# IMPLEMENTASI TANDA TANGAN DIGITAL SEBAGAI METODE PENGAMANAN UJIAN ONLINE

**Mohammad Dimas (13507059)**

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha nomor 10
e-mail: if17059@students.if.itb.ac.id

## ABSTRAK

**Ujian merupakan suatu bentuk kegiatan akademik yang sudah umum kita ketahui dari jenajang pendidikan SD hingga pendidikan S3. Pada dasarnya ujian merupakan suatu bentuk evaluasi yang dilaksanakan untuk menguji apakah materi yang disampaikan di sekolah oleh para pengajar dapat diterima oleh para siswa. Akhir akhir ini ada suatu isu yang cukup menarik yaitu bentuk baru ujian, yaitu ujian online.**

**Apakah itu ujian online? Ujian online padadasarnya sama dengan ujian tertulis yang sudah biasa kita laksanakan dan saksikan. Perbedaannya terletak pada metode pelaksanaan ujian. Ujian tertulis konvensional dilaksanakan dengan menggunakan kertas dan alat tulis, dimana ketika ujian telah seleesai dilakasanakan, peserta akan mengumpulkan lembar ujiannya. Berbeda dengan ujian konvensional, ujian online dilaksanakan dengan menggunakan alat bantu komputer dan internet tentunya. Peserta akan menjalankan ujian dengan cara membuka program ujian yang bisa ditampilkan dalambanyak format, contohnya webbase atau desktopbase. Dalam kasus ujian online biasanya ujian berbentuk pilihan ganda namun tidak menutup kemungkinan jika dalam bentuk jawaban bebas. Pada tipe ujian online ketika peserta telah selesai mengerjakan, peserta akan men-*submit* ujiannya ke server, proses *submit* ini dapat dianalogikan sebagai pengumpulan ujian.**

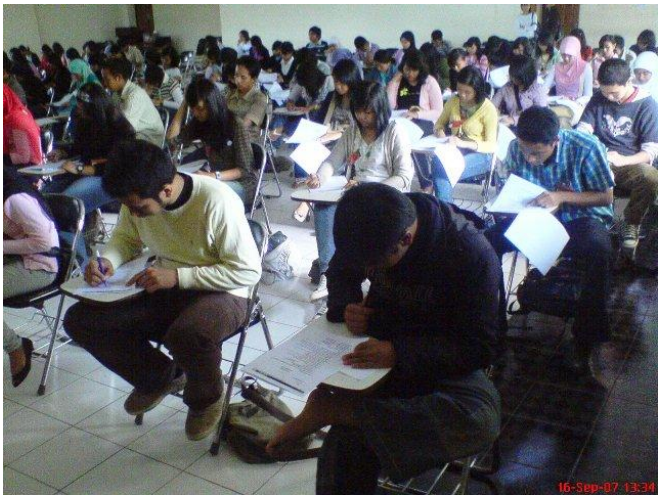
**Masalah yang penulis soroti di sini yaitu bagaimana jika seandainya si peserta memiliki akses ke server melalui jalan lain selain submit, dengan demikian peserta dapat dengan seenaknya mengganti file ujian yang sebelumnya telah ia submit dan terjadilah suatu kecurangan akademik.**

**Dalam makalah ini akan dibahas mengenai pemecahan masalah yang penulis soroti yaitu pengamanan ujian online, solusi yang penulis tawarkan yaitu dengan menggunakan *Digital Signature.* Digital signature atau tanda tangan digital dapat digunakan sebagai metode pembuktian keaslian dokumen. Dalam makalah ini akan dibahas bagaimana aliran proses ujian online nantinya beserta dengan metode pengamanannya yang akan mengimplementasikan konsep tanda tangan digital.**

**Kata kunci:** ujian online, tanda tangan digital, digital signature.

## 1. PENDAHULUAN

Ujian merupakan salah satu bentuk evaluasi yang digunakan untuk menilai ketersampaian pelajaran yang telah diajarkan oleh guru kepada murid. Ujian bisa dilakukan pada media kertas dan alat tulis bisa juga dengan komputer. Ujian dimaksudkan untuk mengukur orang yangmelaksanakannya dalam hal pengetahuan, keterampilan, bakat, atau klasifikasi dibanyak topik lainnya(misalnya keyakinan). Siswa terkadang diperbolehkan untuk melakukan ujian dengan membawa buku teks jika ujian yang dilakukan bertipe *openbook.* Ujian sering dilakukan dalam bidang pendidikan, sertifikasi profesional, konseling, psikologi,militer, dan bidang lainnya.



**Gambar 1 Suasana Ujian SPMB**

Pada suatu ujian tertentu ada yang nilai peserta akan diberikan kepada peserta ada juga yang tidak. Ujian yang bertujuan untuk mengetahui nilai sekelompok orang biasanya tidak akan diberitahukan hasilnya kepada tiap individu yang melaksanakannya, misalnya ujian untuk mengetahui standar tertentu terhadap sekelompok orang.

