ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN KURVA ELIPTIK PADA *AFFINE CIPHER* DENGAN METODE KOBLITZ

SKRIPSI

Oleh
PUTRI LISARO HADI
NIM. 18610093

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2022

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN KURVA ELIPTIK PADA *AFFINE CIPHER* DENGAN METODE KOBLITZ

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
Putri Lisaro Hadi
NIM. 18610093

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2022

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN KURVA ELIPTIK PADA *AFFINE CIPHER* DENGAN METODE KOBLITZ

SKRIPSI

Oleh
Putri Lisaro Hadi
NIM. 18610093

Telah Disetujui untuk Diuji
Malang, 20 Juni 2022

Dosen Pembimbing I	Dosen Pembimbing II
Prof. Dr. H. Turmudi, M.Si., Ph.D	Mohammad Nafie Jauhari, M.Si
NIP. 19571005 198203 1 006	NIDT. 19870218 20160801 1 056

Mengetahui,
Ketua Program Studi Matematika

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

ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN KURVA ELIPTIK PADA *AFFINE CIPHER* DENGAN METODE KOBLITZ

SKRIPSI

Oleh
Putri Lisaro Hadi
NIM. 18610093

Telah Dipertahankan di Depan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 24 Juni 2022

Ketua Penguji : Hisyam Fahmi, M.Kom .....

Anggota Penguji 1 : Muhammad Khudzaifah, M.Si .....

Anggota Penguji 2 : Prof. Dr. H. Turmudi, M.Si., Ph.D .....

Anggota Penguji 3 : Mohammad Nafie Jauhari, M.Si .....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini:

Nama	: Putri Lisaro Hadi
NIM	: 18610093
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Enkripsi dan Dekripsi Pesan Menggunakan Kurva Eliptik pada *Affine Cipher* dengan Metode Koblitz

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

Malang, 16 Juni 2022

Yang membuat pernyataan,

Putri Lisaro Hadi

NIM. 18610093

MOTO

“Pelangi ada setelah badai menerpa”

“Kenikmatan ada setelah terlaksana usaha dan doa”

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:
Kedua orang tua tercinta yaitu Bapak Solikul Hadi dan Ibu Munawaroh, yang senantiasa memberi dukungan, semangat dan doa restu kepada penulis.
Kedua kakak yaitu Rizqi Maulana Hadi dan Fatimah Anggraini dan seluruh keluarga yang senantiasa memberikan dukungan dan nasihat kepada penulis.
Sahabat-sahabat penulis dan seluruh teman-teman Aksioma yang telah memberi semangat kepada penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt. atas rahmat, taufik serta hidayah-Nya, sehingga sampai pada saat ini penulis mampu menyelesaikan penyusunan proposal skripsi yang berjudul "Enkripsi dan Dekripsi Pesan Menggunakan Kurva Eliptik pada *Affine Cipher* dengan Metode Koblitz".

Dengan ini ucapan terima kasih yang sebesar-besarnya penulis sampaikan kepada semua pihak yang membantu dalam proses pembuatan proposal ini, terutama kepada :

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Prof. Dr. H. Turmudi, M.Si., Ph. D, selaku dosen pembimbing I yang telah memberikan bimbingan, arahan, dan berbagi ilmunya kepada penulis.
5. Mohammad Nafie Jauhari, M.Si, selaku dosen pembimbing II yang telah memberikan bimbingan dan berbagi ilmunya kepada penulis.
6. Hisyam Fahmi, M.Kom, selaku Ketua Penguji dalam Ujian Skripsi yang telah memberikan masukan dan saran kepada penulis.
7. Muhammad Khudzaifah, M.Si selaku Anggota Penguji I dalam Ujian Skripsi yang telah memberikan masukan dan arahan kepada penulis.
8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
9. Orang tua tercinta Solikul Hadi dan Munawaroh yang senantiasa memberi restu, doa, dukungan, serta motivasi kepada penulis sampai saat ini.
10. Rizqi Maulana dan Fatimah Anggraini selaku kakak dari penulis yang senantiasa memberikan dukungan, semangat, dan berbagi pengalamannya kepada penulis.

Pada penelitian ini penulis berharap semoga menambah wawasan baru dan memberikan banyak manfaat bagi penulis dan pembaca yang lain. *Aamiin*

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 24 Mei 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

LAMPIRAN

ABSTRAK

Hadi, Putri Lisaro. 2022. **Enkripsi dan Dekripsi Pesan Menggunakan Kurva Eliptik pada *Affine Cipher* Metode Koblitz**. Skripsi Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Prof. Dr, H. Turmudi, M.Si., Ph. D, (II) Mohammad Nafie Jauhari, M.Si.

Kata Kunci: Enkripsi, Dekripsi, *Affine Cipher*, Kurva Eliptik, Metode Koblitz.

Kriptografi merupakan ilmu matematis yang digunakan untuk mengamankan suatu pesan. Pandemi Covid-19 ini membuat masyarakat mengalami sedikit kesulitan untuk berkomunikasi. Penyampaian informasi secara *online* belum tentu menjamin keamanannya. Oleh karena itu, diperlukan suatu teknik untuk pengaman pesan. Pada penelitian ini menggunakan Kriptografi Kurva Eliptik pada *Affine Cipher* dengan metode Koblitz, karena memiliki kelebihan dalam hal panjang kunci yang lebih pendek namun juga memiliki tingkat keamanan yang sama jika dibandingkan dengan algoritma kriptografi asimetris lainnya. Tujuan penelitian ini untuk mengetahui proses enkripsi dan dekripsi menggunakan kurva eliptik pada *Affine Cipher* dengan metode Koblitz untuk mengamankan pesan teks. Tahapan penelitian ini menggunakan pendekatan kualitatif dengan metode *library research*. Metode yang digunakan yaitu sesuai pada algoritma *Affine Cipher* yang menggunakan dua kunci simetris, kemudian kurva eliptik metode Koblitz digunakan untuk proses enkripsi dan dekripsi kunci. Proses enkripsi dari algoritma *Affine Cipher* dengan rumus $C = mP + b\ (mod\ n)$ menghasilkan sebuah *ciphertext*, sedangkan proses enkripsi kunci menggunakan metode Koblitz dengan rumus $x = mk + 1$ yang kemudian disubstitusikan pada persamaan $y^2 = x^3 + 2x + 7(mod\ 127)$ menghasilkan sebuah *cipherkey*. Sedangkan, pada proses dekripsi dilakukan dengan mendekripsi *cipherkey* menggunakan metode Koblitz dengan rumus $m = (x - 1)/k$ dan menghasilkan kunci simetris dari algoritma *Affine Cipher*, selanjutnya akan dilakukan proses dekripsi *ciphertext* dengan menggunakan rumus $P = m^{-1}(C - b) mod\ n$. Hasil dari penelitian ini menunjukkan bahwa proses enkripsi dan dekripsi dapat dilakukan dengan baik serta dapat meningkatkan kemanan suatu pesan, karena adanya penggabungan dua algoritma simetris dan algoritma asimteris.

ABSTRACT

Hadi, Putri Lisaro. 2022. **Encryption and Decryption of Messages Using Elliptic Curves on *Affine Cipher* Koblitz Method**. Thesis of Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisors: (I) Prof. Dr, H. Turmudi, M.Si., Ph. D, (II) Mohammad Nafie Jauhari, M.Si.

Kata Kunci: Encryption, Decryption, *Affine Cipher*, Elliptic Curve, Koblitz Method

Kriptografi is a mathematical science used to secure a message. The Covid-19 pandemic has made it a little difficult for people to communicate. The delivery of information online does not necessarily guarantee its security. Therefore, a technique is needed for security in this study using Elliptic Curve Cryptography on the Affine Cipher with the Koblitz method, because ithas advantages in terms of shorter key lengths but also has the same level of security when compared to cryptographic algorithms other asymmetrical. The purpose of this study was to know the encryption and decryption process using an elliptic curve on Affine Cipher with the koblitz method to secure text messages. This stage of research uses a qualitative approach with the library research method. The method used is appropriate in the Affine Cipher algorithm which uses two symmetric keys, then the elliptic curve of the Koblitz method is used for the process of encryption and decryption of the key. Encryption process of the Affine Cipher algorithm with formulas $C = mP + b\ (mod\ n)$ generates a ciphertext, while the key encryption process uses the Koblitz method with a formula $x = mk + 1$ which is then substituted on the equation $y^2 = x^3 + 2x + 7(mod\ 127)$ generates a cipherkey. Meanwhile, the decryption process is carried out by decrypting the cipherkey using the Koblitz method with the formula $m = (x - 1)/k$ and generates a symmetric key from the Affine Cipher algorithm, then the ciphertext decryption process will be carried out using the formula $P = m^{-1}(C - b) mod\ n$. The results of this study show that the encryption and decryption process can be done well and can improve the security of a message, due to the combination of two symmetric algorithms and asymptomatic algorithms.

المستخلص البحث

هادي، فوتري ليسارو. 2022. **تشفير وفك تشفير الرسائل باستخدام منحنيات إهليلجية على** طريقة ***Affine Cipher*** **Koblitz** . .البث الج امعي ، كلية العلوم والتكنولوجيا، مولانا مالك إبراهيم الدولة الإسلامية جامعة مالانغ.

المشرف :

(I) ،بروفسور الدكتور الترمودي، الماجستير,الحاج ، دكتوراه (II) محمد نافع جوهري، الماجستير.

الكلمات المفتاحية: التشفير، فك التشفير، التشفير *الدقيق*، الخوارزمية، المنحنى الإهليلجي، طريقة كوبليتز.

التشفير هو علم رياضي يستخدم لتأمين رسالة. جائحة Covid-19
هذا يجعل من الصعب قليلا على الناس التواصل. تسليم المعلومات عبر الإنترنت لا يضمن بالضرورة أمنها. لذلك ، هناك حاجة إلى تقنية للأمان في هذه الدراسة باستخدام تشفير المنحنى الإهليلجي على تشفير *Affine* باستخدام طريقة Koblitz ، لأنهيتمتع بمزايا من حيث أطوال المفاتيح الأقصر ولكن لديه أيضا نفس مستوى الأمان عند مقارنته بخوارزميات التشفير غير المتماثلة الأخرى. كان الغرض من هذه الدراسة هو معرفة عملية التشفير وفك التشفير باستخدام منحنى بيضاوي الشكل على *Affine Cipher* باستخدام طريقة Koblitz لتأمين الرسائل النصية. تستخدم هذه المرحلة من البحث نهجا نوعيا مع طريقة *البحث في المكتبة*. الطريقة المستخدمة مناسبة في خوارزمية *Affine Cipher* التي تستخدم مفتاحين متماثلين ، ثم يستخدم المنحنى الإهليلجي لطريقة كوبليتز لعملية تشفير المفتاح وفك تشفيره. عملية تشفير خوارزمية *تشفير Affine* مع الصيغ $C = mP + b \ (mod\ n)$
يولد *نصا مشفرا*، بينما تستخدم عملية تشفير المفتاح أسلوب Koblitz مع صيغة $x = mk + 1$ الذي يتم استبداله بعد ذلك بالمعادلة $y^2 = x^3 + 2x + 7(mod\ 127)$ يولد *مفتاح تشفير*. وفي الوقت نفسه ، يتم تنفيذ عملية فك التشفير عن طريق فك تشفير *مفتاح التشفير* باستخدام طريقة Koblitz مع الصيغة $m = (x - 1)/k$ ويولد مفتاحا متماثلا من خوارزمية *Affine Cipher* ، ثم سيتم تنفيذ عملية فك تشفير *النص المشفر* باستخدام الصيغة $P = m^{-1}(C - b) mod\ n$.تظهر نتائج هذه الدراسة أن عملية التشفير وفك التشفير يمكن أن تتم بشكل جيد ويمكن أن تحسن أمان الرسالة ، بسبب الجمع بين خوارزميتين متماثلتين وخوارزميات بدون أعراض.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi saat ini sangat berpengaruh besar terhadap aspek kehidupan. Tetapi dengan adanya pandemi covid-19 ini membuat masyarakat mengalami sedikit kesulitan untuk berkomunikasi. Pada saat ini yang menjadi masalah yaitu dalam hal penyampaian informasi. Penyampaian informasi untuk saat ini dilakukan secara online yang memanfaatkan perkembangan teknologi. Perkembangan teknologi komunikasi memudahkan manusia untuk berkomunikasi satu sama lain. Dalam perkembangan teknologi komunikasi ini ada banyak media yang dapat digunakan untuk berkomunikasi, salah satunya yaitu media komunikasi umum yang menggunakan telepon genggam dan internet yang berguna untuk mengirim dan menerima suatu pesan kepada pihak lain. Namun, dalam hal ini informasi yang beredar juga belum tentu terjamin keamananya. Pada media komunikasi umum yang digunakan untuk mengirim dan menerima pesan ini masih sangat rawan akan terjadinya penyadapan pesan atau informasi oleh pihak yang tidak berhak menerima pesan atau informasi tersebut. Oleh karena itu, untuk menjaga keamanannya disarankan agar pengguna media komunikasi ini perlu adanya teknik pengamanan pesan. Dengan demikian pesan yang ingin disampaikan dapat terjaga keamananya. Berkaitan dengan menyampaikan pesan kepada yang berhak menerimanya dalam hal ini disinggung dalam al-Qur'an Q.S al-Anfal ayat 27 (LPMQ), 2022):

"Hai orang-orang yang beriman, janganlah kamu menghianati Allah dan Rashulnya (Muhammad) dan (juga) janganlah kamu menghianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui" (Q.S al-Anfal,9,27).

