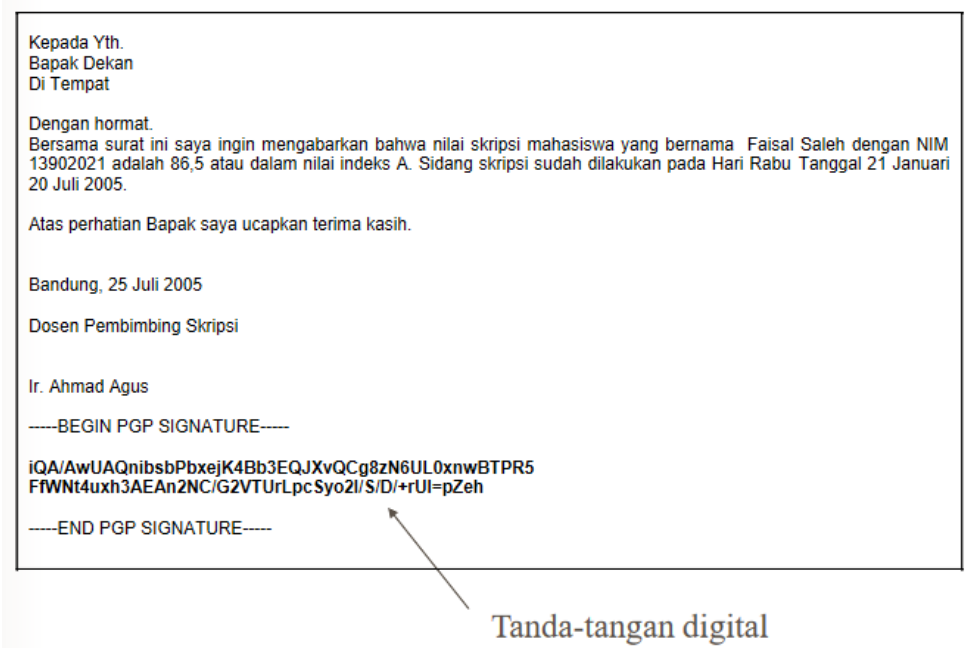
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Di era modern ini penggunaan sertifikat digital semakin marak, hal ini salah satunya disebabkan oleh banyaknya instansi yang mengadakan seminar atau pelatihan secara daring sehingga pemberian sertifikatnya dilakukan secara daring, di mana sertifikatnya berupa sertifikat digital. Seiring dengan banyaknya penggunaan sertifikat digital, pemalsuan terhadap sertifikat digital juga semakin banyak dilakukan.

Akibat dari maraknya pemalsuan sertifikat digital dan dokumen-dokumen yang bersifat penting dan rahasia, diperlukanlah metode yang dapat mengecek keaslian dari suatu dokumen. Para ahli pun melakukan riset mengenai metode-metode pengecekan keaslian dokumen dan ditemukan banyak metode untuk mengecek keaslian suatu dokumen, salah satunya adalah DSA (*Digital Signature Algorithm)*. Alajbegović dkk.(2006) mengatakan bahwa DSA (*Digital Signature Algorithm*) adalah algoritma penandatanganan elektronik yang dapat digunakan untuk mengecek keaslian pengirim suatu pesan atau dokumen, dan dapat memastikan bahwa pesan atau dokumen yang telah dikirim tidak berubah. DSA ini adalah komponen dari DSS *(Digital Signature Standard)* yang dikembangkan oleh NIST *(National Institute of Standards and Technology)*.

Dalam praktiknya *digital signature* dapat menggunakan beberapa metode, salah satunya dengan menggunakan fungsi hash. Munir (2018) memberikan contoh *digital signature* yang diterapkan pada email seperti gambar berikut.



Gambar 1. 1 Contoh *Digital Signature*

Sutopo (2020) juga melakukan implementasi *Digital Signature Algorthm* (DSA) menggunakan *Secure Hash Algorithm*-256 (SHA-256) pada media gambar. Dalam implementasinya, digunakan dokumen berupa file gambar dan diperoleh *digital signature* berupa pasangan string bilangan. Selain itu masih banyak pengimplementasian *digital signature* yang lainnya. Contoh lainnya adalah *digital signature* pada media dokumen digital yang memiliki ekstensi .pdf, menggunakan SHA-256 dengan skema penandatanganan Elgamal dengan tanda tangan berupa pasangan bilangan (Milenium, 2020).

Menurut Munir (2018) dalam bahan kuliahnya, fungsi hash adalah suatu fungsi yang menerima masukan *string* yang panjangnya sembarang lalu mengubah menjadi *string* keluaran yang panjangnya tetap *(fixed)*. Fungsi hash memiliki banyak varian diantaranya adalah MD *(Message Digest)* dan SHA *(Secure Hash Algorithm),* namun MD yang umum digunakan saat ini adalah MD5 karena merupakan pengembangan dari *Message Digest* yang sebelumnya. Menurut Gupta & Kumar (2014) SHA lebih unggul dalam hal keamanan tetapi MD5 lebih cepat pemrosesannya di banding SHA pada mesin 32-bit.

