalisis suatu masalah untuk mendapatkan algoritma yang sesuai. Selanjutnya, peneliti merancang algoritma yang akan digunakan pada proses penelitian selanjutnya.

3.3 Tahapan Penelitian

Penelitian ini memiliki tiga tahapan di antaranya tahap implementasi, tahap enkripsi dan tahap dekripsi, di mana pada tahap implementasi blum-blum shub dibangkitkan agar menghasikan bilangan acak yang nantinya digunakan untuk membangkitkan kunci-kunci di OTP dan pada tahap enkripsi mengubah *plaintext* menjadi *ciphertext.* Sedangkan, tahap dekripsi mengubah *ciphertext* menjadi

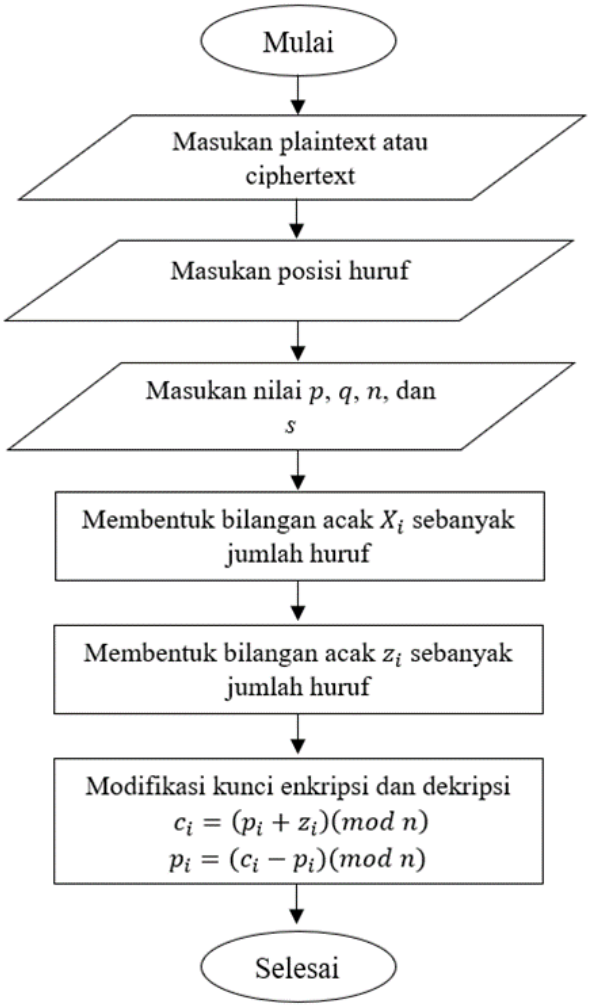
plaintext. Berikut langkah-langkah yang digunakan pada tahap penelitian implementasi *onetime pad* cipher menggunakan algoritma blum-blum shub:

1. Proses Pembentukan Kunci menggunakan Blum-Blum Shub:
    a. Menentukan *plaintext* atau *ciphertext* serta mengkonvensi huruf *plaintex*t ke decimal ASCII tersebut.
    b. Menentukan nilai p dan q, kemudian kalikan keduanya sehingga menghasilkan nilai n.
    c. Mentukan nilai s *(seed)*$x_0 = s^2 (\ mod\ n)$
    d. Membentuk bilangan acak $x_i = x_{i-1^2} (mod\ n)$ dan lakukan iterasi sebanyak jumlah posisi huruf *plaintex*Menentukan hasil gabungan LSB dari bilangan acak.
    e. Membentuk bilangan decimal baru untuk menjadi bilangan acak baru z_i
    f. Melakukan implementasi kunci enkripsi dan kunci dekripsi *One Time Pad Cipher* dengan mengubah nilai k_i menjadi z_i.
    g. Implementasi kunci enkripsi *One Time Pad Cipher*:

$$c_i = (p_i + z_i)(mod\ n)$$

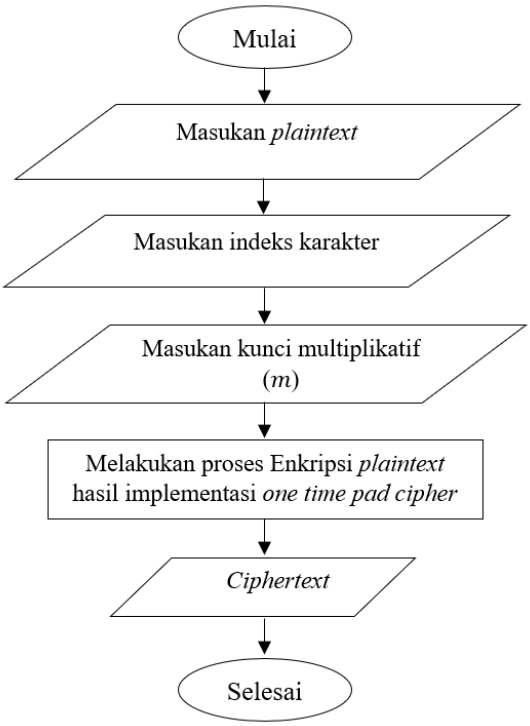
    h. Implementasi kunci dekripsi *One Time Pad Cipher*:

$$p_i = (c_i - z_i)(mod\ n)$$



Gambar 3.1 *Flowchart* Implementasi algoritma Blum-Blum Shub

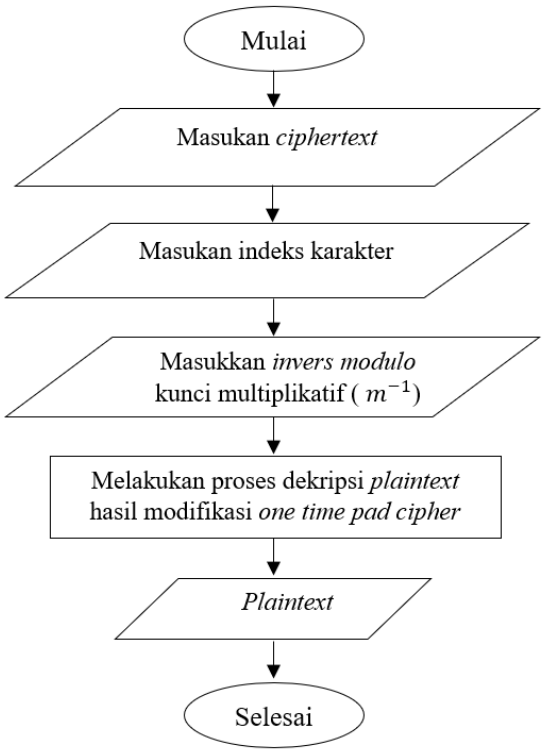
2. Adapun langkah-langkah yang di perlukan untuk membentuk enkripsi adalah:
    a. Proses enkripsi dilakukan dengan menggunakan algoritma *one time pad cipher*. Sebelumnya pengirim mentukan sebuah pesan asli yang akan diubah menjadi indeks karakter dari plainteks selanjutnya memasukan hasil kunci yang sudah di peroleh di proses pembentukan kunci pada algoritma blum-blum shub.
    b. Proses selanjutnya yaitu menentukan karakter yang di hasilkan dari setiap plainteks yang di hasilakan dari perhitungan enkripsi.



Gambar 3.2 *Flowchart* Enkripsi Hasil Implementasi *One Time Pad Cipher*

3. Proses dekripsi hasil implementasi *one time pad cipher* pada algoritma Blum-Blum Shub:

   Proses dekripsi dilakukan dengan menggunakan algoritma one time pad cipher. Pada proses ini cipherteks yang dihasilkan dalam peroses enkripsi akan di ubah menjadi plainteks dengan memasukan kunci yang di peroleh dalam pembentukan algoritma blum-blum shub.



Gambar 3.3 *Flowchart* Dekripsi Hasil Implementasi *One Time Pad Cipher*

BAB IV

HASIL DAN PEMBAHASAN

4.1 Proses Pembentukan Kunci Menggunakan Algoritma Blum-Blum Shub

Pada tahap pembentukan kunci ini merupakan sebuah proses dimana proses ini digunakan untuk membangkitkan kunci yang digunakan untuk proses enkripsi dan dekripsi *One Time Pad Cipher.* Pada penelitian ini melakukan proses pembentukan kunci dengan algoritma blum-blum shub untuk digunakan dalam proses Enkripsi dan dekripsi pada algoritma one time pad cipher. Pada proses pembentukan kunci ini menggunakan algoritma blum-blum shub yang tahapan nya sesuai dengan ketentuan blum-blum shub.

4.1.1 Algoritma Pembentukan Kunci menggunakan Algoritma Blum-Blum Shub

Adapun langkah-langkah yang digunakan dalam pembentukan kunci algoritma blum-blum shub, yaitu:

1. Proses pembentukan kunci dilakukan dengan menggunkan Algoritma Blum-blum Shub, pada proses pembentukan kunci ini dilakukan dengan menentukan plainteks yang digunakan. Selanjutnya menentukan nilai p dan q untuk menentukan nilai n yang di hasilkan setelah itu menentukan nilai s *(seed)*$x_0 = s^2 (\ mod\ n)$, membentuk bilangan acak $x_i = x_{i-1^2} (mod\ n)$ dan lakukan iterasi sebanyak jumlah posisi huruf *plaintext.*
2. Proses selanjutnya menentukan hasil gabungan LSB dari bilangan acak. Dari biangan acak tersebut digunakan untuk membentuk bilangan decimal baru untuk menjadi bilangan acak baru z_i.Melakukan implementasi kunci

enkripsi dan kunci dekripsi *one time pad cipher* dengan mengubah nilai k_i menjadi z_i. Sehingga di peroleh perhitungan sebagai berikut:

Implementasi kunci enkripsi *One Time Pad Cipher*:

$$c_i = (p_i + z_i)(mod\ n)$$

Implementasi kunci dekripsi *One Time Pad Cipher*:

$$p_i = (c_i - z_i)(mod\ n)$$

4.1.2 Simulasi dari Implementasi Kunci dengan Algoritma Blum-Blum Shub

Adapun tahapan pembentukan kunci pada algoritma blum-blum shub: Menentukan *plaintext* atau *ciphertext* serta mengkonvensi huruf *plaintex*t ke desimal ASCII tersebut.