Pada ayat tersebut dijelaskan akan pentingnya menjaga sebuah amanat yang dipercayakan kepada siapapun, termasuk menjaga suatu keamanan suatu pesan. Menjaga kerahasiaan suatu pesan termasuk sebuah amanat yang harus dijaga. Oleh karena itu, kriptografi adalah salah satu ilmu dalam matematika yang digunakan untuk mengamankan suatu pesan. Kriptografi (*cryptography*) berasal dari bahasa Yunani: '*crypto'* artinya '*secret'* (rahasia), sedangkan '*graphein* artinya '*writing'* (tulisan). Jadi, kriptografi secara harfiah berarti "*secret writing"* (tulisan rahasia)(Munir, 2019). Dalam kriptografi ini terdapat istilah enkripsi dan dekripsi pada pesan. Enkripsi adalah proses pembentukan *plaintext* (pesan yang bisa dibaca) menjadi *chipertext* (pesan yang tersandi). Sedangkan dekripsi yaitu proses pengembalian *chipertext* menjadi *plaintext*. Kriptografi sudah mengalami kemajuan yang signifikan, berawal dari algoritma sederhana hingga yang kompleks. Dalam kriptografi terdapat berbagai macam algoritma kriptografi. Kriptografi terbagi menjadi dua jenis, yaitu kriptografi klasik dan kriptografi modern (Ariyus, 2008). Algoritma simetri disebut dengan algoritma klasik karena menggunakan satu kunci untuk enkripsi dan dekripsinya. Oleh karena itu algoritma simetri kurang menjamin keamanannya jika digunakan untuk mengamankan suatu pesan. Algoritma asimetris disebut dengan kriptografi kunci publik, tetapi kunci publik yang digunakan pada saat melakukan enkripsi dan dekripsi berbeda (Ariyus, 2006).

Affine Cipher adalah algoritma kriptografi klasik yang dalam pengkodeannya terdiri dari teknik substitusi dan transposisi. Teknik substitusi adalah proses penggantian karakter pada plainteks. Sedangkan teknik transposisi adalah proses pertukaran huruf. *Affine Cipher* merupakan perluasan dari *Caesar cipher* yang diperkuat dalam penyandiannya.

Salah satu algoritma asimetri adalah *Elliptic Curve Cryptography (ECC).* ECC termasuk ke dalam sistem kriptografi asimetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Dalam sistem ini, masalah logaritma diskrit kurva eliptik digunakan dengan grup kurva eliptik. Struktur kurva eliptik digunakan sebagai grup operasi matematis untuk melakukan proses enkripsi dan dekripsi. Kriptografi kurva eliptik memiliki kelebihan dalam hal panjang kunci yang lebih pendek namun juga memiliki tingkat keamanan yang sama jika dibandingkan dengan algoritma kriptografi asimetris lainnya. Dalam kurva eliptik ini terdapat suatu metode yang dapat digunakan untuk proses penyandian pesan. Metode koblitz ini merupakan cara kedua dari kurva eliptik yang digunakan untuk mengkodekan pesan.

Padma, B., Chandravathi, D., & Roja, P. P menyatakan bahwa kriptografi kurva eliptik atau yang sering disebut dengan *Elliptic Curve Cryptography* (ECC) adalah algoritma kriptografi kunci publik yang lebih baru, meskipun belum dianalisis dengan baik. Pada kriptografi kurva eliptik ini menawarkan tingkat keamanan yang sama dengan algoritma kunci-publik konvensional tetapi dengan ukuran kunci yang lebih pendek. Metode enkripsi dan dekripsi ECC hanya dapat dilakukan dengan mendekripsi titik pada kurva dan bukan pesan. Artikel ini membahas metode Koblitz untuk merepresentasikan pesan ke suatu titik dan sebaliknya. Artikel ini juga menjelaskan hasil implementasi metode Encoding dan Decoding Koblitz (Padma et al., 2010).

Menurut Nasution (2020) algoritma *Affine Cipher* merupakan bagian dari kriptografi klasik yang menggunakan metode substitusi dalam mengamankan data, yaitu dengan cara menggeser plainteks dengan mengalikan nilai plainteks dengan

kunci bilangan prima. Kelemahan dari algoritma ini terletak pada kunci yang mudah digunakan. Pada artikel ini membahas tentang modifikasi *Affine Cipher* dengan menggunakan tiga kombinasi kunci merubah pesan asli (*plaintext)* menjadi pesan yang berkode (*ciphertext)* sehingga pesan menjadi sulit untuk dimengerti maknanya. Kemudian mengembalikan pesan dari bentuk *ciphertext* menjadi *plaintext.* Pesan dienkripsi sehingga data yang lebih acak dapat ditingkatkan dengan modifikasi *Affine Cipher*. Pada penelitiannya hanya memfokuskan pada karakter alphabet (a hingga z), maka diharapkan dapat menambah karakter lainnya. Modifikasi *Affine Cipher* tidak dapat digunakan jika nilai a tidak relatif prima (Nasution, 2020).

Kemudian, penelitian yang dilakukan oleh Setyobudi (2013) menyatakan bahwa proses penyandian menggunakan algoritma dari ElGamal ECC terbatas pada medan berhingga F_P dan didapatkan kode yang merupakan hasil dari proses enkripsi dan dekripsi suatu pesan yang sudah terjamin keamanannya (Setyobudi, 2013).

Berdasarkan beberapa uraian yang telah dijelaskan, maka pada penelitian ini penulis ingin melanjutkan dengan mengambil judul " *Enkripsi dan Dekripsi Pesan Menggunakan Kurva Eliptik pada Affine Cipher dengan metode Koblitz"*.

1.2 Rumusan Masalah

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

1. Bagaimana proses enkripsi menggunakan kurva eliptik pada *Affine Cipher* dengan metode Koblitz untuk mengamankan pesan teks?
2. Bagaimana proses dekripsi menggunakan kurva eliptik pada *Affine Cipher* dengan metode Koblitz untuk mengamankan pesan teks?

1.3 Tujuan Penelitian

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

1. Mengetahui proses enkripsi menggunakan kurva eliptik pada *Affine Cipher* dengan metode koblitz untuk mengamankan pesan teks?
2. Mengetahui proses dekripsi menggunakan kurva eliptik pada *Affine Cipher* dengan metode Koblitz untuk mengamankan pesan teks?

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Bagi penulis, menambah pemahaman tentang mengenai cara menerapkan metode Koblitz pada penyandian kunci.
2. Bagi lembaga, dapat digunakan sebagai rujukan pada penelitian yang membahas kriptografi.
3. Bagi mahasiswa, menambah wawasan keilmuan mengenai pengamanan pesan teks menggunakan *Affine Cipher* pada kurva eliptik dengan metode Koblitz.

1.5 Batasan Masalah

Penelitian ini memfokuskan pada proses enkripsi dan dekripsi pesan dengan metode Koblitz menggunakan persamaan kurva eliptik yang terbatas pada medan berhingga (*finite field)* prima F_P. Dalam penyandian, penulis menggunakan 126 karakter yang digunakan untuk mengonversi *plaintext* pada kode ASCII (*American Standard Code for Information Interchange)* yang terdiri dari karakter (null), huruf alfabet ‘A’ sampai ‘Z’ maupun ‘a’ sampai ‘z’, dan karakter simbol.

1.6 Definisi Istilah

Definisi istilah yang digunakan dalam penelitian ini, secara garis besar dapat ditulis sebagai berikut:

1. Enkripsi

   Enkripsi adalah mengubah pesan asli (*plaintext)* menjadi pesan berkode yang tidak dipahami (*cipher*).

2. Dekripsi

   Dekripsi adalah kebalikan dari enkripsi, yaitu mengembalikan pesan yang telah dienkripsi ke bentuk aslinya. Algoritma yang digunakan untuk deskripsi tentu berbeda dari yang digunakan untuk enkripsi.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Konsep Dasar Matematika Dalam Kriptografi

2.1.1.1 Grup

Grup $(G,*)$ terdiri dari himpunan G bersama-sama dengan operasi biner $*$ pada G, yang memenuhi beberapa aksioma berikut:

1. Tertutup

   Operasi biner $*$ menghasilkan nilai di dalam G, untuk semua a dan b di dalam G,$a * b$ juga berada di dalam G.

2. Assosiatif

   Untuk semua a, b dan c di dalam $G, (a * b) * c = a * (b * c)$.

3. Identitas

   Operasi biner $*$ bersifat identitas jika terdapat sebuah elemen identitas e di G sedemikian sehingga $e * a = a * e = a$.

4. Invers

   Untuk setiap *a* di *G*, terdapat elemen $a^{-1} \in G$ sedemikan hingga:

   $$a * a^{-1} = a^{-1} * a = e$$

   dimana *e* adalah elemen identitas di *G*. Jika ditulis $(G,*)$ maka itu menyatakan sebuah grup dengan operasi penjumlahan. Jika (G, x) menyatakan sebuah grup dengan operasi perkalian.

Sebuah grup dikatakan grup abelian atau grup komutatif jika memenuhi sifat komutatif: $P + Q = Q + P, \forall a, b \in G$ (Munir, 2019). Grup berhingga

(*finite group)* adalah sebuah grup memiliki jumlah elemen berhingga dan order dari grup disebut banyak elemen dalam grup tersebut.

2.1.1.2 Gelanggang (*Ring)*

Misalkan R adalah suatu himpunan tak kosong $(R, +, \times)$ dengan dua operasi biner $+$ dan $\times$. Maka sistem $(R, +, \times)$ disebut *ring* jika memenuhi aksioma sebagai berikut:

1. $(R, +)$ adalah grup abelian dengan elemen identitas 0.
2. Operasi perkalian bersifat asosiatif, yaitu $a \times (b \times c) = (a \times b) \times c$ untuk semua $a, b, c \in R$
3. Terdapat elemen identitas perkalian yang dinyatakan dengan 1, dimana $1 \neq 0$, sedemikian sehingga $1 \times a = a \times 1 = a$, untuk semua $a \in R$.
4. Operasi perkalian bersifat distributif pada penjumlahan, yaitu:

   $a \times (b + c) = (a \times b) + (a \times c)$ dan

   $(b + c) \times a = (b \times a) + (c \times a), \forall\, a, b, c \in R$.

Sebuah ring dikatakan ring komutatif jika berlaku $a \times b = b \times a, \forall\, a, b \in R$.

Definisi 2.1.1.2.2

Suatu Ring $(R, +, \times)$ disebut ring komutatif jika dan hanya jika operasi biner kedua yaitu perkalian $(\times)$ bersifat komutatif di R (Gilbert, 2015).

Contoh :

Diberikan $(\mathbb{Z}, +, \times)$ ring dengan $\mathbb{Z}$ adalah himpunan bilangan bulat maka :

$a \times b = b \times a, \forall\, a, b \in \mathbb{Z}$ (komutatif)

Jadi $(\mathbb{Z}, +, \times)$ adalah ring komutatif.

2.1.1.3 Medan F_p

Medan F adalah sebuah ring komutatif dimana setiap elemen tak-nol mempunyai balikan perkalian. Balikan perkalian adalah untuk setiap $a \neq 0$ yang termasuk di dalam F, terdapat elemen $a^{-1} \in F$ sedemikian sehingga $a \times a^{-1} = 1$ (Munir, 2019).

