BAB I

PENDAHULUAN

1. 1 Latar Belakang

Perkembangan teknologi terus melaju pesat sehingga proses pertukaran informasi tidak lagi menjadi suatu hal yang asing bagi kebanyakan orang. Tak hanya pertukaran informasi, penyimpanan data dalam komputer juga sudah sering dilakukan karena kemudahan untuk mengakses kembali dan mentransfer data. Salah satu program yang sering digunakan untuk menyimpan data adalah *Microsoft Excel*, yaitu program lembar kerja (*spreadsheet)* yang menyimpan data dalam *cell* yang terdiri dari baris horizontal dan kolom vertikal. Aplikasi ini banyak dimanfaatkan oleh usaha mikro dan menengah untuk membantu dalam pengelolaan data atau keuangan maupun untuk pembelajaran dan perhitungan (Hermawati dan Armin, 2021).

Di antara begitu banyaknya data yang tersimpan, terdapat berbagai data rahasia yang tidak boleh sampai diretas oleh pihak yang tidak diinginkan. Akan tetapi, kebocoran data ternyata masih terjadi di Indonesia. Awal September 2022 lalu, masyarakat dikejutkan dengan munculnya *hacker* bernama *Bjorka* yang mempublikasikan data-data rahasia warga Indonesia seperti nomor identitas penduduk (Sutikno dan Stiawan, 2022). Dilansir dari portal berita Voi.id, Bjorka memberikan sampel 1.048.576 data pemilih KPU dari berbagai provinsi dalam bentuk *file excel*.

Melihat *file excel* yang telah digunakan banyak orang ternyata tidak luput dari ancaman kebocoran data, tentu diperlukan adanya usaha untuk meningkatkan keamanan *file excel*. Salah satu caranya adalah dengan bantuan kriptografi, yaitu ilmu yang mempelajari bagaimana cara untuk menjaga data atau pesan tetap aman (Febrianingsih dkk, 2019). Pengamanan data dengan kriptografi diharapkan dapat mencegah kebocoran data meskipun pada faktanya akan selalu ada celah untuk meretas. Untuk mengurangi peluang bocornya data, penelitian ini mengaplikasikan dua algoritma kriptografi, yakni *Diffie-Hellman* dan RSA.

Algoritma *Diffie-Hellman* atau disebut juga dengan *Diffie-Hellman Key Exchange* adalah algoritma yang berfokus pada pertukaran kunci simetris. *Diffie-Hellman Key Exchange* ditemukan pada tahun 1976 atas hasil kerjasama antara

Whitfield Diffie dan *Martin Hellman* (Saepulrohman dan Negara, 2021). *Diffie-Hellman* memiliki kekurangan di mana algoritma ini hanya terbatas pada proses pertukaran kunci saja dan membutuhkan algoritma lain untuk proses enkripsi dan dekripsi (Nisa dkk, 2020). Oleh karenanya, pembangkitan kunci dengan *Diffie-Hellman* seringkali digabungkan dengan algoritma enkripsi lain untuk mendapatkan tingkat keamanan yang lebih tinggi.

Algoritma RSA ditemukan oleh tiga peneliti pada tahun 1977, ketiga peneliti tersebut adalah *Rivest-Shamir-Adleman* yang kemudian disingkat menjadi RSA (Prastya dkk, 2022). Algoritma RSA termasuk ke dalam kriptografi algoritma asimetris, yang menggunakan kunci publik untuk menghasilkan kunci privat (Nisha dan Farik, 2017). Kekurangan dari algoritma asimetris adalah proses pembangkitan kunci dan penyandian pesan membutuhkan waktu yang lama akibat menggunakan perhitungan yang kompleks, algoritma RSA sendiri menggunakan bilangan prima dan aritmetika modulo untuk proses enkripsi dan dekripsi. Selain itu, pembangkitan kunci memiliki peran penting dalam keamanan RSA karena pembangkitan kunci yang lemah dapat menyebabkan kerentanan terhadap serangan (Nisha dan Farik, 2017).

Tidak sedikit jurnal maupun karya tulis ilmiah lain yang telah memanfaatkan metode *Diffie-Hellman* maupun algoritma RSA yang dipadukan dengan algoritma kriptografi lainnya. Di antaranya Mufadilah (219) yang mengimplementasikan kriptografi *Rivest Shamir Adleman* (RSA) yang ditingkatkan dan steganografi *Least Significant Bit* (LSB) untuk penyandian pesan, Hermawan (2021) yang menggunakan *SHA-256* dengan *Diffie-Hellman*-RSA untuk *Digital Signature*. Sedangkan untuk pengamanan *file excel* pernah diteliti oleh Sari (2019) yang mengimplementasikan *Gronsfeld Cipher* untuk mengamankan *file spreadsheet* pada data keuangan, serta Wahdini, dkk (2021) yang berfokus mengamankan data pelanggan dan penjualan dengan algoritma RSA.

Kombinasi dari metode *Diffie-Hellman* dan algoritma RSA diharapkan dapat memberikan pengamanan yang lebih kuat dibandingkan jika hanya satu metode yang digunakan untuk mengenkripsi data. Algoritma *Diffie-Hellman* membutuhkan perhitungan logaritma diskrit yang sulit untuk dipecahkan (Nisa dkk, 2020). Menurut Munir (2018) dalam bahan ajarnya, letak kekuatan algoritma RSA berada

pada sulitnya memfaktorkan bilangan menjadi faktor-faktor prima. Oleh karena itu, penulis mengambil judul "Implementasi Kriptografi dalam Pengamanan Data Pada *File Excel* dengan *Diffie-Hellman-RSA*".

1. 2 Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan sebelumnya, berikut rumusan masalahnya:

1. Bagaimana skema penggabungan algoritma *Diffie-Hellman* dan RSA untuk pengamanan data pada *file excel*?
2. Bagaimana konstruksi program aplikasi pengamanan data pada *file excel* dengan algoritma *Diffie-Hellman* dan RSA?

1. 3 Tujuan Penelitian

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

1. Membuat skema penggabungan algoritma *Diffie-Hellman* dan RSA untuk pengamanan data pada *file excel.*
2. Mengkonstruksi program aplikasi pengamanan data pada *file excel* dengan kriptografi *Diffie-Hellman* dan RSA.

1. 4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Data pada *file excel* yang dapat diberikan pengamanan adalah data teks.
2. Pengamanan data pada *file excel* yang dimaksud adalah terjaga kerahasiannya (*confidentiality*).

1. 5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Manfaat Teoritis

   Diharapkan penelitian ini bermanfaat secara teoritis. Manfaat yang dimaksud adalah memberikan pemahaman mengenai implementasi kriptografi *Diffie-Hellman-RSA* dalam pengamanan data pada *file excel.*
2. Manfaat Praktis

Secara praktiknya, penelitian ini akan menghasilkan suatu program komputer dengan bahasa pemrograman *Python* untuk melindungi data pada *file excel* dengan algoritma *Diffie-Hellman* dan RSA.