Tabel 4.1 Konversi Plainteks ke dalam Bentuk Desimal

Posisi	Plaintext	Desimal ASCII
P_1	S	83
P_2	R	82
P_3	I	73
P_4	Spasi	32
P_5	I	73
P_6	B	66
P_7	U	85
P_8	N	78
P_9	Y	89
P_{10}	A	65
P_{11}	Spasi	32
P_{12}	N	78
P_{13}	O	79
P_{14}	V	86
P_{15}	I	73

1. Menentukan nilai p dan$q$, kemudian kalikan keduanya sehingga menghasilkan nilai n.

Dipilih nilai $p = 131$ dan $q = 367$ sehingga diperoleh nilai dari n yaitu $n = pq = 48.077$

2. Menentukan nilai s (seed) kemudian hitung $x_0 = s^2(mod\ n)$.

   Nilai umpan (seed) yang dipilih yaitu $s = 81$ jadi nilai $x_0 = 81^2(mod\ 48.077)$

3. Membentuk bilangan acak $x_i = x_{i-12}\ (mod\ n)$ dan lakukan iterasi sebanyak jumlah posisi huruf plaintext.

Tabel 4.2 Bilangan Acak x_i

Barisan bilangan acak	Proses Algoritma Blum-Blum Shub ($x_{i-1^2}\ mod\ n$)	Hasil
x_1	$81^2(mod\ 48077)$	6561
x_2	$6561^2(mod\ 48077)$	20936
x_3	$20936^2(mod\ 48077)$	20942
x_4	$20942^2(mod\ 48077)$	10124
x_5	$10124^2(mod\ 48077)$	19750
x_6	$19750^2(mod\ 48077)$	34581
x_7	$34581^2(mod\ 48077)$	41996
x_8	$41996^2(mod\ 48077)$	43641
x_9	$43641^2(mod\ 48077)$	1600
x_{10}	$1600^2(mod\ 48077)$	26502
x_{11}	$26502^2(mod\ 48077)$	9205
x_{12}	$9205^2(mod\ 48077)$	34566
x_{13}	$34566^2(mod\ 48077)$	1963
x_{14}	$1963^2(mod\ 48077)$	9441
x_{15}	$9441^2(mod\ 48077)$	23241

4. Membentuk bilangan acak baru z_i,karena bilangan acak baru z_i tidak harus satu *least significant bit* maka peneliti memilih $j = 6$ (j tidak melebihi $log_2(log_2\ 48077 = 15{,}553059)$.

   a. $x_1 = 6561 = 1100110100001$

      $z_1 = 6561 = 100001_{basis\ 2} \equiv 33\ (mod\ 2^6)$ diambil 6 bit LSB dari 6561.

b. $x_2 = 20936 = 101000111001000$

$z_2 = 20936 = 001000_{basis\ 2} \equiv 8\ (mod\ 2^6)$ diambil 6 bit LSB dari 20936.

c. $x_3 = 20942 = 101000111001110$

$z_3 = 20942 = 001110_{basis\ 2} \equiv 14\ (mod\ 2^6)$ diambil 6 bit LSB dari 20942.

d. $x_4 = 10124 = 10011110001100$

$z_4 = 10124 = 001100_{basis\ 2} \equiv 12\ (mod\ 2^6)$ diambil 6 bit LSB dari 10124.

e. $x_5 = 19750 = 100110100100110$

$z_5 = 19750 = 100110_{basis\ 2} \equiv 36\ (mod\ 2^6)$ diambil 6 bit LSB dari 19750.

f. $x_6 = 34851 = 1000100000100011$

$z_6 = 34851 = 100011_{basis\ 2} \equiv 35\ (mod\ 2^6)$ diambil 6 bit LSB dari 34851.

g. $x_7 = 41996 = 1010010000001100$

$z_7 = 41996 = 001100_{basis\ 2} \equiv 12\ (mod\ 2^6)$ diambil 6 bit LSB dari 41996.

h. $x_8 = 43641 = 1010101001111001$

$z_8 = 43641 = 111001_{basis\ 2} \equiv 57\ (mod\ 2^6)$ diambil 6 bit LSB dari 43641.

i. $x_9 = 1600 = 11001000000$

$z_9 = 1600 = 000000_{basis\ 2} \equiv 0\ (mod\ 2^6)$ diambil 6 bit LSB dari 1600.

j. $x_{10} = 26502 = 110011110000110$

$z_{10} = 26502 = 000110_{basis\ 2} \equiv 12\ (mod\ 2^6)$ diambil 6 bit LSB dari 26502.

k. $x_{11} = 9205 = 10001111110101$

$z_{11} = 9205 = 110101_{basis\ 2} \equiv 53\ (mod\ 2^6)$ diambil 6 bit LSB dari 9205.

l. $x_{12} = 34566 = 1000011100000110$

$z_{12} = 34566 = 000110_{basis\ 2} \equiv 6\ (mod\ 2^6)$ diambil 6 bit LSB dari 34566

m. $x_{13} = 1963 = 11110101011$

$z_{13} = 1963 = 101011_{basis\ 2} \equiv 43\ (mod\ 2^6)$ diambil 6 bit LSB dari 1963.

n. $x_{14} = 9441 = 10010011100001$

$z_{14} = 9441 = 100001_{basis\ 2} \equiv 33\ (mod\ 2^6)$ diambil 6 bit LSB dari 9441.

o. $x_{15} = 23241 = 101101011001001$

$z_{15} = 23241 = 001001_{basis\ 2} \equiv 9\ (mod\ 2^6)$ diambil 6 bit LSB dari 23241.

Jadi, barisan blok bit acak baru (z_i) yang dihasilkan adalah 33,8,14,12,36,35,12,57,0,12,53,6,23,33,9.

4.2 Proses Enkripsi

Proses Enkripsi adalah proses pengubah pesan asli menjadi pesan rahasia. Pada penelitian ini dilakukannya enkripsi setelah ditentukannya kunci yang diperoleh dalam pembentukan kunci dalam algoritma blum-blum shub. Pada proses

enkripsi ini peneliti mengunakan algoritma *one time pad cipher* untuk menghasilkan pesan rahasia. Proses enkripsi dapat dilakukan dengan adanya kunci.