2.1.1.4 Medan Berhingga F_p

Untuk p bilangan prima, maka F_p adalah medan berhingga berorde p dengan anggotanya adalah $Z_P = \{0, 1, 2, p-1\}$, yang dalam hal ini operasi penjumlahan dan perkalian dilakukan dalam modulus p, yang didefinisikan sebagai berikut:

1. Penjumlahan

   jika $a, b \in F_p$, maka $a + b = r$, yang dalam hal ini $r = (a + b) mod\ p$.

2. Perkalian

   jika $a, b\ \in F_p$, maka $a \times b = s$, yang dalam hal ini $s = (a \times b) mod\ p$.

   Semua operasi penjumlahan dan perkalian di dalam F_p selalu menghasilkan nilai di dalam himpunan $\{0, 1, 2, p-1\}$.

2.1.1.5 Aritmetika Integer

Operasi aritmatika terdiri dari penjumlahan, perkalian, pengurangan, dan pembagian. Pada aritmatika *integer* terdiri dari himpunan *integer* dan operasi aritmatika. Himpunan *integer* dapat disimbolkan dengan $\mathbb{Z}$ yang merupakan bilangan bulat dari $-\infty$ sampai ∞ seperti,

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

Pada bilangan bulat memiliki 3 operasi biner: penjumlahan $(a + b)$, pengurangan $(a - b)$, dan perkalian $(a \text{ x } b)$. Operasi pembagian $\frac{a}{n}$ pada bilangan *integer* diinterpretasikan memiliki hasil bagi (q) dan sisa bagi (r) (Sadikin, 2012).

Contoh:

Jika $a = 33, n = 16$ dapat ditemukan $q = 2$ (*integer* terbesar yang $n \times q \leq a$) dan sisa bagi $r = 1$ atau memenuhi $a = q \times n + r$ yaitu $33 = 2 \times 16 + 1$.

Suatu bilangan *a* dikatakan habis dibagi oleh *n* jika tidak memiliki sisa bagi $(r = 0)$ atau $a = n \times q$ dinyatakan dengan $a|n$. Sedangkan $a \nmid n$ menyatakan bahwa *a* tidak habis dibagi *n.* Himpunan *integer* yang membagi habis sebuah *integer* disebut dengan *divisor*, 42 memiliki *divisor* {1,2,3,6,7,14,21,42}. Perhatikan bahwa bilangan 1 yang memiliki satu *divisor* sedangkan *integer* lainnya memiliki paling sedikit dua *divisor* yaitu bilangan itu sendiri dan 1. *Integer* p yang memiliki *divisor* {1, p} disebut bilangan prima selain itu merupakan bilangan komposit.

Selanjutnya, salah satu sifat pembagian dalam matematika yaitu keterbagian merupakan salah satu pokok bahasan dari teori bilangan. Penjelasan mengenai definisi dan teorema yang berkaitan dengan keterbagian telah banyak dijelaskan banyak buku dengan penjelasan yang berbeda.

Definisi Keterbagian:

Untuk setiap $a, b \in \mathbb{Z}$ dengan $a \neq 0$. a dikatakan habis membagi b jika ada $k \in \mathbb{Z}$ yang memenuhi $a = k \cdot b$ dan dinotasikan $a|b$ (Irawan et al., 2014).

Contoh:

a. $4|24$ karena ada $6 \in \mathbb{Z}$, sehingga $24 = 4 \cdot 6$
b. $4 \nmid 15$ karena ada $15 \neq 4 \cdot c$, untuk setiap $c \in \mathbb{Z}$.

2.1.1.6 Aritmatika Modulo

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a \bmod m$ memberikan sisa apabila a dibagi dengan *m.* Bilangan m disebut modulus atau modulo, dan hasil operasi modulo m terletak di dalam himpunan $\{0, 1, 2, \ldots, m-1\}$. $a(mod\ m) \equiv r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r \leq m$ (Munir, 2019).

1. Kekongruenan

   Jika $m > 0$ dan $m|(a-b)$ maka terdapat suatu bilangan bulat t sehingga $a - b = mt$. Sehingga $a \equiv b\ (mod\ m)$ dapat dinyatakan sebagai $a - b = mt$, maka dapat diartikan dengan $a \equiv b\ (mod\ m)$ atau beda antara a dan b merupakan kelipatan *m*. Jadi $a \equiv b\ (mod\ m)$ dapat juga dinyatakan dengan $a = mt + b$, yaitu $a = b$ ditambah kelipatan *n* (Irawan et al., 2014).

   Teorema 2.1.4.1

   Misalkan *m* adalah bilangan bulat positif.

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

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

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

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

   Bukti**:**

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

      $$\Leftrightarrow a = b + km$$

      $$\Leftrightarrow a - b = km$$

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

$$\Leftrightarrow ac = bc + Km$$

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

b. $a \equiv b \ (mod\ m) \Leftrightarrow a = b + k1m$

$$c \equiv d \ (mod\ m) \Leftrightarrow c = d + k2m +$$

$$\Leftrightarrow (a + c) = (b + d) + (k1 + k2)m$$

$$\Leftrightarrow (a + c) = (b + d) + km \ \ (k = k1 + k2)$$

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

Contoh:

$32 \equiv 4 \ (mod\ 7)$ karena $32 - 4$ terbagi oleh 5

$24 \not\equiv 4 \ (mod\ 6)$ karena $24 - 4$ tidak terbagi oleh 6

$-8 \equiv 24 \ (mod\ 16)$ karena $-8 - 24$ terbagi oleh 16

$-8 \not\equiv 24 \ (mod\ 10)$ karena $-8 - 24$ tidak terbagi oleh 10

Kekongruenan $a \equiv b \ (mod\ m)$ dapat juga dituliskan dalam hubungan

$$a = b + km$$

dalam hal ini *k* merupakan bilangan bulat.

Contoh:

$18 \equiv 3 \ (mod\ 3)$ dapat ditulis sebagai $18 = 3 + 5 \cdot 3$

$-7 \equiv 13 \ (mod\ 10)$ dapat ditulis sebagai $-7 = 13 + (-3)10$

Contoh:

Misalkan $18 \equiv 3 \ (mod\ 3)$ dan $12 \equiv 3 \ (mod\ 3)$

$18 + 5 = 3 + 5 \ (mod\ 3) \Leftrightarrow 23 = 8 \ (mod\ 3)$

$18 \cdot 5 = 5 \cdot 3 \ (mod\ 3) \Leftrightarrow 90 = 15 \ (mod\ 3)$

$18 + 12 = 3 + 3 \ (mod\ 3) \Leftrightarrow 30 = 6 \ (mod\ 3)$

$18 \cdot 12 = 3 \cdot 3 \ (mod\ 3) \Leftrightarrow 216 = 9 \ (mod\ 3)$

2. Balikan Modulo *(modulo invers*)

   Balikan (invers) perkalian di dalam bilangan riil dapat ditunjukkan sebagai balikan dari a adalah $1/a$ sedemikian sehingga $a \times \frac{1}{a} = 1$. Bilangan bulat a memiliki balikan dalam modulus m hanya jika a dan m relatif prima dan $m > 1$. Balikan dari $a\ (mod\ m)$ adalah sebuah bilangan bulat a^{-1}sedemikan sehingga

   $$a \times a^{-1} \equiv 1\ (mod\ m)$$

   Jadi, dapat ditulis $a^{-1}(mod\ m)$ balikan dari $a(mod\ m)$.

2.1.2 Kriptografi

Kriptografi adalah cabang matematika yang berhubungan dengan teknik keamanan informasi, yang mencakup berbagai kerahasiaan data, integritas data, dan otentikasi. Kriptografi juga dapat diartikan sebagai ilmu yang digunakan untuk menjaga keamanan pesan. Kriptografi *(cryptography)* berasal dari bahasa Yunani, yang terdiri dari kata *cryptos* yang berarti tersembunyi dan *graphein* yang berarti menulis atau tulisan. Secara terminologi, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari suatu tempat ke tempat lain (Ariyus, 2006). Kriptografi juga dapat diartikan ilmu dan seni untuk menjaga kerahasiaan pesan dengan menyandikan pesan ke dalam bentuk yang tidak dapat dipahami maknanya lagi (Meyer & Matyas, 1982).

Menurut sejarahnya, tentara Sparta di Yunani pada permulaan tahun 400 SM sudah menggunakan alat yang disebut *scytale*. Alat ini terdiri dari sebuah gulungan pita dari daun *papyrus* yang dililitkan pada batang silinder (Munir, 2019).

Ada istilah yang sering ditemukan atau terminologi dalam kriptografi, yaitu pesan, *plaintext*, *ciphertext*, pengirim, penerima, sistem kriptografi, penyadap, kriptanalisis, dan kriptologi.

a. Pesan, *Plainteks*, dan *Cipherteks*

Pesan merupakan sebuah informasi yang dapat dibaca, dan dipahami artinya. Pesan dapat berupa teks, citra, suara / suara (audio), video, atau bentuk biner lainnya, baik digital maupun analog. *Plaintext* disebut sebagai pesan teks. *Ciphertext* merupakan pesan teks yang dikodekan. Pesan yang dikodekan harus dapat dibalik menjadi pesan yang dapat dimengerti.

b. Pengirim dan Penerima

Ada dua entitas pertukaran pesan yaitu mencakup pengirim dan penerima. Pengirim adalah entitas yang mengirim pesan kepada penerima. Penerima adalah entitas yang menerima pesan. Tidak hanya berupa orang, pengirim juga dapat berupa mesin, robot, atau komputer (Munir, 2019).

c. Sistem Kriptografi

Sebuah himpunan yang berisikan algoritma enkripsi, algoritma dekripsi, ruang kunci, semua *plaintext* dan *ciphertext* disebut dengan sistem kriptografi (*cryptosystem*). Kriptografi terbagi dari dua jenis sistem, yang pertama yaitu sistem kriptografi kunci-simetri (*symmetric-key cryptosystem*) dan yang kedua sistem kriptografi kunci-publik (*public-key cryptosystem*). Terdapat perbedaan dari kedua sistem tersebut, yaitu dalam proses enkripsi dan dekripsi. Sistem pertama menerapkan kunci yang sama, sedangkan sistem kedua menerapkan kunci yang berbeda untuk enkripsi dan dekripsi.

d. Penyadap

Orang yang ingin mengetahui isi pesan dalam proses pengiriman disebut penyadap. Dengan cara mencari informasi pada sistem kriptografi penyadap akan mengetahui isi pesan tersebut. Cara tersebut dilakukan agar penyadap dapat memecahkan pesan berkode (*ciphertext*).

e. Kriptanalisis

Ilmu yang digunakan untuk menyelesaikan cipherteks tanpa mengetahui kunci yang dipakai dalam enkripsi-dekripsi disebut kriptanalisis. Pelaku kriptanalisis disebut kriptanalis (Munir, 2019).

2.1.2.1 Algoritma Kriptografi

Algoritma kriptografi adalah langkah logis bagaimana menyembunyikan pesan dari orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi yang digunakan untuk enkripsi dan dekripsi disebut juga *chiper* dapat diartikan sebagai aturan untuk *enchipering* dan *deciphering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *chiper* memerlukan algoritma yang berbeda untuk proses enkripsi dan dekripsi. Proses tersebut membutuhkan sebuah kunci untuk enkripsi dan dekripsi pesan. Untuk enkripsi kuncinya juga bisa sama dengan deskripsi tetapi ada juga sekelompok algoritma kriptografi dengan kunci yang berbeda untuk enkripsi dan dekripsi.

Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu :

1. Enkripsi, merupakan hal yang sangat penting dalam kritik reaksi yang merupakan pengaman data yang dikirimkan terjaga rahasianya. Pesan asli disebut *plaintext* yang diubah menjadi kode yang tidak dipahami, enkripsi ini dapat disebut dengan *cipher* atau kode.

2. Dekripsi, adalah kebalikan dari mengenkripsi pesan yang telah dienkripsi dikembalikan ke bentuk aslinya yang disebut deskripsi pesan. Algoritma yang digunakan untuk deskripsi tentu berbeda dari yang digunakan untuk enkripsi.
3. Kunci, adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian yaitu: kunci rahasia (private key) dan kunci umum (public key*)* (Ariyus, 2006).

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi algoritma kriptografi dapat dikelompokkan ke dalam kelompok algoritma kunci simetri dan algoritma kunci asimetris.