Sejarah dari ujian ini diketahui sebagai ujian yang dilaksanakan di China yang dimulai padatahun 587. Di eropa, biasanya ujian dilaksanakan secara lisan, siswa diharuskan menjawab pertanyaan yang diberikan oleh gurunya, dan gurunya akan memberikan nilai atas jawabannya. Ujian tertulis pertama diadakan di Universitas Cambridge, Inggris di 1792 oleh professor yang mempunyai gaji rata-rata, dan dia menganggap bahwa ujian tertulis akan dapat menambah penghasilannya.

Ujian dapat dilakukan dalam berbagai macam format. Format-format itu meliputi pilihan ganda, isian bebas, simulasi, benar/salah, dan tipe Likert. Tidak format terbaik untuk dilaksanakan, format ujian yang dilaksanakan harus melihat kepada tujuan ujian itu dilaksanakan. Sebagai contoh, ujian yang bertujuan menguji kemampuan psikomotrik seseorang lebih baik dilaksanakan dalam bentuk simulasi dibandingkan dengan soal tertulis lainnya.

Ujian pilihan ganda, merupakan jenis ujian yang palingumum dilaksanakan,pembuat soalakan menyediakan pilihan kemuingkinan jawaban, biasanya terdiri dari empat atau lima buah pilihan,dan seseorang yang menjalankan test harus memilih dari pilihan-pilihan yang disediakan tersebut. Biasanya pada tipe pilihan ganda hanya ada satu jawaban yang benar, biasanya ditandai oleh pilihan yang benar. Namun pada tipe pilihan tertentu mengharuskan kita melihat pilihan lain dikarenakan jawaban yang benar tidak hanya pada satu pilihan.

Pembuat soal pilihan ganda akan membuat pilihan-pilihan yang salah, yang akan digunakan sebagai pengecoh jawaban, sehingga peserta yang tidak bena-benar tahu akan memilih jawaban yang salah. Sebagai contoh, jawaban pengecoh mungkin direpresentasikan sebagai kesalan konsep yang mungkin terjadi saat proses belajar. Pembuatan jawaban pengecoh yang efektif merupakan suatu tantangan yang harus dihadapi dalam kasus pembuatan ujian pilihan ganda dimana tiap pilihan memiliki kemungkinan kebenaran yang tinggi. Dengan pilihan pengecoh yang berkualitas, dapat meningkatkan kesalahan yang terjadi ketika peserta melakukan penebakan jawaban. Pembuatan pilihan pada soal pilihan ganda memerlukan kemampuan dan pengalaman dari pembuatnya.

Keunggulan dari tipe ujian ini adalah kemudahan dalam pemberian nilai. Mesin seperti Scantron dan mesin penilai lain untuk memeriksa LJK dapat melakukan penelian dengan sangat cepat. Hal tersebut akan ssangat berguna ketika kita tidak memiliki cukup sumber daya untuk mengoreksi ujian dalam skala besar, contohnya pada SPMB atau SNPTN. Ujian tipe ini juga menjadi sangat berguna ketika penyelenggara ujian menginkan hasil yang secepat mungkin, contoh pada saat *tryout*, dimana hasil harus sudah keluar ketika ujian selesai dilakukan.

Bagaimanapun juga tipepilihan gandabukanlah metode yang paling tepat untuk menguji kemampuan dan keahlian.

Format ujian lainnya yaitu tipe jawaban bebas. Format ujian ini tidak memberikan tantangan yang terlalu besar untuk pembuat soal saat iya membuat soal, namun maslaah yang timbul adalah ketika melakukan pemeriksaan. Pemeriksaan yang efektif dapat dicapai dengan membaca seluruh jawaban dengan sangat hati-hati dan mencari katakunci serta kelogisan jawaban.

Tipe ujian seperti ini memungkinkan peserta yang tidak mengetahui jawabannya untuk mengarang bebas, dengan kata lain ia akan menuliskan serangkaian kata yang bersifat umum dan masih memiliki nilai kebenaran, walaupun itu tidak disengaja ia mungkin memperoleh nilai walaupun sebenarnya ia tidak mengetahui jawaban sebenarnya.

**Gambar 2 Ujian Online**

Namun demikian tipe ujian ini lebih dapat membedakan antar peserta yang bisa dan tidak bisa, sehingga penilaian yang diberikan akan lebih objektif dan tepat sasaran.

Suatu isu yang menarik adalah format ujian online. Ujian online merupakan ujian yang dilakukan dengan alat bantu komputer. Ujian dikerjakan di depan komputer dengan format ujian yang biasanya pilihan ganda. Ketika ujian selesai dikerjakan, biasanya hasil dari ujian langsung dikeluarkan.