4.2.1 Algoritma Enkripsi Algoritma *One Time Pad Cipher*

Adapun beberapa langkah-langkah yang di perlukan untuk membentuk enkripsi adalah:

1. Menentukan pesan teks asli (*plaintext).*
2. Menentukan indeks karakter dari *plaintext* tersebut.
3. Memasukan kunci z_i
4. Melakukan proses perhitungan $c_i \equiv (p_i + z_i) mod\ n$ dengan implementasi *one time pad cipher* menggunakan algoritma Blum-Blum Shub.

4.2.2 Simulasi Enkripsi

Langkah–langkah dekripsi hasil implementasi algoritma blum-blum shub cipher pada algoritma *one time pad cipher* adalah sebagai berikut:

1. Menentukan pesan teks asli serta menentukan indeks karakter. Peneliti melakukan proses enkripsi menggunakan pesan asli adalah **SRI IBUNYA NOVI.** Plaintext tersebut bisa dirubah sesuai dengan kebutuhan dan keinginan peneliti selanjutnya.
2. Menentukan indeks karakter dari *plaintext*

Tabel 4.3 Mengubah Plainteks Menjadi Bilangan Desimal

Plaintext	Desimal ASCII
S	83
R	82
I	73
Spasi	32
I	73
B	66
U	85
N	78
Y	89
A	65

Spasi	32
N	78
O	79
V	86
I	73

3. Melakukan proses enkripsi hasil implementasi algoritma blum-blum shub pada *one time pad cipher*.Langkah–langkah enkripsi hasil implementasi algoritma blum-blum shub cipher pada algoritma *one time pad cipher* adalah sebagai berikut:

Tabel 4.4 Proses Enkripsi Menggunakan Algoritma OTP

Indeks *Plaintext*	**Bilangan z_i**	**Kunci Enkripsi Hasil Implementasi**	**Indeks Ciphertext**	**Cipher text**
83	33	$(83 + 33) mod\ 256$	116	t
82	8	$(82 + 8) mod\ 256$	90	Z
73	14	$(73 + 14) mod\ 256$	87	W
32	12	$(32 + 12) mod\ 256$	44	,
73	36	$(73 + 36) mod\ 256$	109	m
66	35	$(66 + 35) mod\ 256$	101	E
85	12	$(85 + 12) mod\ 256$	97	A
78	57	$(78 + 57) mod\ 256$	135	‡
89	0	$(89 + 0) mod\ 256$	89	Y
65	12	$(65 + 12) mod\ 256$	77	M
32	53	$(32 + 53) mod\ 256$	85	U
78	6	$(78 + 6) mod\ 256$	84	T
79	43	$(78 + 43) mod\ 256$	121	y
86	33	$(87 + 33) mod\ 256$	120	x
73	9	$(73 + 9) mod\ 256$	82	R

Ciphertext yang dihasilkan adalah "**tZW,mea‡YMUTyxR**"

4.3 Proses Dekripsi

Proses dekripsi adalah proses mengubah pesan rahasia menjadi pesan asli. Proses dekripsi ini mengubah pesan rahasia yang ada pada proses enkripsi. Dalam penelitian ini dekripsi pesan rahasian menjadi pesan asli mengunakan algoritma one time pad cipher.

4.3.1 Algoritma Dekripsi pada Algoritma *One Time Pad Cipher*

Proses dekripsi hasil implementasi *one time pad cipher* pada algoritma Blum-Blum Shub adalah:

1. Memasukan pesan rahasia (*ciphertext)*
2. Menentukan indeks karakter dari *ciphertext* tersebut.
3. Memasukan Kunci z_i
4. Melakukan proses perhitungan $p_i \equiv (c_i + z_i) mod\ n$ dengan implementasi *One Time Pad Cipher* menggunakan algoritma Blum-Blum Shub.

Proses dekripsi dilakukan dengan menggunakan algoritma one time pad cipher. Pada proses ini cipherteks yang dihasilkan dalam peroses enkripsi akan di ubah menjadi plainteks dengan memasukan kunci yang di peroleh dalam pembentukan algoritma blum-blum shub.

4.3.1 Simulasi Dekripsi

Langkah–langkah dekripsi hasil implementasi algoritma blum-blum shub cipher pada algoritma *one time pad cipher* adalah sebagai berikut:

1. Peneliti melekukan proses dekripsi menggunakan hasil dari enkripsi. Cipherteks yang digunakan adalah "**tZW,mea‡YMUTyxR**"
2. Menentukan indeks karakter dari cipherteks.