A. Algoritma Simetris

Algoritma simetris merupakan algoritma kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Algoritma simetris sering juga disebut algoritma kunci tunggal. Sebelum berkomunikasi pengirim dan penerima diharuskan menyepakati sebuah kunci. Tingkat keamanan algoritma simetris tergantung pada kuncinya, oleh karena itu kunci tersebut harus dirahasiakan. Algoritma simetris mempunyai kelebihan dan kekurangan. Kelebihan pada algoritma ini yaitu pada tingkat kecepatan saat melakukan proses enkripsi dan dekripsi lebih cepat dibandingkan dengan algoritma asimetris. Kelemahan algoritma simetris ini terletak pada penggununaan kunci, sehingga jika melakukan pertukaran informasi dengan pengguna lain harus membuat kunci yang berbeda agar terjadi kesulitan dalam memecahkan kunci tersebut. Contoh algoritma simetris adalah cipher permutasi, cipher substitusi, *Hill Cipher,* OTP, RC6, Twofish (Ariyus, 2008).

B. Algoritma Asimetris

Algoritma asimetris sering juga dikenal dengan algoritma kunci publik. Ketika melakukan proses pengiriman pesan pada algoritma asimetris ini menggunakan dua jenis kunci yaitu kunci publik (*public key)* dan kunci privat (*private key*). Keuntungan pada algoritma yaitu memberikan keamanan bagi pelaku pertukaran informasi walaupun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya. Kelemahan dari algoritma asimetris ini terletak pada lebih rendahnya proses melakukan enkripsi dan dekripsi dibandingkan dengan algoritma simetris. Kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi lebih panjang. Contoh dari algoritma asimetris adalah RSA, *Elgamal*, McEliece, LUC dan DSA (*Digital Signature Algorithm*) (Ariyus, 2008).

2.1.2.2 Kriptografi Kurva Eliptik

Kriptografi yang menggunakan kurva eliptik dinamakan kriptografi kurva eliptik. Kriptografi kurva eliptik termasuk ke dalam sistem kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Kurva eliptik adalah kurva matematik yang memiliki salah satu sifat yaitu ketertutupan, yaitu operasi penjumlahan dua buah titik di dalam kurva eliptik yang selalu menghasilkan titik yang terletak di kurva eliptik.

Operasi matematika yang digunakan pada kriptografi kurva eliptik didefinisikan dengan persamaan:

$$y^2 = x^3 + ax + b \tag{2.1}$$

dengan syarat

$$4a^3 + 27b^2 \neq 0$$

Setiap nilai a dan b yang berbeda memberikan kurva eliptik yang berbeda. Untuk menggambar kurva, maka perlu dihitung:

$$y = \sqrt{x^3 + ax + b}$$

Untuk nilai a dan b yang diberikan, gambar akan bernilai positif dan negatif pada y untuk setiap nilai x. Sehingga setiap kurva eliptik akan berbebtuk simetris terhadap sumbu x atau garis $y = 0$. Kurva eliptik juga dapat dipandang sebagai suatu himpunan yang terdiri dari titik-titik (x, y) yang memenuhi persamaan $y^2 = x^3 + ax + b$. Himpunan tersebut dinotasikan dengan $E(a, b)$. Untuk setiap nilai a dan b yang berbeda memberikan kurva eliptik yang berbeda (Stallings, 2017).

2.1.2.3 Kurva Eliptik pada GF(p) atau F_p

Bentuk umum kurva eliptik pada GF(p) atau F_p adalah sebagai berikut:

$$y^2 = x^3 + ax + b \ (mod\ p)$$

Dalam hal ini p adalah bilangan prima dan elemen-elemen di dalam medan galois adalah $\{0, 1, 2, 3, \dots, p-1\}$

Contoh: Tentukan semua titik $P(x, y)$ pada kurva eliptik $y^2 = x^3 + 2x + 5\ (mod\ 11)$ dengan x dan y didefinisikan di dalam GF(11).

Jawaban: Elemen-elemen dalam $GF(11)$ adalah $\{0, 1, 2, 3, 4, \dots, 10\}$. Lakukan perhitungan untuk menentukan semua titik di dalam kurva eliptik dengan persamaan $y^2 = x^3 + 2x + 5\ (mod\ 11)$ sebagai berikut:

$x = 1 \rightarrow y^2 = 8\ mod\ 11$ → Tidak ada hasil yang memenuhi

$x = 2 \rightarrow y^2 = 17 mod\ 11$ → Tidak ada hasil yang memenuhi

$x = 3 \rightarrow y^2 = 38\ mod\ 11$ → $y_1 = 4$ dan $y_2 = 7$ → $P_1(3, 4)$ dan $P_2(3, 7)$

$x = 4 \rightarrow y^2 = 77\ mod\ 11 \rightarrow y_1 = 0$ dan $y_2 = 0 \rightarrow P_1(4,0)$ dan $P_2(4,0)$

$x = 5 \rightarrow y^2 = 140 mod\ 11 \rightarrow$ Tidak ada hasil yang memenuhi

$x = 6 \rightarrow y^2 = 233\ mod\ 11 \rightarrow$ Tidak ada hasil yang memenuhi

$x = 7 \rightarrow y^2 = 362\ mod\ 11 \rightarrow$ Tidak ada hasil yang memenuhi

$x = 8 \rightarrow y^2 = 533\ mod\ 11 \rightarrow y_1 = 4$ dan $y_2 = 7 \rightarrow P_1(8,4)$ dan $P_2(8,7)$

$x = 9 \rightarrow y^2 = 752\ mod\ 11 \rightarrow y_1 = 2$ dan $y_2 = 9 \rightarrow P_1(9,2)$ dan $P_2(9,9)$

$x = 10 \rightarrow y^2 = 1025\ mod\ 11 \rightarrow$ Tidak ada hasil yang memenuhi

Sehingga diperoleh tabel 2.1 sebagai berikut:

Tabel 2.1 Hasil Titik pada Kurva Eliptik

x	y^2	$y_{1,2}$	$P_1(x,y)$	$P_2(x,y)$
0	5	(4, 7)	(0, 4)	(0, 7)
1	8	-	-	-
2	6	-	-	-
3	5	(4, 7)	(3, 4)	(3, 7)
4	0	0	(4, 0)	(4, 0)
5	8	-	-	-
6	2	-	-	-
7	10	-	-	-
8	5	(4, 7)	(8, 4)	(8, 7)
9	4	(2, 9)	(9, 2)	(9, 9)
10	2	-	-	-

2.1.2.4 *Affine Cipher*

Affine Cipher merupakan *monoalphabetic substitution cipher* yang setiap huruf-huruf alfabetnya dapat diubah ke dalam angka-angka, kemudian dienkripsi dan dekripsi dengan suatu persamaan. Kunci untuk enkripsi algoritma *affine cipher*

terdiri dari dua parameter *m* dan *b*. Supaya *m* mempunyai invers (a^{-1}), maka *m* harus memenuhi $(m, n) = 1$ (Kromodioeljo, 2010).

A. Enkripsi *Affine Cipher*

Proses enkripsi pada *Affine cipher* menggunakan dua buah kunci (*m*) dan kunci (*b*) untuk dapat menghasilkan *ciphertext*. *Plaintext* (*P*) akan dikonversikan menggunakan tabel konversi, dan akan diperoleh sebuah *ciphertext* (C) dari proses enkripsi *plaintext* pada persamaan

$$C \equiv mP + b \ (mod\ n) \tag{2.2}$$

Pada persamaan 2.2 di atas dijelaskan bahwa *C* merupakan *ciphertext* dari *P* yang masing-masing merupakan pergeseran karakter dari *plaintext. m* adalah bilangan bulat yang harus relatif prima dengan *n*, apabila *m* tidak relatif prima dengan *n* maka proses dekripsi pesan tidak dapat dilakukan. Sedangkan kunci *b* merupakan pergeseran nilai relative prima dari kunci *m.* Agar memperoleh *ciphertext* maka dilakukan perhitungan dengan persamaan di atas dan mengonversi bilangan desimal menggunakan tabel (Munir, 2019).

Contoh**:**

Diberikan suatu pesan atau *plaintext* KRIPTO. *Plaintext* tersebut akan dienkripsi mengunakan *Affine Cipher*.

Langkah pertama yang dilakukan yaitu mengonversi karakter pada *plaintext* pada tabel ASCII, seperti pada Tabel 2.2.

Tabel 2.2 Hasil Konversi pada Tabel ASCII

Karakter	**Angka**
K	75
R	82
I	73
P	80
T	84
O	79

Langkah selanjutnya menentukan dua kunci yang akan digunakan untuk proses enkripsi, yaitu kunci m = 7 (karena 7 relatif prima dengan 97), dan kunci b = 10. Kemudian dengan persamaan rumus enkripsi pada (2.2) diperoleh hasil enkripsi seperti pada Tabel 2.3

Tabel 2.3 Hasil Proses Enkripsi

Plaintext	$C \equiv mP + b \ (mod\ 127)$
75	$C \equiv 7 \cdot 75 + 10\ mod\ 127$ $\equiv 27\ mod\ 127 =$ karakter W
82	$C \equiv 7 \cdot 82 + 10\ mod\ 127$ $\equiv 76\ mod\ 127 =$ karakter HT
73	$C \equiv 7 \cdot 73 + 10\ mod\ 127$ $\equiv 13\ mod\ 127 =$ huruf I
80	$C \equiv 7 \cdot 80 + 10\ mod\ 127$ $\equiv 62\ mod\ 127 =$ huruf z
84	$C \equiv 7 \cdot 84 + 10\ mod\ 127$ $\equiv\ 90\ mod\ 127 =$ karakter ETB
79	$C \equiv 7 \cdot 79 + 10\ mod\ 127$ $\equiv 55\ mod\ 127 =$ huruf s

Pada tabel (2.3) diperoleh hasil ciphertext yang sudah dikonversi menggunakan tabel ASCII maka menjadi WHTIzETBs

B. Dekripsi *Affine Cipher*

Proses dari dekripsi *Affine Cipher* menggunakan dua kunci yang sama dengan kunci pada saat proses enkripsi. Agar diperoleh sebuah *plaintext* maka kunci (m) akan diubah dalam bentuk invers m, dan dituliskan dengan $m^{-1}\ (mod\ n)$. Sehingga rumus persamaan dekripsi sebagai berikut:

$$P \equiv m^{-1}(C - b)(mod\ n) \tag{2.3}$$

Pada rumus persamaan 2.3 dijelaskan bahwa *P* merupakan *plaintext* dari pergeseran karakter pada *ciphertext.* Sedangkan *C* adalah pergeseran karakter pada *ciphertext*. a^{-1} dan b merupakan dua kunci yang sama dengan kunci yang digunakan pada proses enkripsi. Sebelum melakukan proses dekripsi, maka *P* dan *C* harus dikonversi ke dalam bentuk bentuk desimal dan hasil dari perhitungannya akan dikonversi Kembali menggunakan tabel ASCII untuk memperoleh *plaintext*.

Contoh:

Mencari kunci $m^{-1}\ mod\ 125$ yang akan digunakan pada proses dekripsi

$$m^{-1} = 7x \equiv 1\ mod\ 127$$

$$= 7(109) \equiv 1 mod\ 127$$

Setelah mendapatkan $m^{-1} = 109$ dan $b = 10$, maka dapat dilakukan proses dekripsi. Dari *ciphertext* yang berupa WHTIzETBs akan dikonversi menjadi angka menggunakan tabel ASCII seperti pada tabel 2.4

Tabel 2.4 Konversi Karakter Menggunakan Kode ASCII

Karakter	**Angka**
ESC	27
L	76
CR	13
>	62
Z	90
7	55

Lakukan proses dekripsi menggunakan rumus dekripsi pesan pada algoritma *Affine Cipher* seperti pada Tabel 2.5 dibawah ini:

Tabel 2.5 Proses Dekripsi pada *Affine Cipher*

Ciphertext	$P \equiv m^{-1}(C-b)(mod\ 127)$
27	$P \equiv 109\ (27-10)(mod\ 127) \equiv 75\ mod\ 127$
76	$P \equiv 109(76-10)(mod\ 127)\ \equiv 82\ mod\ 127$
13	$P \equiv 109(13-10)(mod\ 127)\ \equiv 73\ mod\ 127$
62	$P \equiv 109(62-10)(mod\ 127)\ \equiv 80\ mod\ 127$
90	$P \equiv 109(90-10)(mod\ 127) \equiv 84\ mod\ 127$
55	$P \equiv 109(55-10)(mod\ 127) \equiv 79\ mod\ 127$

Dari tabel (2.5) didapatkan *plaintext* berupa angka yaitu 75 82 73 80 84 79, kemudian dikonversi menggunakan tabel ASCII dan mendapatkan sebuah pesan asli yaitu KRIPTO.

