BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Identitas menurut kamus besar bahasa Indonesia adalah keadaan, sifat, atau ciri-ciri khusus seseorang atau benda. Melalui identitas, manusia dapat dibedakan antara satu dengan yang lain. Penduduk Indonesia dalam hal ini, juga mempunyai dokumen identitas. Dalam pembuatan dokumen identitas ini diperlukan suatu rangkaian kegiatan penataan dan penerbitan melalui pendaftaran penduduk, pencatatan sipil, pengelolaan informasi penduduk serta pendayagunaan hasilnya untuk pelayanan publik dan pembangunan sektor lain. Pendaftaran penduduk merupakan pencatatan biodata penduduk, pelaporan peristiwa kependudukan, dan pendataan penduduk serta penerbitan dokumen yang berupa identitas, kartu atau surat keterangan penduduk. Adapun salah satu dokumen identitas adalah Kartu Tanda Penduduk elektronik, e KTP atau KTP-el merupakan Kartu Tanda Penduduk (KTP) yang dibuat secara elektronik, dalam artian baik dari segi fisik maupun penggunaannya berfungsi secara komputerisasi. Di Indonesia e-KTP merupakan sebuah nomor identitas unik yang terintegrasi dengan gabungan data dari berbagai macam instansi pemerintahan dan swasta. (Gondohanindijo dan Sediyono 2013). Pada e KTP terdapat NIK yang bersifat rahasia yang perlu disembunyikan dan dilin- dungi. NIK pada e KTP merupakan hal yang perlu tetap terjaga kerahasiaannya dari penyadap *(attacker)*. Penyadap pesan diasumsikan mempunyai akses yang lengkap dalam saluran komunikasi antara pengirim pesan dan penerima pesan.

Menurut liputan6.com dalam beritanya bahwa. Menteri Komunikasi dan Informatika (Menkominfo) Rudiantara, mengimbau kepada masyarakat untuk tidak sembarangan memberikan informasi KTP dan KK kepada pihak lain. Sama halnya dengan guru pada SMPN 1 Tanjung Pura memiliki beberapa informasi yang dirahasiakan. NIK sangat diperlukan dan penting untuk syarat login di laman Guru atau Tenaga Kependidikan (GTK) di website *http://info.gtk.kemdikbud.go.id/*. Dimana laman tersebut berisi informasi penting bagi guru salah satunya adalah informasi mengenai

sertifikasi guru.

Kriptografi dapat diartikan sebagai teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi. Kriptografi terbagi menjadi dua proses utama yaitu enkripsi dan dekripsi. Enkripsi merupakan proses merahasiakan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus, sedangkan dekripsi adalah proses pengembalian data hasil enkripsi. (Islamiyah 2017). Matematika adalah ilmu yang mendasari algoritma kriptografi. Pada kriptografi modern terdapat berbagai macam algoritma, secara umum kriptografi modern dikelompokkan menjadi algoritma simetris yang menggunakan kunci yang sama untuk melakukan enkripsi dan deskripsi dan algoritma asimetris yang menggunakan kunci yang berbeda untuk melakukan enkripsi dan deskripsi.

Adapun kriptografi adalah cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Kriptografi adalah ilmu untuk menjaga kerahasiaan berita (*Bruce Schneier Applied Cryptography*). Selain itu kriptografi juga diartikan sebagai ilmu yang mendalami teknik-teknik matematika yang kaitannya dengan aspek keamanan informasi misalnya kerahasiaan data, kesahan data, kredibilitas data, serta keaslian data. Tetapi tidak segala aspek keamanan dan keselamatan informasi diatasi oleh kriptografi.

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Salah satu hal penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data, ataupun informasi adalah enkripsi. (Alvianto dan Darmanji 2015) Tidak dipungkiri lagi sekarang kebutuhan akan teknologi sangat penting dirasakan, bahkan kita tidak menyadari akan keamanan dalam menggunakan teknolgi jaman sekarang nah, untuk menyelamatkan data-data yang kita miliki berikut adalah implementasi kritografi dikehidupan seharihari : Transaksi lewat Anjungan Tunai Mandiri, Pay TV, Transaksi E-commerce dan sebagainya (Hidayatullah dan Entik Insanuddin 2016). Kebocoran data biometrik juga dapat berbahaya bagi kedaulatan bangsa. Misal data biometrik e-KTP. Jika data biometrik e-KTP bocor, data ini dapat digunakan pihak lain atau pihak tidak bertanggung jawab untuk mengindenti- fikasi data pribadi berdasarkan data biometrik yang diperoleh. Lembaga Studi dan Advokasi Masyarakat (ELSAM), Jumat (13/12)

mengingatkan tentang peluang potensi eksploitasi data kependudukan pribadi warga. Respons ini terlontar usai kesepakatan kerja sama antara Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) Kemendagri dan PT Jelas Karya Wasantara. Dalam siaran pers tersebut disebutkan, kerja sama meliputi akses pemanfaatan data kependudukan (Pasal 58 UU Adminduk), juga akses terhadap foto wajah dari data biometrik. Kesalahan dalam penggunaannya bakal memicu terjadinya diskriminasi, kesalahan identifikasi, penipuan, pengecualian, atau ekslusivisme terhadap kelompok rentan, hingga tindakan pengawasan massal.