Tabel 4.5 Mengubah Cipherteks Menjadi Bilangan Desimal

Posisi	Ciphertext	Desimal ASCII
C_1	t	116
C_2	Z	90
C_3	W	87
C_4	,	44
C_5	m	109
C_6	e	101
C_7	a	97
C_8	‡	135
C_9	Y	89

C_{10}	M	77
C_{11}	U	85
C_{12}	T	84
C_{13}	y	121
C_{14}	x	120
C_{15}	R	82

3. Melakukan proses dekripsi hasil implementasi *One Time Pad Cipher* menggunakan algoritma Blum-Blum Shub.

Tabel 4.6 Proses Dekripsi Menggunakan Algoritma OTP

Posisi huruf ke-i	**Bilangan z_i**	**Kunci Enkripsi Hasil Implementasi**	**Indeks Plaintext**	**Plain text**
116	33	$(116-33) mod\ 256$	83	S
90	8	$(90-8) mod\ 256$	82	R
87	14	$(87-14) mod\ 256$	73	I
44	12	$(44-12) mod\ 256$	32	Spasi
109	36	$(109-36) mod\ 256$	73	I
101	35	$(101-35) mod\ 256$	66	B
97	12	$(97-12) mod\ 256$	85	U
135	57	$(135-57) mod\ 256$	78	N
89	0	$(89-0) mod\ 256$	89	Y
77	12	$(77-12) mod\ 256$	65	A
85	53	$(85-53) mod\ 256$	32	Spasi
84	6	$(84-6) mod\ 256$	78	N
121	43	$(121-43) mod\ 256$	79	O
120	33	$(120-33) mod\ 256$	86	V
82	9	$(82-9) mod\ 256$	73	I

Plaintext yang di hasilkan adalah **SRI IBUNYA NOVI**

4.4 Kajian Integrasi Agama

Berdasarkan hasil dari pembahasan yang telah didapatkan dapat ditarik kesimpulan bahwa, implementasi algoritma blum-blum shub pada algoritma *one time pad* cipher dalam pembentukan pesan dapat di kaitkan dengan integrasi agama maka diperoleh bahwa pada pembentukan pembentukan kunci dan proses yang terdapat di dalam mengenkripsi dan dekripsi pesan yang ada didalam nya . Sehingga pada algoritma ini mempunyai beberapa tahapan untuk mencari bilangan acak baru

antara lain memulai dengan mencari bilangan acak baru, setelah itu mencari nilai bilangan acak tersebut sehingga menghasilan kunci baru. Pada tahapan ini dapat di perumpamakan seperti surah al-zalzalah ayat 7 dan 8 yang memiliki arti:

"Siapa yang mengerjakan kebaikan seberat zarah, dia akan melihat (balasan)-nya (7). Siapa yang mengerjakan kejahatan seberat zarah, dia akan melihat (balasan)-nya." (Q.S. Al-Zalzalah: 7-8)

Sehingga melalui ayat ini, Allah SWT coba jelaskan perlakuan adil-Nya terhadap seluruh manusia. Di mana masing-masing amal meski sedikit atau kecil yang mereka kerjakan sungguh akan menerima ganjarannya. Seperti halnya, seorang yang menganggap perbuatan baiknya tak seberapa, tapi di mata Allah SWT hal sekecil itu tetap memberikan pahala bagi si pelaku. Begitu pula dengan orang yang meremehkan segelintir aksi kejinya, di mata-Nya itu tetaplah dosa yang mampu memasukkan pelaku ke neraka.

Pada hadits lain riwayat Abu Hurairah, Rasul SAW juga coba terangkan perihal amal yang dilakukan dengan ikhlas mengharap ridha Allah SWT akan memberi balasan meski dianggap sederhana. Tafsir Ibnu Katsir Jilid 15(Ghoffar, 2000), berikut sabda Nabi SAW:

"Kuda itu untuk tiga orang. Bagi seseorang kuda itu akan menjadi pahala, bagi seorang lagi akan menjadi satar (penutup), dan bagi seorang yang lainnya akan menjadi dosa."

Adapun orang yang mendapatkan pahala adalah orang yang mengikat kuda itu di jalan Allah SWT, lalu dia membiarkannya di tempat penggembalaan atau taman dalam waktu yang lama, maka apa terjadi selama masa penggembalaannya di tempat penggembalaan dan taman itu, maka itu akan menjadi kebaikan baginya.

Dan jika dia menghentikan masa penggembalaannya lalu kuda itu melangkah satu atau dua langkah, maka jejak kaki dan juga kotorannya akan

menjadi kebaikan baginya. Dan jika kuda itu menyeberangi sungai lalu ia minum air dari sungai tersebut, maka yang demikian itu menjadi kebaikan baginya, dan kuda itu pun bagi orang tersebut adalah pahala.

Dan orang yang mengikat kuda itu karena untuk memperkaya diri dan demi kehormatan diri tetapi dia tidak lupa hak Allah SWT dalam pemeliharaannya, maka kuda itu akan menjadi satar baginya. Serta orang yang mengikatnya karena perasaan bangga dan riya, maka ia hanya akan menjadi dosa baginya. (HR Muslim)(Materi et al., n.d.)

Dalam ayat dan hadits tersebut dapat dilihat bagaimana proses untuk mendapatkan pahala dari allah kita dapat melihat berapa tahapan tahapan seperti pada algoritma blum-blum shub bahwa ada tahapan-tahapan untuk mencari kunci acak lalu menenkripsi dan dekripsi suatu bilangan acak tersebut menggunakan metode OTP untuk bisa membaca kunci yang sudah di ubah di algoritma blum-blum shub dengan mendekripsi pesan.