2.1.3 Kode ASCII

ASCII (*American Standard Code for Information Interchange)* yang merupakan salah satu standar yang banyak digunakan pada komputer dan perangkat komunikasi, untuk merepresentasikan sebuah karakter. Kode ASCII memiliki komposisi bilangan biner sebanyak 8 bit. Mulai dari 00000000 hingga 11111111. Total kombinasi yang dihasilkan adalah 256, dimulai dari kode 0 hingga 255, terdiri dari abjad a-z dan A-Z, angka 0-9, beberapa tanda baca yang umum digunakan, dan beberapa karakter kontrol (Kurnia, 2013).

2.1.4 Metode Koblitz

Metode Koblitz merupakan metode yang dikembangkan oleh Neil Koblitz. Yang digunakan untuk implementasi kriptografi kurva eliptik pengkodean *plaintext*. Pada pengkodean ini harus dilakukan sebelum enkripsi dan dekripsi. Metode enkripsi dan dekripsi ECC hanya dapat mengenkripsi dan dekripsi titik pada kurva dan bukan pesan. Oleh karena itu, sembarang pesan harus dikodekan terlebih dahulu menjadi titik pada kurva eliptik. Cara yang paling sederhana adalah mengkodekan setiap karakter pesan ke dalam kode ASCII. Metode Koblitz ini merupakan cara kedua untuk mengkodekan pesan. Dengan beberapa langkah-langkah yang telah ditentukan (Padma et al., 2010).

2.2 Kajian Integrasi Topik dengan Al-Quran/Hadist

Menyampaikan pesan yang dikirimkan dan bertujuan agar pesan yang disampaikan terjaga keamananya merupakan suatu amanah yang harus dijaga. Secara etimologi Amanah berasal dari bahasa Arab yang masih berbentuk mashdar

dari kata (amina-amanatan) yang berarti jujur atau dapat dipercaya. Dari pengertian tersebut dapat diambil suatu pengertian bahwa Amanah adalah menyampaikan hak kepada pemiliknya, tidak megambil sesuatu melebihi haknya dan tidak mengurangi hak orang lain. Amanah merupakan kepercayaan yang diberikan orang lain terhadapnya sehingga menimbulkan ketenangan jiwa. Hal ini dijelaskan dalam al-Qur'an surat an-Nisa' 58 ((LPMQ), 2022).

"*Sungguh, Allah menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baiknya yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat"* (QS. an-Nisa':58)

(Sesungguhnya Allah menyuruh kamu untuk menyampaikan amanat) artinya kewajiban-kewajiban yang dipercayakan dari seseorang (kepada yang berhak menerimanya). Ayat ini turun ketika Ali ra hendak mengambil kunci Ka'bah dari Usman bin Thalhah al-Hajabi penjaganya secara paksa yakni ketika Nabi Saw dating ke Mekah pada tahun pembebasan. Usman ketika itu tidak mau memberikannya lalu katanya, "Seandainya saya tahu bahwa ia Rasulullah tentulah saya tidak akan menghalanginya." Maka Rasulullah Saw pun menyuruh mengembalikan kunci itu padanya seraya bersabda, "Terimalah ini untuk selama-lamanya tiada putus-putusnya!" Usman merasa heran atas hal itu lalu dibacakannya ayat tersebut sehingga Usman pun masuk Islam. Ketika akan meninggal kunci itu diserahkan kepada saudaranya Syaibah lalu tinggal pada anaknya. Ayat ini walaupun dating dengan sebab khusus tetapi umumnya berlaku disebabkan persamaan di antaranya (dan apabila kamu mengadili di antara manusia) maka Allah menitahkanmu (agar menetapkan hukum dengan adil. Sesungguhnya Allah amat baik sekali) pada ni'imma diidghamkan mim kepada ma, yaitu nakirah

maushufah artinya ni'ma syaian atau sesuatu yang amat baik (nasihat yang diberikann-Nya kepadamu) yaitu menyampaikan amanat dan menjatuhkan putusan secara adil. (Sesungguhnya Allah Maha Mendengar) akan semua perkataan (lagi Maha Melihat) segala perbuatan (Asy-Syuyuthi, 2009).

2.3 Kajian Topik dengan Teori Pendukung

Penelitian ini disusun menggunakan beberapa teori pendukung, seperti kriptografi kurva eliptik, kriptografi kurva eliptik termasuk ke dalam sistem kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Kurva eliptik adalah kurva matematik yang memiliki salah satu sifat yaitu ketertutupan, yaitu operasi penjumlahan dua buah titik di dalam kurva eliptik yang selalu menghasilkan titik yang terletak di kurva eliptik. Operasi matematika yang digunakan pada kriptografi kurva eliptik didefinisikan dengan persamaan $y^2 = x^3 + ax + b$ (Munir, 2019). Pada kriptografi kurva eliptik juga membahas mengenai aljabar abstrak yang meliputi grup, ring, medan F_p, medan berhingga F_p, kemudian teori pendukung lain yaitu *affine cipher* yang merupakan *monoalphabetic substitution cipher* yang setiap huruf-huruf alfabetnya dapat diubah ke dalam angka-angka, kemudian dienkripsi dengan suatu persamaan. Kunci untuk enkripsi algoritma *affine cipher* terdiri dari dua parameter *m* dan *b*. Supaya *m* mempunyai invers (a^{-1}), maka *m* harus memenuhi $(m, n) = 1$ (Kromodioeljo, 2010), teori pendukung yang terakhr yaitu metode Koblitz. Metode Koblitz merupakan metode yang dikembangkan oleh Neil Koblitz. Yang digunakan untuk implementasi kriptografi kurva eliptik pengkodean *plaintext*. Pada pengkodean ini harus dilakukan sebelum enkripsi dan dekripsi. Metode enkripsi dan dekripsi ECC

hanya dapat mengenkripsi dan dekripsi titik pada kurva dan bukan pesan. Oleh karena itu, sembarang pesan harus dikodekan terlebih dahulu menjadi titik pada kurva eliptik. Cara yang paling sederhana adalah mengkodean setiap karakter pesan ke dalam kode ASCII. Metode Koblitz ini merupakan cara kedua untuk mengkodekan pesan. Dengan beberapa langkah-langkah yang telah ditentukan (Padma et al., 2010).

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

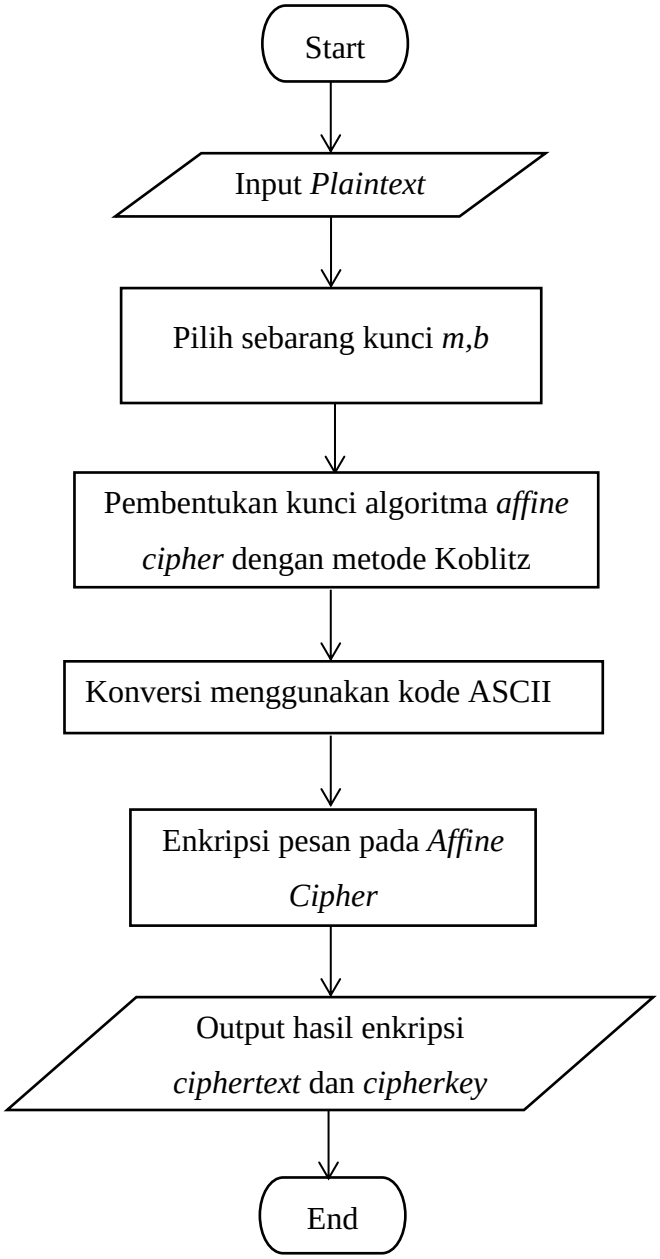
Penelitian ini menggunakan jenis penelitian kualitatif, yang lebih menekankan pada aspek pengamatan, pemahaman secara mendalam pada suatu objek yang digunakan (Siyoto & Sodik, 2015). Penelitian ini menggunakan metode kajian pustaka (*library research)*. Kajian pustaka yaitu kajian yang dilakukan pada buku, jurnal penelitian, laporan penelitian, tesis, skripsi, dan diskusi ilmiah dengan topik yang berkaitan dengan *Affine Cipher*, kurva eliptik, metode Koblitz.

3.2 Tahapan Penelitian

Metode yang digunakan pada penelitian ini adalah metode kajian pustaka (*library research)*. Kajian yang dilakukan pada buku, jurnal penelitian, laporan penelitian, tesis, skripsi, dan diskusi ilmiah dengan topik yang berkaitan dengan kurva elliptik, algoritma *Affine Cipher* dan metode Koblitz.

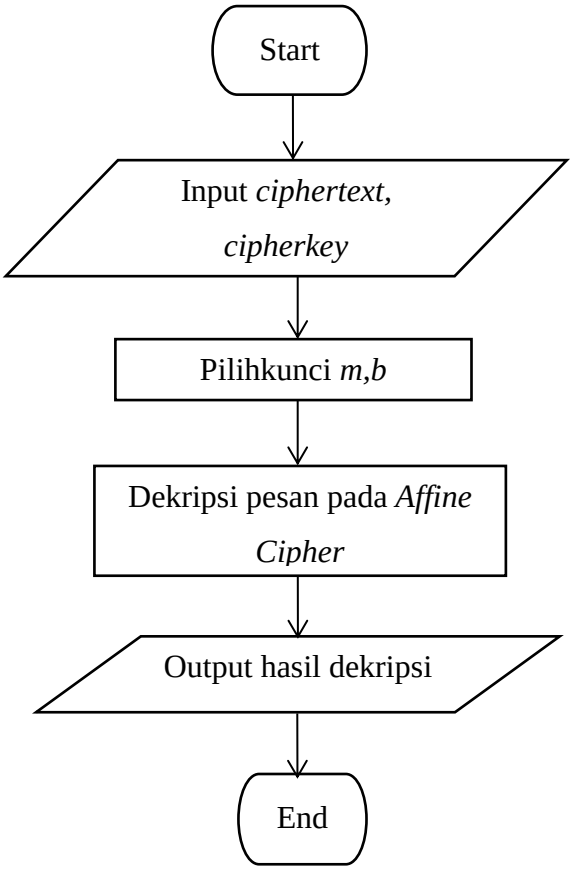
Untuk mencapai tujuan maka langkah-langkah yang dilakukan adalah:

1. Enkripsi pesan menggunakan kurva eliptik pada *Affine Cipher* dengan metode Koblitz.
    a. Menentukan *plaintext.*
    b. Melakukan enkripsi pesan teks menggunakan algoritma *Affine Cipher*.
    c. Menentukan persamaan kurva eliptik pada medan (*field*) berhingga prima F_p.
    d. Melakukan proses enkripsi kunci algoritma *Affine Cipher* dengan kurva eliptik metode Koblitz



Gambar 3.1 *Flowchart* Enkripsi Menggunakan *Affine Cipher* Metode Koblitz

2. Dekripsi pesan menggunakan kurva eliptik pada *Affine Cipher* dengan metode Koblitz
   a. Melakukan proses dekripsi kunci dari *Affine Cipher* dengan metode Koblitz.
   b. Melakukan dekripsi pesan teks menggunakan algoritma *Affine Cipher* dan menghasilkan sebuah *plaintext*.



