BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan dunia industri telah berlangsung, mulai dari Revolusi Industri 1.0 paling tidak sampainya Revolusi Industri 3.0 membawa banyak sekali kemajuan yang penting dalam bidang ini. Teknologi komunikasi serta teknologi informasi telah menyebabkan perubahan yang besar dalam bidang ekonomi dan bidang sosial . Dengan berkembangnya Teknologi komunikasi serta teknologi informasi, cara berpikir telah berubah dari manual ke digital mengenai batas wilayah, bentuk objek, waktu, nilai, dan batasan perilaku sosial [1]. Semakin berkembangnya industri juga mengakibatkan semakin banyaknya serangan digital. Tidak kurang dari 92 juta pengguna serta setidaknya lebih dari 7.000.000 data pedagang dari Tokopedia hampir dijual di *dark web*, dengan harga US$5.000 atau sekitar Rp 75 juta. [2]. Dengan tingginya kasus kebocoran data tersebut menunjukan bahwa kurangnya keamanan terhadap data yang ada.

Selain itu menurut BSSN (Badan Siber dan Sandi Negara), Letnan Jenderal TNI (Purn) Hinsa S. telah mengungkapkan, setidaknya dari data yang telah terhimpun di BSSN Pusopskamsinas atau yang dikenal dengan Pusat Operasi Keamanan Siber Nasional, masyarakat mencatat antara awal tahun sampai hamper akhir tahun yaitu pada bulan november 2020, ada lebih dari empat ratus dua puluh tiga juta serangan siber. Tepatnya 423.244.053 serangan. Sedangkan pada tahun 2019 terdapat 182 juta lebih serangan siber. S kata Hinsa dala sambutannya di simposium yang dimana digelar pada hotel Royal Ambarukmo, Senin (14/12/2020) setidaknya sudah ada kurang lebih 3 kali lipat serangan dibandingkan tahun 2019. Dari data tersebut membuktikan bahwasanya data yang diberikan melalui digital sering terjadi kebocoran data. Hal ini tentunya menjadi sinyal bahwa aspek keamanan harus terus ditingkatkan dari segala bidang, termasuk bidang *database* atau yang biasa disebut dengan basis data. Basis data atau database adalah sumber daya yang digunakan oleh siapa saja yang ingin memindahkan dan menempatkan

informasi dengan menggunakan komputer , dari metode kertas tradisional ke metode yang lebih digitalisasi [3].

Kurangnya keamanan terhadap data menyebabkan kerugian yang signifikan bagi para pengguna internet dan perusahaan. Sejauh ini banyak metode keamanan yang dapat digunakan untuk mengamankan data. Method yang umum digunakan yaitu kriptografi.

Cryptography merupakan sebuah teknik yang menyandikan sebuah informasi ke suatu karakter tertentu dan menyusunnya dengan acak yang mengakibatkan tidak mudah dipahami. [4]. Kriptografi juga memiliki sistem enkripsi dan dekripsi. Enkripsi adalah proses mengenkripsi data atau informasi dalam aplikasi menggunakan algoritma enkripsi sedangkan dekripsi adalah proses memulihkan atau mengambil data atau informasi yang dienkripsi. [5].

Penelitian ini akan berfokus terhadap bagaimana merancang sistem keamanan berbasis kriptografi *Merkle-hellman Knapsack* dan *Advanced Encryption Standard* dengan menggunakan objek penelitian *database* yang bersifat dump pada website rancangan peneliti sendiri serta menguji seberapa efektif kinerja dari sistem dalam mengamankan data. Tahapan dalam penelitian ini sendiri adalah studi kepustakaan, perancangan sistem dan pengujian dari sistem yang dibuat. Hasil pengujian kemudian disajikan dalam bentuk grafik atau tabel.

1.2 Rumusan Masalah

Menurut penetian yang akan dilakukan ini peneliti telah menentukan rumusan masalah yaitu:

1. Bagaimana kerja metode kriptografi *Merkle-hellman Knapsack* dan *Advanced Encryption Standard* dalam mengamankan *Database*?
2. Bagaimana Proses enkripsi *Merkle-hellman Knapsack* dan *Advanced Encryption Standard* terhadap data?
3. Bagaimana Proses dekripsi *Merkle-hellman Knapsack* dan *Advanced Encryption Standard* terhadap data?
4. Bagaimana Hasil analisis setelah system melakukan pengujian?

1.3 Tujuan Penelitian

Rumusan masalah yang terjadi membuat peneliti memiliki tujuan dari penelitian ini, yang dimanan terdapat 4 tujuan penelitian yaitu:

1. Memahami cara kerja metode kriptografi *Merkle-hellman Knapsack* dan Advanced *Encryption* Standard (AES) dalam mengamankan Data.
2. Mengetahui hasil enkripsi dari data yang sudah dibuat.
3. Mengetahui hasil dekripsi dari data yang dibuat.
4. Menyimpulkan hasil analisis setelah dilakukan pengujian sistem .

1.4 Batasan Masalah

Tahapan ini peneliti memiliki batasan-batasan dalam masalah penelitian yang telah dituliskan diatas, ada 3 batasan masalah dalam penelitian ini yaitu:

1. Penelitian yang dilakukan ini hanya berfokus pada aspek keamanan Data.
2. Penelitian ini hanya berfokus pada methode kriptografi *Merkle-hellman Knapsack dan Advanced Encryption Standard* (AES) dalam keamanan Data.
3. Penelitian ini hanya berfokus pada enkripsi Text.
4. Penekanan penelitian pada perancangan system sebagai solusi terhadap masalah yang diangkat.

1.5 Manfaat Penelitian

Manfaat dari penelitian yang dilakukan peneliti yaitu memberikan rasa keamanan informasi kepada pemilik informasi dan membawa perspektif baru dalam perkembangan teknologi, khususnya di bidang keamanan. Penelitian ini setidakya bisa bermanfaat sebagai referensi atau rujukan untuk penelitian yang akan datang. Selain itu, diharapkan selanjutnya dapat mengimplementasikan sistem dengan benar, yaitu sistem dengan keamanan kriptografi *Merkle-Hellman Knapsack dan Advanced Encryption Standard*.