Dalam makalah ini akan dibahas suatu metode untuk mengamankan ujian online dalam format jawaban bebas. Ketika ujian online yang dilaksanakan diselenggarakan dengan format jawaban bebas, maka penilaian jawaban

tidak akan dilakukan secara isntan oleh program, melainkan akan diserahkan kepada penyelenggara ujian.

Mekanisme dari ujian ini secara singkat berarti, setelah peserta selesai dengan ujiannya, ia akan mensubmit jawaban yang akan disimpan di server dan kemudian, saat proses pemeriksaan jawaban, jawaban-jawaban yang telah di submit akan dibuka oleh pemeriksa. Masalah yang mungkin terjadi yaitu ketika peserta memiliki akses untuk mengapload jawaban melalui jalan lain selain dari program ujian itu sendiri. Dampaknya adalah, peserta bisa mengganti jawabannya, dan kemudian ia mengirimkan ke server melalui jalan lain tersebut, dan tentunya ujian yang ia kumpulkan itu menjadi tidak valid.

Solusi yang penulis coba ajukan ialah dengan menggunakan tanda tangan digital atau Digital Signature. Metode ini merupakan metode yang dapatdigunakan untuk mengecek keaslian suatu berkas atau dokum dalam format digital.

Dengan metode ini diharapkan akan diketahui ketika peserta melakukan kecurangan dalam bentuk penggantian berkas yang telah disubmit dengan memeriksa tanda tangan digitalnya.

## 2. DASAR TEORI

Tanda tangan digital atau digital signature bukanlah tanda tangan yang digitasikan. Tanda tangan digital merupakan suatu skema matematis yang digunakan untuk melakukan validasati atas suatu pesan, berkas, ataupun dokumen. Tanda tangandigital memberikan penggunanya alasan untuk percaya bahwa pesan yang ia terima merupakan pesan yang asli dan berasal dari pengirim yang ia ketahui. Tanda tangan digital digunakan secara umum untuk software distribusi,transaksi keuangan, dan kasus lain yang penting untuk mendeteksi keaslian.

Tanda tangan digital sering digunakan untuk menerapkan tanda tangan elektronik, sebuah istilah yang lebih luas yang mengacu kepada data elektronik yang membawa tanda tangan digital, namun tidak semua data elektronik membawa tanda tangan digital. Pada beberapa negara, Amerika serikat, dan anggota Uni eropa contohnya, tanda tangan elektronik memiliki makna hukum. Namun undang-undang tentang tanda tangan elektronik tidak terlalu jelas apakah mengacu pada tanda tangan digital dalam artian kriptografi atau tidak.

Tanda tangan digital menerapkan konsep kriptografi asimetrik. Untuk pesan yang dikirimkan melalui saluran tidak aman, seperti email, tanda tangan digital memberikan suatu alasan bagi penerima untuk percaya kepada pesan tersebut bahwa ia dikirim oleh pengirim yang diketahui.

Tanda tangan digital dapat memberikan kepercayaan selama kunci privat yang dimiliki oleh pembuat tanda tangan tetap privat, dengan kata lain tidak diketahui orang lain.

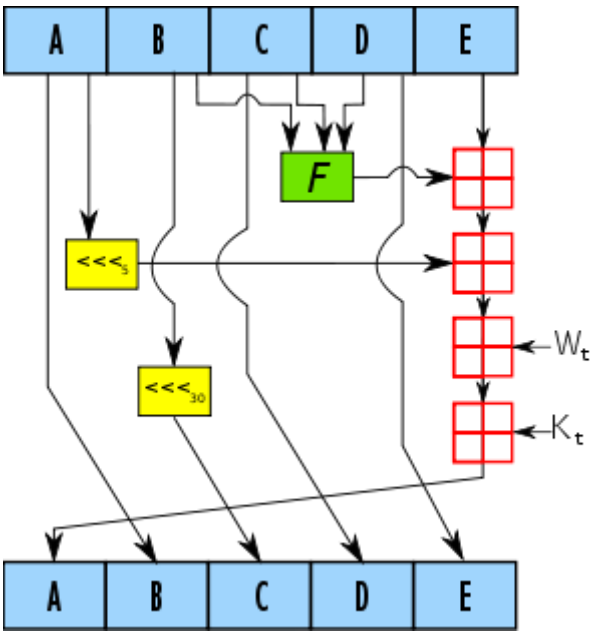
Beberapa konsep yang akan diterapkan disini yaitu pembuatan tanda tangan digital dengan RSA dan SHA1 atau MD5. Dalam implementasinya penulis akan menggunakan library c# sebagai bantuan. Pada makalah ini juga dibahas pemilihan antara SHA1 atau MD5 sebagai fungsi hashnya.