Gambar 3.2 Flowchart Proses Dekripsi Pesan

BAB IV
HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang proses enkripsi dan dekripsi pesan menggunakan kriptografi kurva eliptik pada algoritma *Affine Cipher* dengan metode Koblitz. Kurva eliptik mempunyai ilmu matematika pada setiap prosesnya. Pada penelitian ini dilakukan proses enkripsi dan dekripsi dengan menggunakan algoritma *Affine Cipher* pada kriptografi kurva eliptik dengan metode Koblitz.

4.1 Enkripsi Pesan Menggunakan algoritma *Affine Cipher*

Proses enkripsi pesan dilakukan oleh pengirim dengan menggunakan algoritma *Affine Cipher*. Kunci yang digunakan pengirim adalah kunci simetris dari algoritma *Affine Cipher*. Oleh karena itu, hal yang harus diperhatikan yaitu menentukan dua kunci *m* dan *b* pada algoritma *Affine Cipher* yang digunakan untuk proses enkripsi pesan asli (*plaintext)*.

4.1.1 Pembentukan Kunci Simetris Algoritma *Affine Cipher*

Algoritma *Affine Cipher* menggunakan dua kunci untuk melakukan proses enkripsi dan dekripsi yaitu kunci simetris. Dalam hal ini, pengirim menggunakan kunci *m.* Kunci *m* adalah bilangan bulat yang harus relatif prima dengan *n* (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan *b* adalah jumlah pergeseran. Pengirim menentukan kunci $m = 3$ dan $b = 8$ yang digunakan untuk proses enkripsi dan dekripsi pesan pada algoritma *Affine Cipher*.

4.1.2 Proses Enkripsi Pesan Menggunakan Algoritma *Affine Cipher*

Proses enkripsi pesan pengirim menentukan pesan asli (*plaintext)* yang akan disandikan menggunakan algoritma *Affine Cipher*. Berikut ini langkah-langkah dalam proses enkripsi pesan:

a. Menentukan *plaintext.* Misalkan pesan yang dikirim berisi kalimat **MATEMATIKA UIN MALANG**

b. Mengkonversi *plaintext* menggunakan kode ASCII 127.

Tabel 4.1 Konversi *plaintext* pada kode ASCII

Plaintext	Kode ASCII	*Plaintext*	Kode ASCII
M	77	U	85
A	65	I	73
T	84	N	78
E	69	Spasi	32
M	77	M	77
A	65	A	65
T	84	L	76
I	73	A	65
K	75	N	78
A	65	G	71
Spasi	32		

Selanjutnya akan dilakukan proses enkripsi pesan pada algoritma *Affine Cipher* dengan menggunakan rumus pada persamaan $C \equiv (mP + b)\ mod\ n$, yang mana kunci *m* dan *b* sudah diperoleh dari hasil enkripsi kunci menggunakan metode Koblitz. Jadi, kunci $m = 3$ dan $b = 8$, maka proses enkripsi pesan dapat dituliskan sebagai berikut:

Karakter M

$P_1 = 77$

$C_1 \equiv (3 \cdot 77 + 8)\ mod\ 127 = 112$

Karakter A

$P_2 = 65$

$C_2 \equiv (3 \cdot 65 + 8)\ mod\ 127 = 76$

Karakter T

$P_3 = 84$

$C_3 \equiv (3 \cdot 84 + 8)\ mod\ 127 = 6$

Karakter E

$P_4 = 69$

$C_4 \equiv (3 \cdot 69 + 8)\ mod\ 127 = 88$

Karakter M

$P_5 = 77$

$C_5 \equiv (3 \cdot 77 + 8)\ mod\ 127 = 112$

Karakter A

$P_6 = 65$

$C_6 \equiv (3 \cdot 65 + 8)\ mod\ 127 = 76$

Karakter T

$P_7 = 84$

$C_7 \equiv (3 \cdot 84 + 8)\ mod\ 127 = 6$

Karakter I

$P_8 = 73$

$C_8 \equiv (3 \cdot 73 + 8)\ mod\ 127 = 100$

Karakter K

$P_9 = 75$

$C_9 \equiv (3 \cdot 75 + 8)\ mod\ 127 = 106$

Karakter A

$P_{10} = 65$

$C_{10} \equiv (3 \cdot 65 + 8)\ mod\ 127 = 76$

Karakter spasi

$P_{11} = 32$

$C_{11} \equiv (3 \cdot 32 + 8)\ mod\ 127 = 104$

Karakter U

$P_{12} = 85$

$C_{12} \equiv (3 \cdot 85 + 8)\ mod\ 127 = 9$

Karakter I

$P_{13} = 73$

$C_{13} \equiv (3 \cdot 73 + 8)\ mod\ 127 = 100$

Karakter N

$P_{14} = 78$

$C_{14} \equiv (3 \cdot 78 + 8)\ mod\ 127 = 115$

Karakter spasi

$P_{15} = 32$

$C_{15} \equiv (3 \cdot 32 + 8)\ mod\ 127 = 104$

Karakter M

$P_{16} = 77$

$C_{16} \equiv (3 \cdot 77 + 8)\ mod\ 127 = 112$

Karakter A

$P_{17} = 65$

$C_{17} \equiv (3 \cdot 65 + 8)\ mod\ 127 = 76$

Karakter L

$P_{18} = 76$

$C_{18} \equiv (3 \cdot 76 + 8)\ mod\ 127 = 109$

Karakter A

$P_{19} = 65$

$C_{19} \equiv (3 \cdot 65 + 8)\ mod\ 127 = 76$

Karakter N

$P_{20} = 78$

$C_{20} \equiv (3 \cdot 78 + 8)\ mod\ 127 = 115$

Karakter G

$P_{21} = 71$

$C_{21} \equiv (3 \cdot 71 + 8)\ mod\ 127 = 94$

Hasil yang di dapatkan dari proses enkripsi pesan menggunakan algoritma *Affine Cipher* berupa *ciphertext* dari karakter dan huruf-huruf pada kode ASCII seperti pada tabel 4.2 berikut,

Tabel 4.2 Hasil *Ciphertext Affine Cipher*

Ciphertext	Kode ASCII	*Ciphertext*	Kode ASCII
p	112	HT	9
L	76	d	100
ACK	6	s	115
X	88	h	104
p	112	p	112
L	76	L	76
ACK	6	m	109
d	100	L	76
j	106	s	115
L	76	^	94
h	104		

4.1.3 Enkripsi Kunci *Affine Cipher* Menggunakan Metode Koblitz

Proses enkripsi kunci dilakukan oleh pengirim setelah mengenkripsi pesan dengan menggunakan algoritma *Affine Cipher*. Kunci yang akan di enkripsi adalah kunci simetris yang dibentuk dari algoritma *Affine Cipher*. Kunci tersebut kemudian dienkripsi dengan menggunakan metode Koblitz.

Berikut langkah-langkah melakukan proses enkripsi kunci,

1. Menentukan persamaan dari kurva eliptik.

   Misalkan $p > 3$ adalah bilangan prima, dan $a, b \in F_p$ memenuhi $4a^3 + 27b^2 \neq 0 (mod\ p)$ maka sebuah kurva eliptik pada medan berhingga (F_p) dinotasikan dengan $G(F_p)$ menurut (Ariyus, 2006) merupakan himpunan titik-titik $P(x, y)$ dan sebuah titik khusus $\varphi(\infty, \infty)$ yang merupakan titik tak hingga, dimana $x, y \in F_p$ yang memenuhi persamaan $y^2 = x^3 + ax + b$. Titik-titik pada $G(F_p)$ membentuk suatu grup eliptik modulo prima yang mana titik-titik tersebut nantinya akan digunakan untuk proses

penyandian. Diberikan medan berhingga pada modulo 127 yang dinotasikan dengan $\mathbb{Z}_{127}$, dan dipilih $a = 2$ dan $b = 7$

$$4a^3 + 27b^2 = 4 \cdot 2^3 + 27 \cdot 7^2$$

$$\equiv 1355\ (mod 127)$$

$$\equiv 85(mod 127)$$

$$\not\equiv 0(mod 127)$$

Jadi persamaan kurva eliptik pada F_{127} yang akan digunakan yaitu:

$$y^2 = x^3 + 2x +$$

Teorema 4.1**:** Kurva eliptik $(G(F_p), +)$ dengan operasi biner $+$ adalah suatu grup.

Bukti**:**

a. Akan dibuktikan $G(F_p)$ tertutup pada operasi penjumlahan. Ambil sebarang titik $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$ dengan $P \neq \pm Q$, maka $P + Q = R$, merupakan garis yang memotong kurva eliptik tepat di suatu titik, misalkan titik $-R$. Pembuktian secara perhitungan yaitu $R = (x_3, y_3)$ dengan $x_3 = (\lambda^2) - x_1 - x_2$ dan $y_3 = (\lambda)(x_1 - x_3) - y_1$ dengan $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, nilai x_3 dan y_3 dapat dihitung dengan menggunakan prinsip penjumlahan pada $G(F_p)$ dan didapatkan $R = (x_3, y_3) \in G(F_p)$. Untuk nilai $Q = -P$, maka λ tidak akan terdefinisi karena nilai $x_1 = x_2$, jadi titik R akan berada pada titik *infinity*. Untuk titik $Q = P$, titik $R = (x_3, y_3)$ didefinisikan $x_3 = (\lambda)^2 - 2x_1$ dan $y_3 = (\lambda)(x_1 - x_3) - y_1$ dengan $\lambda = \frac{3x_1^2 + a}{2y_1}$, sehingga $R = (x_3, y_3) \in$

$G(F_p)$. Maka jelas bahwa $P + Q = R$ terpenuhi, jadi terbukti bahwa $G(F_p)$ tertutup pada operasi penjumlahan.

b. Akan dibuktikan bahwa penjumlahan titik di $G(F_p)$ memenuhi sifat assosiatif yaitu sebarang $P, Q, R \in G(F_p)$ berlaku $(P + Q) + R = P + (Q + R)$.

c. Akan dibuktikan bahwa $G(F_p)$ unsur identitas. Misalkan ambil sebarang titik $P \in G(F_p)$ maka akan nada titik $-P$ yang merupakan garis vertical yang tidak memotong kurva eliptik di titik ketiga, jika titik P dan $-P$ dijumlahkan akan menyebabkan kurva eliptik meliputi titik *invinity* dengan definisi penjumlahannya $P + (-P) = \infty$.

d. Akan dibuktikan bahwa $G(F_p)$ adalah invers. Dari pembuktian ke (3) dari grup diatas secara jelas terlihat bahwa elemen dari kurva eliptik mempunyai invers. Titik P mempunyai invers $-P$.

Dari pembuktian diatas dapat disimpulkan bahwa kurva eliptik membentuk suatu grup terhadap operasi penjumlahan titik.

Teorema 4.2: $(F_p, +, \mathrm{x})$ adalah medan (*field*) dimana p adalah bilangan prima

Bukti:

Diketahui $F_p = \{0,1,2, \dots, p-1\}$. Misalkan $a \times b = 0$, dan $a, b \in F_p$ artinya $0(mod\ p)$ maka $p \mid a$. Karena p bilangan prima dan $p \mid ab$ maka $p \mid a$ atau $p \mid b$. Jadi $a \equiv 0(mod\ p)$ atau $b \equiv 0(mod\ p)$ artinya $a = 0$ atau $b = 0$. Jadi terbukti bahwa $(F_p, +, \mathrm{x})$ tanpa pembagi nol yang

artinya $(F_p, +, \mathrm{x})$ adalah domain integral sehingga $(F_p, +, \mathrm{x})$ adalah medan.

2. Pilih sembarang nilai *k* (pengirim dan penerima menyepakati nilai ini).
3. Menentukan sebuah karakter bernilai m.
4. Hitung $x = mk + 1$ dan substitusikan ke dalam y untuk mendapatkan titik-titik dari kurva eliptik.