Pada kasus *digital signature* untuk memeriksa keaslian dokumen, umumya menggunakan SHA karena dalam proses *digital signature,* segi keamanan merupakan prioritas yang diutamakan. Dalam jurnal publikasinya di tahun 2015

NIST menjelaskan bahwa SHA memiliki beberapa keluarga yaitu, SHA-1 dan SHA-2, di mana SHA-2 ini merupakan pengembangan dari SHA-1. Sebelum ditemukan SHA-2 dalam proses *digital signature* biasanya digunakan SHA-1. Rijmen & Oswald (2005) mempublikasi penemuan mengenai serangan pada SHA-1, di mana dua buah pesan yang berbeda memiliki nilai hash yang sama oleh karena itu penggunaan SHA-1 tergantikan oleh SHA-2. Pada *digital signature,* nilai hash yang didapatkan dari proses *hashing* selajutnya akan dienkripsi menjadi *signature*.

Proses enkripsi pada penerapan *digital signature* kebanyakan menggunakan RSA (Rivest–Shamir–Adleman). RSA merupakan algoritma kriptografi yang menggunakan kunci publik atau dikenal juga sebagai enkripsi asimetris untuk menghasilkan kunci privat yang dikenalkan pada tahun 1977 dan ditemukan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman (Nisha & Farik, 2017). Menurut Nisha & Farik (2017), pembangkitan kunci yang lemah pada RSA akan menyebabkan kerentanan terhadap serangan, oleh karena itu proses pembangkitan kunci yang baik menjadi sangat penting pada penggunaan algoritma RSA agar dapat menghindari serangan.

Menurut Merkle (1978) pertukaran kunci Diffie-Hellman adalah metode pertukaran kunci kriptografi dengan aman melalui saluran publik dan merupakan salah satu protokol kunci publik pertama yang dibuat oleh Ralph Merkle dan dinamai menurut Whitfield Diffie dan Martin Hellman. Pertukaran kunci Diffie-Hellman dapat digunakan untuk membangkitkan suatu kunci privat. Tak jarang algoritma Diffie-Hellman ini digabungkan dengan algoritma enkripsi lain, untuk membangkitkan kunci sehingga didapatkan kemanan yang lebih tinggi lagi.

Dalam pengimplementasiannya, *digital signature* memiliki kerumitan pada perhitungannya, baik dalam melakukan *hashing* maupun pembangkitan kuncinya. Untuk mempermudah hal tersebut maka diperlukan suatu program aplikasi yang mudah digunakan oleh pengguna nantinya.

Berdasarkan pemaparan di atas maka penulis tertarik untuk melakukan penelitian berkenaan implementasi algoritma *digital signature* menggunakan algoritma SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA.

1.2 Rumusan Masalah

Dari pemaparan latar belakang, dapat diperoleh permasalahan yang dapat dirumuskan sebagai berikut:

1. Bagaimana perancangan *digital signature* menggunakan algoritma SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA?
2. Bagaimana konstruksi aplikasi *digital signature* menggunakan algoritma SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA?

1.3 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah:

1. Dokumen yang akan digunakan untuk penandatanganan digital dalam penelitian ini memiliki ekstensi .pdf.
2. Kunci privat d harus lebih besar dari 255

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dikemukakan sebelumnya, maka tujuan dari penelitian ini adalah:

1. Mengidentifikasi rancangan serta skema dari *digital signature* menggunakan algoritma SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA.
2. Dapat membuat program aplikasi *digital signature* menggunakan algoritma SHA-256 dengan skema penandatanganan Diffie-Hellman-RSA

1.5 Manfaat Penelitian

1 Manfaat Teoritis

Secara Teoritis hasil dari penelitian ini diharap dapat bermanfaat bagi bidang kriptografi khususnya untuk *digitalsignature.* Adapun manfaat tersebut ialah:

a. Memberikan pemahaman mengenai skema enkripsi *hybrid* Diffie-Hellman-RSA
b. Memberikan pemahaman mengenai *digital signature* dengan algoritma SHA-256

2 Manfaat Praktis

Dalam praktiknya hasil dari penelitian ini diharap memberikan manfaat untuk mengkonstruksi program DSA dengan algoritma SHA-256 dengan skema enkripsi *hybrid* Diffie-Hellman-RSA.

1.6 Sistematika Penulisan

Secara umum, sistematika penulisan penelitian ini terdiri atas tiga bagian, yaitu bagian awal, isi dan bagian penutup. Berikut ini merupakan, sistematika penulisan penelitian secara lebih rinci:

- Bab I Pendahuluan, memaparkan tentang latar belakang penelitian, rumusan masalah penelitian, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.
- Bab II Landasan Teori, memaparkan konsep-konsep/teori-teori dalam bidang yang dikaji, penelitian terdahulu yang relevan,
- BAB III Metode Penelitian, memaparkan langkah-langkah yang digunakan dalam menyelesaikan penelitian.
- BAB IV Hasil dan Pembahasan, memaparkan mengenai hasil penelitian yang telah dilakukan.
- BAB V Simpulan dan Saran, menjelaskan simpulan yang didapat dari hasil penelitian, dan memberikan saran atas penelitian yang telah dilakukan.