Ayat yang di bahas seperti perumpamaan manusia tidak tahu apa yang di lakukan memiliki ganjaran walaupun itu sekecil atom. Sama hal nya kita tidak tau bagai mana algoritma ini bekerja untuk meyelesakan kunci acak tersebut hingga bisa terbaca. Maka dari itu kita dapat mengetahui bagimana tahapan allah memberi ganjaran untuk setiap hambanya.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasakan hasil dan pembahasan di atas, dapat diambil beberapa kesimpulan:

1. Proses pembentukan kunci menggunakan algoritma Blum-Blum Shub, pada pembentukan kunci dengan menggunakan algoritma Blum-Blum Shub peneliti memilih niai p dan q yaitu $p = 131$ dan $q = 367$ dipilih nilai tersebut sehingga dihasilkan $n = 48.077$,karena s dan n relatif prima sehingga dipilih nilai $s = 81$ kemudian digunakan untuk menentukan nilai $x_0 = s^2 \, mod \, n = 81^2 mod \, 48077$, nilai tersebut digunakan untuk menghasilkan bilangan acak sebanyak plainteks yang ditentukan. Kunci acak yang dihasilkan tersebut digunakan untuk mengenkripsi plainteks atau mendekripsi cipherteks pada algoritma *one time pad cipher.*
2. Proses enkripsi pesan menggunakan algoritma *one time pad cipher* diawali dengan menentukan nilai indeks dari pesan asli yang telah di tentukan selanjutnya memasukan kunci acak yang telah di hasilkan dari pembentukan kunci algoritma Blum-Blum Shub. Selanjutnya melakukan perhitungan sehingga menghasilkan kunci yang sangat acak.
3. Proses dekripsi hasil implementasi ciperteks diawali dengan memasukan kunci acak yang telah di hasilkan dari implementasi algoritma Blum-Blum Shub, kemudian lakukan perhitungan sehingga menghasilkan plainteks.

5.2 Saran

Penelitian ini membahas mengenai implementasi algoritma blum-blum shub pada algoritma one time pad cipher. Untuk penelitian selanjutnya disarkanakn menggunakan nilai yang lebih tinggi, penambahan karakter baru serta menggunakan seluruh karakter ASCII pada peroses enkripsi dan dekripsi. Selain itu, penelitian selanjutnya disarankan membuat suatu modifikasi algoritma lainnya yang lebih mudah digunakan serta dapat ditingkatkan keamanan yang lebih tinggi.

DAFTAR PUSTAKA

Al-Qur'an dan Terjemahannya. (2019) Kementrian Agama RI.

Al-Bantani, Rohimudin Nawawi, Syekh Nawawi al-Bantani Ulama Indonesia yang Jadi Imam Besar di Masjidil Haram, Depok: Mentari Media, 2017.

Aly, M. R. (2019). *Asbāb An-Nuzūl Dalam Tafsir Ibnu Katsir (Seputar Ayat Khamar Dan Ayat Bencana Alam)*. 46.

Amin, M. M. (2016). Komunikasi Berbasis Teks. *Jurnal Pseudocode*, *III* (September), 129–136.

Amiruddin. (2021). Amanah dalam Perspektif Al-Quran (Studi Komparatif Tafsir Al-Misbah dan Al-Azhar). *Jurnal Mudarrisuna: Media Kajian Pendidikan Agama Islam*, *11* (4), 833–850.

Ayuni Saputri, S. (n.d.). *Penerapan Algoritma One Time Pad ... 1193*.

Bakir, & Hozairi. (2018). Implementasi Metode Least Significant Bit (LSB) Dengan Enkripsi Cipher Caesar Pada Steganografi Menggunakan Image Processing. *JUSTINDO (Jurnal Sistem & Teknologi Informasi Indonesia)*, *3*, 75–81.

Ghoffar, A. (2000). *Tafsir Ibnu Katsir 1 a.pdf*.

Gunawan, I. (2018). Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *2*(1), 57. https://doi.org/10.30645/j-sakti.v2i1.48

Harahap, M. K., & Khairina, N. (2018). Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks. *Jurnal & Penelitian Teknik Informatika*, *1*(April 2017), 58–62.

Materi, T., Dalam, H., An, Q. U. R., Madrasah, H., Hadits, A. M., & Madrasah, P. (n.d.). *Hadits Dalam Qur'an Hadits Madrasah Tsanawiyah*. *1395*(1628), 36–89.

Maulana, U. I. N., & Ibrahim, M. (2020). *Halaman Sampul Fakultas Psikologi Universitas Islam Negeri Maulana Malik Ibrahim Malang 2020*.

Munir, R. (2006). Kriptografi. Bandung: Informatika.

Munir, Rinaldi. 2019. Kriptografi, Bandung: Informatika Bandung

Munir, R. (2010). Matematika Diskrit. Bandung: Informatika.

Naufal, M. F. (2021). *Muhammad Fakhri Naufal, 2021 Kriptografi Audio Menggunakan Transposisi Dan Affine Cipher Yang Dikembangkan Dengan Algoritma Blum Blum Shub Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu*.

Nguyen, T. T., & Lee, H. (2016). High-speed low-complexity elliptic curve cryptographic processor. In *ISOCC 2015 - International SoC Design Conference: SoC for Internet of Everything (IoE)*. https://doi.org/10.1109/ISOCC.2015.7401749

Parry, A., Nim, L., Blum, L., Blum, M., & Shub, M. (1986). *Blum Blum Shub dan Inversive Congruential Generator Beserta Implementasinya*. 1–4.

Setyaningsih, E (2015). Kriptografi & Implementasinya Menggunakan Matlab.