Langkah awal yaitu menentukan enkripsi kunci dari algoritma *Affine Cipher* yang berupa *m* dan *b* dengan menggunakan metode Koblitz.

a. Menentukan enkripsi kunci *m*, pengirim memilih $m_m = 3, k = 8$. Hitung $x = mk + 1$ sebagai berikut:

$$x = mk + 1$$
$$= 3 \cdot 8 + 1 = 25$$

Kemudian cari nilai y dengan cara subtitusikan hasil dari $x = mk + 1$ untuk mendapatkan titik-titik kurva eliptik.

$$y^2 \equiv x^3 + 2x + 7 \ (mod\ 127)$$
$$\equiv 25^3 + 2 \cdot 25 + 7 \ (mod\ 127)$$
$$\equiv 61\ mod\ 127 \ \rightarrow y_1 = 51, y_2 = 76 \rightarrow P_1(25{,}51) \text{dan } P_2(25{,}76)$$

Maka nilai y yang memenuhi adalah 51 dan 76. Jadi, titik pada kurva eliptik adalah $(25, 51)$ dan $(25, 76)$. Langkah selanjutnya adalah ambil salah satu titik dari kurva eliptik untuk dijadikan sebuah kunci dari proses enkripsi pada algoritma *Affine Cipher.* Dalam penelitian ini penulis mengambil titik $(25{,}51)$. Jadi, hasil dari enkripsi kunci pada algoritma *Affine Cipher* m adalah 25.

Gambar 4.1 Kurva Eliptik pada Proses Enkripsi Kunci *m*

b. Menentukan enkripsi kunci *b*, pengirim memilih $m_b = 8, k = 8$.

$$x = mk + 1$$

$$= 8 \cdot 8 + 1 = 65$$

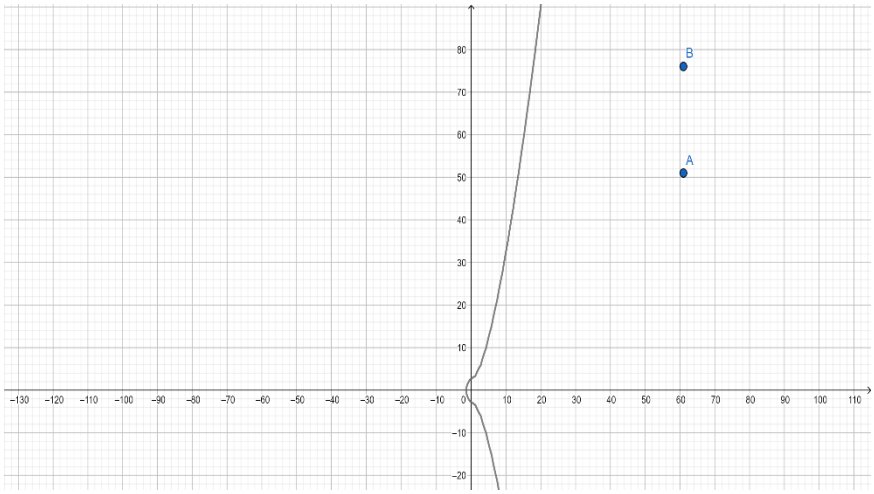
Kemudian cari nilai y dengan cara subtitusikan hasil dari $x = mk + 1$ untuk mendapatkan titik-titik kurva eliptik.

$$y^2 \equiv x^3 + 2x + 7 \ (mod\ 125)$$

$$\equiv 65^3 + 2 \cdot 65 + 7 \ (mod\ 125)$$

$$\equiv 61\ mod\ 125 \ \rightarrow y_1 = 51, y_2 = 76 \rightarrow P_1(61{,}51) \text{dan } P_2(61{,}76)$$

Maka nilai y yang memenuhi adalah 51 dan 76. Jadi, titik pada kurva eliptik adalah $(61, 51)$ dan $(61, 76)$. Langkah selanjutnya adalah ambil salah satu titik dari kurva eliptik untuk dijadikan sebuah kunci dari proses enkripsi pada algoritma *Affine Cipher*. Dalam penelitian ini penulis mengambil titik $(61{,}76)$, maka hasil dari enkripsi kunci pada algoritma *Affine Cipher* adalah $b = 61$.



Gambar 4.2 Kurva Eliptik pada Proses Enkripsi kunci *b*

4.2 Dekripsi Pesan Menggunakan algoritma *Affine Cipher*

Dekripsi pesan merupakan proses yang dilakukan oleh penerima pesan dengan mendekripsikan kunci menggunakan kurva eliptik dengan metode Koblitz. Sehingga diperoleh kunci yang akan digunakan untuk melakukan proses dekripsi *ciphertext* pesan.

4.2.1 Dekripsi Kunci *Affine Cipher* dengan Metode Koblitz

Proses dekripsi kunci algoritma *Affine Cipher* metode Koblitz dilakukan oleh penerima setelah menerima pesan berkode (*ciphertext)*. Kunci yang akan di dekripsi yaitu kunci yang telah di enkripsi dengan metode Koblitz. Proses dekripsi kunci metode Koblitz dengan menggunakan rumus $m = (x - 1)/k$. Nilai m adalah bilangan bulat terbesar yang lebih kecil dari $(x - 1)/k$. Kemudian dengan mensubtitusikan nilai x dan k, maka proses dekripsi kunci sebagai berikut,

a. Dekripsi kunci *m*

$$m = \frac{x-1}{k}$$

$$= \frac{25-1}{8} = 3$$

b. Dekripsi kunci *b*

$$m = \frac{x-1}{k}$$

$$= \frac{61-1}{8} = 7.5 = 8$$

Jadi hasil dari proses dekripsi kunci dari $m_m = 25$ dan $m_b = 61$ yaitu mendapatkan hasil $m = 3$ dan $m = 8$. Dimana 3 dan 8 merupakan kunci simetris dari algoritma *Affine Cipher* yang berupa *m* dan *b.*

4.2.2 Proses Dekripsi Pesan Menggunakan *Affine Cipher*

Proses dekripsi yang diperlukan adalah pesan berkode (*ciphertext*) dari pesan yang telah di enkripsi. Kemudian langkah yang digunakan untuk mendekripsi pesan dengan menggunakan rumus algoritma *Affine Cipher* $P \equiv m^{-1}(C-b)(mod\ n)$. Mencari kunci $m^{-1}\ mod\ 127$ yang akan digunakan pada proses dekripsi sebagai berikut,

$$m^{-1} = 3x \equiv 1\ mod\ 127$$

$$= 3(85) \equiv 1\ mod\ 127$$

Kemudian proses dekripsi dilakukan oleh penerima pesan menggunakan rumus dekripsi algoritma *Affine Cipher* $P \equiv m^{-1}(C-b)(mod\ n)$ sebagai berikut,

Karakter p

$C_1 = 112$

$P_1 \equiv 85(112-8)\ mod 127 = 77$

Karakter L

$C_2 = 76$

$P_2 \equiv 85(76 - 8)\ mod 127 = 65$

Karakter ACK

$C_3 = 6$

$P_3 \equiv 85(6 - 8)\ mod 127 = 84$

Karakter X

$C_4 = 88$

$P_4 \equiv 85(88 - 8)\ mod 127 = 69$

Karakter p

$C_5 = 112$

$P_5 \equiv 85(112 - 8)\ mod 127 = 77$

Karakter L

$C_6 = 76$

$P_6 \equiv 85(76 - 8)\ mod 127 = 65$

Karakter ACK

$C_7 = 6$

$P_7 \equiv 85(6 - 8)\ mod 127 = 84$

Karakter d

$C_8 = 100$

$P_8 \equiv 85(100 - 8)\ mod 127 = 73$

Karakter j

$C_9 = 106$

$P_9 \equiv 85(106 - 8)\ mod 127 = 75$

Karakter L

$C_{10} = 76$

$P_{10} \equiv 85(76 - 8)\ mod 127 = 65$

Karakter h

$C_{11} = 104$

$P_{11} \equiv 85(104 - 8)\ mod 127 = 32$

Karakter HT

$C_{12} = 9$

$P_{12} \equiv 85(9 - 8)\ mod 127 = 85$

Karakter d

$C_{13} = 100$

$P_{13} \equiv 85(100 - 8)\ mod 127 = 73$

Karakter s

$C_{14} = 115$

$P_{14} \equiv 85(115 - 8)\ mod 127 = 78$

Karakter h

$C_{15} = 104$

$P_{15} \equiv 85(104 - 8)\ mod 127 = 32$

Karakter p

$C_{16} = 112$

$P_{16} \equiv 85(112 - 8)\ mod 127 = 77$

Karakter L

$C_{17} = 76$

$P_{17} \equiv 85(76 - 8)\ mod 127 = 65$

Karakter m

$C_{18} = 109$

$P_{18} \equiv 85(109 - 8)\ mod 127 = 76$

Karakter L

$C_{19} = 76$

$P_{19} \equiv 85(76 - 8)\ mod 127 = 65$

Karakter s

$C_{20} = 115$

$P_{20} \equiv 85(115 - 8)\ mod 127 = 78$

Karakter ^

$C_{21} = 94$

$P_{21} \equiv 85(94 - 8)\ mod 127 = 71$

Tabel 4.3 Hasil Dekripsi Pesan

Plaintext	Kode ASCII	*Plaintext*	Kode ASCII
M	77	U	85
A	65	I	73
T	84	N	78
E	69	Spasi	32
M	77	M	77
A	65	A	65
T	84	L	76
I	73	A	65
K	75	N	78
A	65	G	71
Spasi	32		

Berdasarkan hasil dari proses dekripsi pesan diperoleh pesan asli (*plaintext*) yaitu **MATEMATIKA UIN MALANG**. Proses dekripsi menggunakan

algoritma *Affine Cipher* dilakukan dengan mengalikan hasil pengurangan *ciphertext* dengan invers dari kunci simetris *m*.

Dengan demikian pesan yang dikirimkan sesuai dengan pesan yang telah diterima. Baik dengan mengenkripsi dan dekripsi kunci simetris dari algoritma *Affine Cipher* dengan metode Koblitz yang digunakan sebagai kunci publik, agar pesan yang disampaikan sulit untuk dipecahkan oleh pihak-pihak yang tidak berhak menerima pesan tersebut. Sehingga mengamankan pesan menggunakan proses enkripsi dan dekripsi menggunakan algoritma *Affine Cipher* dengan metode Koblitz berhasil dilakukan. Kemudian akan dibuktikan bahwa *ciphertext* pada algoritma *Affine Cipher* akan memenuhi fungsi enkripsinya sebagai berikut,

$C \equiv mP + b \ (mod\ n)$	Rumus Enkripsi
$n \mid C - (mP + b)$	Definisi kongruensi
$C - (mP + b) = n$	Definisi keterbagian
$-C + (mP + b) = n(-k)$	Kedua ruas di kali -1
$mP + b - C = n(-k)$	Sifat komutatif
$mP - (C - b) = n(-k)$	Sifat assosiatif
$n \mid mP - (C - b)$	Definisi keterbagian
$mP \equiv (C - b)\ mod\ n$	Definisi kongruensi
$m^{-1} \cdot mP \equiv m^{-1}(C - b)\ mod\ n$	Kedua ruas di kali m^{-1}
I$P \equiv m^{-1}(C - b)\ mod\ n$	Sifat identitas
$P \equiv m^{-1}(C - b)\ mod\ n$	Rumus dekripsi

Jadi terbukti bahwa *ciphertext* pada algoritma *Affine Cipher* memenuhi fungsi enkrisp dekripsi

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan diatas, maka didapatkan sebuah kesimpulan sebagai berikut:

1. Proses enkripsi pesan pada algoritma *Affine Cipher* menggunakan metode Koblitz menghasilkan sebuah pesan berkode (*ciphertext*). Proses enkripsi (*plaintext*) dilakukan setelah mengkonversi *plaintext* menggunakan tabel ASCII yang berbatas hingga 127. Pada proses enkripsi menggunakan kunci $m = 3$ dan $b = 8$, maka dihasilkan sebuah *ciphertext.* Kemudian, dilakukan proses enkripsi kunci simetris dengan metode Koblitz, dengan nilai karakter $m_m = 3, m_b = 8,$ dan $k = 8$. Persamaan yang digunakan untuk enkripsi kunci yaitu $y^2 = x^3 + 2x + 7$ $(mod\ 127)$. Kunci yang telah dienkripsi akan digunakan sebagai kunci publik. Dengan demikian pesan yang akan disampaikan lebih terjamin keamanannya.
2. Proses dekripsi dengan algoritma *Affine Cipher* dapat mengubah *ciphertext* menjadi *plaintext*. Proses dekripsi merupakan proses pengembalian *ciphertext* menjadi *plaintext* semula. Karena *ciphertext* yang diperoleh adalah *ciphertext* pesan, maka terlebih dahulu menentukan *plaintext* dari kunci dengan merubah *ciphertext* kunci menggunakan metode Koblitz. Kunci yang digunakan untuk dekripsi kunci yaitu $m_m = 25, m_b = 61$. Menghasilkan kunci simetris yang digunakan sebagai kunci untuk melakukan proses dekripsi pesan. Algoritma *Affine Cipher* digunakan untuk memperoleh *plaintext* asli sesuai dengan pesan yang dikirimkan oleh pengirim. Sehingga

proses dekripsi ini dapat dilakukan dengan baik.