Algoritma *One Time Pad* (OTP) ditemukan pada tahun 1917 oleh Major Joseph Mauborgne. Algoritma ini termasuk ke dalam kelompok algoritma kriptografi simetri. One Time Pad (pad = kertas blok not) berisi barisan karakter- kararkter kunci yang dibangkitkan secara acak. Aslinya, 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 (Harahap dan Khairina 2017). Privasi bagi seseorang sehingga tidak semua orang dapat mengetahuinya dan tidak diberikan ke sembarang orang karena dapat mengungkapkan identitas personal pemiliknya karena apabila data tersebut tersebar maka dapat disalah gunakan untuk tujuan yang tidak benar salah satu contohnya adalah pemalsuan informasi.

Algoritma *One Time Pad* (OTP) terpilih untuk melakukan proses enkripsi dan dekripsi karena algoritma OTP kuat dan aman apabila memenuhi kriteria pengoperasian, salah satunya yaitu mengacak kunci yang akan digunakan secara random dan tidak menggunakan kunci tersebut untuk operasi lain. Hal ini tentu menyulitkan ketika panjang kunci yang dimaksud harus sama panjang dengan data induk yang akan dienkripsi, sehingga perlu adanya sauatu algoritma lain yang dapat membantu mengacak kunci (Rosal 2017).

Algoritma RSA yang dibuat oleh Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1976 merupakan algoritma asimetris. Keamanan RSA terletak pada sulitnya untuk memfaktorkan bilangan prima yang relatif lebih besar. Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi dan salah satu penemuan besar dalam kriptografi kunci publik. Dari sekian banyak algoritma

kriptografi dengan kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Keamanan algoritma rsa terletak pada sulitnya untuk memfaktorkan bilangan prima yang relatif lebih besar. Pemfaktoran dilakukan untuk memperoleh kunci privat (Gunawan 2018).

Pada penelitian sebelumnya yang dilakukan oleh Jutono Gondohanindijo dan Eko Sediyono yang berjudul ”*Analisis Efesiensi Algoritma RSA pada Database Kependudukan (e-KTP)*” data yang diamankan berupa Nomor Induk Kependudukan menggunakan algoritma RSA yang diimplementasikan pada komputer server untuk proses enkripsinya dan pada penelitian yang dilakukan oleh Muhammad Khoiruddin Harahap dan Nurul Khairina yang berjudul ”*Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks*” data yang diamankan berupa pesan teks menggunakan algoritma One Time Pad dengan mengganti plaintext dan kunci menjadi angka sesuai dengan tabel yang telah diberikan dan menggunakan algoritma Cipher Transposisi dengan cara membagi karakter ciphertext secara vertikal (dari atas ke bawah) sebanyak kunci yang telah ditentukan sebelumnya.

Algoritma RSA merupakan algoritma kriptografi kunci publik yang terkenal aman karena sulitnya memecahkan fungsi matematis yang dipakai sebagai dasar pembuatan algoritmanya. Algoritma OTP merupakan suatu metode yang sangat kuat karena panjang kunci sama dengan panjang pesan yang dikirim dan kunci yang digunakan adalah session key, dimana kunci hanya berlaku untuk satu kali proses enkripsi. Metode ini sangat baik untuk mengirim pesan yang panjang karena akan semakin sulit untuk mengetahui kunci yang digunakan.

Berdasarkan kelebihan dari algoritma RSA dan OTP diatas, maka penulis tertarik untuk melakukan penelitian yang berjudul ”Kombinasi Algoritma One Time Pad dan Algoritma RSA (Rivest Shamir Adleman) untuk Mengamankan Data (E- KTP)”.

1.2 Rumusan Masalah

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

1. Bagaimana cara mengamankan data dengan menggunakan algoritma One Time Pad dan algoritma RSA pada studi kasus Nama dan NIK guru berser- tifikasi di SMPN 1 Tanjung Pura.

2. Bagaimana cara memanfaatkan kombinasi algoritma One Time Pad dan RSA pada pengamanan data NIK e KTP dan mengubahnya dalam bentuk kode ASCII.

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Data yang diamankan berupa NIK guru yang sudah mendapatkan sertifikasi di SMPN 1 Tanjung Pura.
2. Hasil enkripsi yang dihasilkan berupa kode ASCII

1.4 Tujuan Penelitian

Adapun yang menjadi tujuan penelitian adalah:

1. Mengamankan NIK menggunakan algoritma One Time Pad dan algoritma RSA.
2. Memanfaatkan kombinasi algoritma One Time Pad dan RSA pada penga- manan data NIK e KTP dan menghasilkan kode ASCII.

1.5 Manfaat Penelitian

Dengan diadakannya penelitian ini diharapkan dapat memberi manfaat sebagai berikut:

1. Penelitian ini bermanfaat untuk menambah ilmu pengetahuan tentang algoritma kriptografi khususnya algoritma One Time Pad dan RSA.
2. Menambahan informasi untuk meningkatkan keamanan data dengan teknik kriptografi algoritma One Time Pad dan algoritma RSA bagi pembaca yang hendak melakukan penelitian serupa.