Yogyakarta, ANDI

Sianturi, C. F. (2020). Modifikasi Pembangkit Kunci Algoritma RSA Dengan Menerapkan Algoritma Blum Blum Shub (BBS). *BUilding of Informatics, Technology and Sicience (BITS)*, *2*(1), 39–43. http://ejurnal.seminar-id.com/index.php/bits/article/view/333

LAMPIRAN

Tabel ASCII

Desimal	Heksadesimal	Oktal	Karakter Deskripsi	
0	00	000	NULL	Null
1	01	001	SOH	start of header
2	02	002	STX	start of text
3	03	003	ETX	end of text
4	04	004	EOT	end of transmissoion
5	05	005	ENQ	Enquiry
6	06	006	ACK	Acknowledgement
7	07	007	BEL	Bell
8	08	010	BS	Backspace
9	09	011	HT	horizontal tab
10	0A	012	LF	line feed
11	0B	013	VT	vertical tab
12	0C	014	FF	form feed
13	0D	015	CR	Enter
14	0E	016	SO	shift out
15	0F	017	SI	shift in
16	10	020	DLE	data link escape
17	11	021	DC1	device control 1
18	12	022	DC2	device control 2
19	13	023	DC3	device control 3
20	14	024	DC4	device control 4
21	15	025	NAK	negative acknowledgement
22	16	026	SYN	synchronous idle
23	17	027	ETB	end of transmission block
24	18	030	CAN	Cancel
25	19	031	EM	end of medium
26	1A	032	SUB	substitue / ctrl + z
27	1B	033	ESC	Escape
28	1C	034	FS	file separator
29	1D	035	GS	group separator
30	1E	036	RS	record separator
31	1F	037	US	unit separator
32	20	040		Spasi
33	21	041	!	tanda seru
34	22	042	"	tanda petik
35	23	043	#	tanda pagar
36	24	044	$	Dollar
37	25	045	%	Persen
38	26	046	&	Ampersand

39	27	047	'	tanda petik tunggal
40	28	050	(	tanda kurung kiri
41	29	051	)	tanda kurung kanan
42	2A	052	*	Bintang
43	2B	053	+	Plus
44	2C	054	,	Koma
45	2D	055	-	Setrip
46	2E	056	.	Titik
47	2F	057	/	garis miring
48	30	060	0	Nol
49	31	061	1	Satu
50	32	062	2	Dua
51	33	063	3	Tiga
52	34	064	4	Empat
53	35	065	5	Lima
54	36	066	6	Enam
55	37	067	7	Tujuh
56	38	070	8	Delapan
57	39	071	9	sembilan
58	3A	072	:	titik dua
59	3B	073	;	titik koma
60	3C	074	<	kurang dari
61	3D	075	=	sama dengan
62	3E	076	>	lebih dari
63	3F	077	?	tanda Tanya
64	40	100	@	simbol at
65	41	101	A	kapital A
66	42	102	B	kapital B
67	43	103	C	kapital C
68	44	104	D	kapital D
69	45	105	E	kapital E
70	46	106	F	kapital F
71	47	107	G	kapital G
72	48	110	H	kapital H
73	49	111	I	kapital I
74	4A	112	J	kapital J
75	4B	113	K	kapital K
76	4C	114	L	kapital L
77	4D	115	M	kapital M
78	4E	116	N	kapital N
79	4F	117	O	kapital O
80	50	120	P	kapital P
81	51	121	Q	kapital Q
82	52	122	R	kapital R
83	53	123	S	kapital S

84	54	124	T	kapital T
85	55	125	U	kapital U
86	56	126	V	kapital V
87	57	127	W	kapital W
88	58	130	X	kapital X
89	59	131	Y	kapital Y
90	5A	132	Z	kapital Z
91	5B	133	[	tanda kurung siku kiri
92	5C	134	\	garis miring terbalik
93	5D	135	]	tanda kurung siku kanan
94	5E	136	^	Caret
95	5F	137	_	Underscore
96	60	140	`	grave accent
97	61	141	a	huruf kecil a
98	62	142	b	huruf kecil b
99	63	143	c	huruf kecil c
100	64	144	d	huruf kecil d
101	65	145	e	huruf kecil e
102	66	146	f	huruf kecil f
103	67	147	g	huruf kecil g
104	68	150	h	huruf kecil h
105	69	151	i	huruf kecil i
106	6A	152	j	huruf kecil j
107	6B	153	k	huruf kecil k
108	6C	154	l	huruf kecil l
109	6D	155	m	huruf kecil m
110	6E	156	n	huruf kecil n
111	6F	157	o	huruf kecil o
112	70	160	p	huruf kecil p
113	71	161	q	huruf kecil q
114	72	162	r	huruf kecil r
115	73	163	s	huruf kecil s
116	74	164	t	huruf kecil t
117	75	165	u	huruf kecil u
118	76	166	v	huruf kecil v
119	77	167	w	huruf kecil w
120	78	170	x	huruf kecil x
121	79	171	y	huruf kecil y
122	7A	172	z	huruf kecil z
123	7B	173	{	tanda kurung kurawal kiri
124	7C	174	|	vertical bar
125	7D	175	}	tanda kurung kurawal kanan
126	7E	176	~	Tilde
127	7F	177	DEL	
128	80	200	€	