5.2 Saran

Setelah melakukan penelitian mengenai proses enkripsi dan dekripsi pesan teks menggunakan algoritma *Affine Cipher* kurva eliptik dengan metode Koblitz peneliti memberikan saran kepada pembaca bahwa pada penelitian ini proses enkripsi dan dekripsi dapat dilakukan dengan baik. Namun untuk peneliti yang lain diharapkan untuk meningkatkan kerumitan algoritma dalam melakukan pengamanan teks. Dengan memodifikasi algoritma *Affine Cipher* dengan metode yang lain.

DAFTAR PUSTAKA

(LPMQ), L. P. M. A.-Q. (2022). *Qur'an Kemenag*.

Ariyus, D. (2006). *Kriptografi Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

Ariyus, D. (2008). *Pengantar Ilmu Komputer Teori Analisis dan Implementasi.* Yogyakarta: C.V Andi Offset.

Asy-Syuyuthi, J. (2009). *Tafsir Jalalain*.

Gilbert, L. . & G. J. (2015). *Elements of Modern Algebra*.

Irawan, W. H., Hijriyah, N. ., & Habibi, A. R. (2014). *Pengantar Teori Bilangan.* UIN Malang Press.

Kromodioeljo, S. (2010). *Teori dan Apilkasi Kriptografi.* Jakarta: SPK IT Consuling.

Kurnia, D. A. (2013). *Optimasi Konversi String Biner Hasil Least Significant Bit Steganography*.

Meyer, C. ., & Matyas, S. M. . (1982). *Criptography, A New Dimension in Computer Data Security* (John Wiley & Sons (ed.)).

Munir, R. (2019). *Kriptografi* (kedua). Informatika.

Nasution, A. B. (2020). Modifikasi Algoritma Affine Cipher untuk Mengamankan Data. *Jurnal Teknologi Informasi*, *4*(2).

Padma, B., Chandravathi, D., & Roja, P. P. (2010). Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method. *(IJCSE) International Journal on Computer Science and Engineering*, *02*(05), 1904–1907.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*.

Setyobudi, F. (2013). *Penggunaan Kriptografi Kurva Eliptik Pada Proses Penyandian Elgamal* . Universitas Islam Negeri Maulana Malik Ibrahim Malang .

Siyoto, S., & Sodik, A. (2015). *Dasar Metodologi Penelitian*. Literasi Media Publishing.

Stallings, W. (2017). *Criptography and Net Securitywork Principles and Practice* (7th ed.). Pearson Education Limited.

LAMPIRAN

Lampiran 1 Program Python Untuk Menentukan Titik Kurva Eliptik

```
INF_POINT = None
class EllipticCurve:
	def __init__(self, a, b, p):
		self.a = a
		self.b = b
		self.p = p
		self.points = []
		self.definePoints()

	def definePoints(self):
		self.points.append(INF_POINT)
		for x in range(self.p):
			for y in range(self.p):
				if self.equalModp(y * y, x * x * x + self.a * x + 
self.b):
					self.points.append((x,y))

	def addition(self, P1, P2):
		if P1 == INF_POINT:
			return P2
		if P2 == INF_POINT:
			return P1

		x1 = P1[0]
		y1 = P1[1]
		x2 = P2[0]
		y2 = P2[1]

		if self.equalModp(x1, x2) and self.equalModp(y1, -y2):
			return INF_POINT

		if self.equalModp(x1, x2) and self.equalModp(y1, y2):
			u = self.reduceModp((3 * x1 * x1 + self.a) * 
self.inverseModp(2 * y1))
		else:
			u = self.reduceModp((y1 - y2) * self.inverseModp(x1 - x2))

		v = self.reduceModp(y1 - u * x1)
		x3 = self.reduceModp(u * u - x1 - x2)
		y3 = self.reduceModp(-u * x3 - v)

		return (x3, y3)
```

```
        def testAssociativity(self):
                n = len(self.points)
                for i in range (n):
                        for j in range(n):
                                for k in range(n):
                                        P = self.addition(self.points[i],
self.addition(self.points[j], self.points[k]))
                                        Q = self.addition(self.addition(self.points[i],
self.points[j]), self.points[k])
                                        if P != Q:
                                                return False
                return True




        def numberPoints(self):
                return len(self.points)

        def discriminant(self):
                D = -16 *(4 * self.a * self.a * self.a + 27 * self.b * self.b)
                return self.reduceModp(D)

        def printPoints(self):
                print(self.points)

        # helper functions

        def reduceModp(self, x):
                return x % self.p

        def equalModp(self, x, y):
                return self.reduceModp(x - y) == 0

        def inverseModp(self, x):
                for y in range(self.p):
                        if self.equalModp(x * y, 1):
                                return y
                return None

ec = EllipticCurve(1,3,97)
ec.printPoints()
print(ec.numberPoints())
```

Lampiran 2 Tabel Kode ASCII (Kode Karakter 0-126)

Desimal	Biner	Hexadesimal	Karakter
0	00000000	00	NUL
1	00000001	01	SOH
2	00000010	02	STX
3	00000011	03	ETX
4	00000100	04	EOT
5	00000101	05	ENQ
6	00000110	06	ACK
7	00000111	07	BEL
8	00001000	08	BES
9	00001001	09	HT
10	00001010	0A	LF
11	00001011	0B	VT
12	00001100	0C	FF
13	00001101	0D	CR
14	00001110	0E	SO
15	00001111	0F	SI
16	00010000	10	DLE
17	00010001	11	DC1
18	00010010	12	DC2
19	00010011	13	DC3
20	00010100	14	DC4
21	00010101	15	NAK
22	00010110	16	SYN
23	00010111	17	ETB
24	00011000	18	CAN
25	00011001	19	EM
26	00011010	1A	SUB
27	00011011	1B	ESC
28	00011100	1C	FS
29	00011101	1D	GS

30	00011110	1E	RS
31	00011111	1F	US
32	00100000	20	*(Space)*
33	00100001	21	!
34	00100010	22	"
35	00100011	23	#
36	00100100	24	$
37	00100101	25	%
38	00100110	26	&
39	00100111	27	'
40	00101000	28	(
41	00101001	29	)
42	00101010	2A	*
43	00101011	2B	+
44	00101100	2C	,
45	00101101	2D	-
46	00101110	2E	.
47	00101111	2F	/
48	00110000	30	0
49	00110001	31	1
50	00110010	32	2
51	00110011	33	3
52	00110100	34	4
53	00110101	35	5
54	00110110	36	6
55	00110111	37	7
56	00111000	38	8
57	00111001	39	9
58	00111010	3A	:
59	00111011	3B	;
60	00111100	3C	<

61	00111101	3D	=
62	00111110	3E	>
63	00111111	3F	?
64	01000000	40	@
65	01000001	41	A
66	01000010	42	B
67	01000011	43	C
68	01000100	44	D
69	01000101	45	E
70	01000110	46	F
71	01000111	47	G
72	01001000	48	H
73	01001001	49	I
74	01001010	4A	J
75	01001011	4B	K
76	01001100	4C	L
77	01001101	4D	M
78	01001110	4E	N
79	01001111	4F	O
80	01010000	50	P
81	01010001	51	Q
82	01010010	52	R
83	01010011	53	S
84	01010100	54	T
85	01010101	55	U
86	01010110	56	V
87	01010111	57	W
88	01011000	58	X
89	01011001	59	Y
90	01011010	5A	Z
91	01011011	5B	[

92	01011100	5C	\
93	01011101	5D	]
94	01011110	5E	^
95	01011111	5F	_
96	01100000	60	`
97	01100001	61	a
98	01100010	62	b
99	01100011	63	c
100	01100100	64	d
101	01100101	65	e
102	01100110	66	f
103	01100111	67	g
104	01101000	68	h
105	01101001	69	i
106	01101010	6A	j
107	01101011	6B	k
108	01101100	6C	l
109	01101101	6D	m
110	01101110	6E	n
111	01101111	6F	o
112	01110000	70	p
113	01110001	71	q
114	01110010	72	r
115	01110011	73	s
116	01110100	74	t
117	01110101	75	u
118	01110110	76	v
119	01110111	77	w
120	01111000	78	x
121	01111001	79	y
122	01111010	7A	z

123	01111011	7B	{
124	01111100	7C	|
125	01111101	7D	}
126	01111110	7E	~

RIWAYAT HIDUP

Putri Lisaro Hadi, dilahirkan di Kabupaten Mojokerto pada tanggal 04 November 2000. Memiliki nama panggilan Putri. Bertempat tinggal Jalan Mertojoyo Selatan Gang II NO. 4, Kecamatan Lowokwaru, Kota Malang. Merupakan putri kedua dari pasangan Bapak Solikul Hadi dan Ibu Munawaroh serta memiliki kakak laki-laki yang bernama Rizqi Maulana Hadi. Jenjang pendidikannya dimulai sejak bersekolah di TK Dharma Wanita yang lulus pada tahun 2006. Setelah itu melanjutkan Pendidikan di SDN Banjartanggul yang lulus pada tahun 2012. Pendidikan selanjutnya ditempuh di SMPBP Amanatul Ummah Pacet yang lulus pada tahun 2015. Kemudian melanjutkan Pendidikan di MBI Amanatul Ummah Pacet yang lulus pada tahun 2018. Pada jenjang perguruan tinggi ia melanjutkan pendidikannya dengan berkuliah di UIN Maulana Malik Ibrahim Malang dengan memilih menekuni bidang Matematika murni di Fakultas Sains dan Teknologi. Selama menempuh Pendidikan di Kampus Ulul Albab UIN Maulana Malik Ibrahim Malang, selain menyelesaikan tugasnya sebagai mahasiswa, Ia juga memiliki aktivitas yakni menjadi guru les privat. Menurutnya dengan kegiatan tersebut, dapat semakin mengasah ilmu yang didapatkan di bangku perkuliahan sembari menambah pengalaman. Baginya, Matematika adalah salah satu ilmu yang istimewa karena hingga saat ini hasil penelitiannya sangat berguna bagi kemajuan peradaban dan mampu diaplikasikan langsung dalam beberapa kasus pada kehidupan sehari-hari.

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 : Putri Lisaro Hadi
NIM : 18610093
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Enkripsi dan Dekripsi Pesan Menggunakan Kurva Eliptik pada *Affine Cipher* dengan Metode Koblitz
Pembimbing I : Prof. Dr. H. Turmudi, M.Si., Ph.D
Pembimbing II : Mohammad Nafie Jauhari, M.Si

No	Tanggal	Hal	Tanda Tangan
1.	10 Februari 2022	Konsultasi Bab 1	1.
2.	11 Februari 2022	Konsultasi Kajian Agama	2.
3.	18 Februari 2022	Konsultasi Bab 2	3.
4.	24 Februari 2022	Konsultasi Kajian Agama	4.
5.	28 Februari 2022	Konsultasi Bab 2	5.
6.	5 Maret 2022	Konsultasi Kajian Agama	6.
7.	10 Maret 2022	Konsultasi Bab 2	7.
8.	18 Maret 2022	Konsultasi Bab 3	8.
9.	25 Maret 2022	ACC Seminar Proposal	9.
10.	25 Maret 2022	ACC Seminar Proposal	10.
11.	18 April 2022	Konsultasi Bab 4	11.
12.	28 April 2022	Konsultasi Bab 4	12.
13.	11 Mei 2022	Konsultasi Bab 5	13.
14.	17 Mei 2022	Konsultasi Kajian Agama	14.
15.	7 Juni 2022	ACC Seminar Hasil	15.
16.	8 Juni 2022	ACC Seminar Hasil	16.
17.	17 Juni 2022	Konsultasi Bab 4	17.
18.	18 Juni 2022	ACC Sidang Skripsi	18.
19.	20 Juni 2022	ACC Sidang Skripsi	19.

Malang, 23 Juni 2022
Mengetahui,
Ketua Program Studi Matematika

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