129	81	201		
130	82	202	‚	
131	83	203	*ƒ*	
132	84	204	„	
133	85	205	…	
135	87	207	‡	
136	88	210	ˆ	
137	89	211	‰	
138	8A	212	Š	
139	8B	213	‹	
140	8C	214	Œ	
141	8D	215		
142	8E	216	Ž	
143	8F	217		
144	90	220		
145	91	221	‘	
146	92	222	’	
147	93	223	“	
148	94	224	”	
149	95	225	•	
150	96	226	–	
151	97	227	—	
152	98	230	˜	
153	99	231	™	Trademark
154	9A	232	š	
155	9B	233	›	
156	9C	234	œ	
157	9D	235		
158	9E	236	ž	
159	9F	237	Ÿ	
160	A0	240		
161	A1	241	¡	
162	A2	242	¢	
163	A3	243	£	
164	A4	244	¤	
165	A5	245	¥	
166	A6	246	¦	
167	A7	247	§	
168	A8	250	¨	
169	A9	251	©	Copyright
170	AA	252	ª	
171	AB	253	«	
172	AC	254	¬	
173	AD	255	-	
174	AE	256	®	

175	AF	257	¯	
176	B0	260	°	Derajat
177	B1	261	±	
178	B2	262	²	
179	B3	263	³	
180	B4	264	´	
181	B5	265	µ	
182	B6	266	¶	
183	B7	267	·	
184	B8	270	¸	
185	B9	271	¹	
186	BA	272	º	
187	BB	273	»	
188	BC	274	¼	satu per empat
189	BD	275	½	Setengah
190	BE	276	¾	tiga per empat
191	BF	277	¿	
192	C0	300	À	
193	C1	301	Á	
194	C2	302	Â	
195	C3	303	Ã	
196	C4	304	Ä	
197	C5	305	Å	
198	C6	306	Æ	
199	C7	307	Ç	
200	C8	310	È	
201	C9	311	É	
202	CA	312	Ê	
203	CB	313	Ë	
204	CC	314	Ì	
205	CD	315	Í	
206	CE	316	Î	
207	CF	317	Ï	
208	D0	320	Đ	
209	D1	321	Ñ	
210	D2	322	Ò	
211	D3	323	Ó	
212	D4	324	Ô	
213	D5	325	Õ	
214	D6	326	Ö	
215	D7	327	×	simbol perkalian
216	D8	330	Ø	
217	D9	331	Ù	
218	DA	332	Ú	
219	DB	333	Û	

220	DC	334	Ü	
221	DD	335	Ý	
222	DE	336	Þ	
223	DF	337	ß	
224	E0	340	à	
225	E1	341	á	
226	E2	342	â	
227	E3	343	ã	
228	E4	344	ä	
229	E5	345	å	
230	E6	346	æ	
231	E7	347	ç	
232	E8	350	è	
233	E9	351	é	
234	EA	352	ê	
235	EB	353	ë	
236	EC	354	ì	
237	ED	355	í	
238	EE	356	î	
239	EF	357	ï	
240	F0	360	ð	
241	F1	361	ñ	
242	F2	362	ò	
243	F3	363	ó	
244	F4	364	ô	
245	F5	365	õ	
246	F6	366	ö	
247	F7	367	÷	simbol pembagian
248	F8	370	ø	
249	F9	371	ù	
250	FA	372	ú	
251	FB	373	û	
252	FC	374	Ü	
253	FD	375	Ý	
254	FE	376	þ	
255	FF	377	Ÿ	

RIWAYAT HIDUP

Novi Hardiyantik lahir di Kumai pada tanggal 15 November 2000, biasa dipanggil Novi. Penulis tinggal di Jalan Swadaya, RT 04, Desa Sungai Kapitan, Kecamatan Kumai, Kabupaten Kotawaringin Barat. Anak keempat dari lima bersaudara yakni putri dari Bapak Baharudin dan Ibu Sri Anik.

Penulis telah menempuh Pendidikan formal mulai dari TK Sadar Bakti (2006-2007). Kemudian, melanjutkan Pendidikan dasar di SDN 1 Kumai Hilir (2007-2013). Setelah itu, penulis melanjutkan Pendidikan menengah pertama di MTs Negeri 1 Kumai (2013-2016). Selanjutnya penulis melanjutkan Pendidikan menengah atas di SMAN 1 Kumai (2016-2019) dan pada tahun 2019 penulis menempuh pendidikan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil program studi matematika.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Novi Hardiyantik
NIM : 19610013
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Implementasi Algoritma Blum-Blum Shub Pada Algoritma *One Time Pad Cipher* Dalam Pengmanan Pesan
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Ari Kusumastuti, M.Pd., M.Si.

No	Tanggal	Hal	Tanda Tangan
1.	13 Januari 2023	Konsultasi Topik dan Data	1.
2.	17 Maret 2023	Konsultasi Bab I, II, dan III	2.
3.	3 Mei 2023	Konsultasi Bab I, II, dan III	3.
4.	8 Agustus 2023	ACC Bab I, II, dan III	4.
5.	13 Agustus 2023	Konsultasi Kajian Agama Bab I dan II	5.
6.	18 Agustus 2023	ACC Kajian Agama Bab I dan II	6.
7.	30 Agustus 2023	ACC Seminar Proposal	7.
8.	15 September 2023	Konsultasi Revisi Seminar Proposal	8.
9.	10 Oktober 2023	Konsultasi Bab IV dan V	9.
10.	12 Oktober 2023	ACC Bab IV dan V	10.
11.	19 Oktober 2023	Konsultasi Kajian Agama Bab IV	11.
12.	24 Oktober 2023	ACC Kajian Agama Bab IV	12.
13.	22 November 2023	ACC Seminar Hasil	13.
14.	8 Desember 2023	Konsultasi Revisi Seminar Hasil	14.
15.	19 Desember 2023	ACC Sidang Skripsi	15.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

16.	26 Desember 2023	ACC Keseluruhan	16.

Malang, 26 Desember 2023
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005