### 2.1 KONSEP SHA1 dan MD5

SHA1 merupakan suatu algoritma hash 160 bit. Algoritma ini merupakan penyusunan ulang atas algoritma MD5, algoritma ini dirancang oleh National Security Agency(NSA) dalam bagiannya menjadi DSA(digital signature algorithm). Algoritma ini biasa disebut denganSHA,namun setelah dipublikasikannya kecacatan pada algoritma tersebut algoritma ini disebut sebagai SHA-1 sebagai versi revisinya.

SHA-1 melakukan proses yang panjang untuk menghasillkan string hasnnya. Prosesnya seacara singkat yaitu, penambahan bit pada berkas yang akan dihash sedemikian hingga panjang bitnya menjadi kelipatan512. Penambahan itu berupa penambahan 1bit true dan sejumlah penambahan bit false dan penambahan panjang berkas sebelumnya dalam64bit.

Setelahnya akan dilakukan pemrosesan terhadap berkas yang telah di padding per512 bit. Berikut adalah gambaran skemanya.



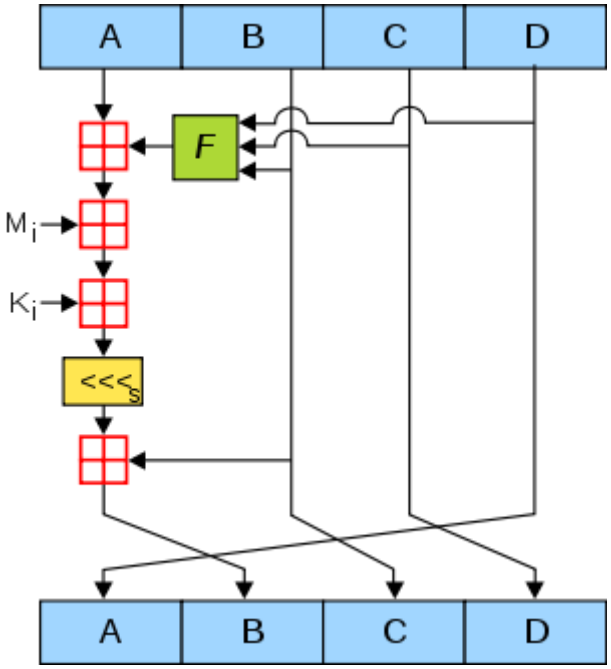

**Gambar 3 skema algoritma SHA1**

Algoritma ini akan selalu menghasilkan panjang string hash yang sama, dalam hal ini 160 bit. Namun algoritma ini memiliki batasan berkas yang akan diprosesnya yaitu batasan panjang sebesar $2^{64}$. Serangan atas algoritma ini

dilaporkan pada tahun 2005 oleh Wang et al, ia berhasil menghasilkan hash yang bertabrakan dengan kompleksitas $2^{64}$ operasi.

MD5 merupakan algoritma hash 128 bit. Algoritma ini merupakan algoritma hash yang paling sering digunakan. Penggunaan algoritma ini biasanya untuk mengecek keintegritasan suatu berkas. MD5 dirancang oleh Ron Rivest pada tahun 1991 untuk menggantikan algoritma hash sebelumnya yaitu md4. Beliau(Ron Rivest) melihat suatu ketidak amanan pada MD4 yang ditemukan oleh Hans Dobbertin sehingga ia memutuskan untuk membuat algoritma hash baru dengan nama MD5. Serangan pada algoritma ini kemudian ditemukan pada tahun2007 oleh M.M J Stevensdengan kompleksitas $2^{24}$, dan serangan ini dilaporkan hanya dilakukan dengan komputer biasa.

Berikut adalah skema algoritmanya:




**Gambar 4 skema algoritma MD5**

Kedua algoritma sama-sama telah dilaporkan celah keamanannya. Dalam implementasinyasebagai aplikasi tanda tangan digital SHA1 lebih cocok dikarenakan, pada tahun 1996 ditemukan suatu celah keamanan padadesain MD5. Namun celah tersebut bukanlah celah yang begitu fatal, lebih lanjut padatahun 2004, celah yang lebih serius ditemukan. Dan pada tahun 2007, sekelompokpeneliti menggambarkan bahwa sepasang berkas yang berbeda dapat menghasilkan MD5 hash yang sama, oleh karena itu US-CERT dari US tidak merekomendasikan algoritma hash ini untuk dijadikan aplikasi tanda tangan digital.

Dengan demikian penulis memilih untuk menggunakan algoritma SHA1sebgai pembuat hash dibandingkan dengan MD5.

## 2.2 KONSEP RSA dan TANDA TANGAN DIGITAL

RSA merupakan metode enkripsi asimetrik. Asimetrik maksudnya untuk melakukan enkripsi dan dekripsi akan digunakan kunci yang berbeda.

RSA berasal dari nama ketika orang penemunya yaitu Rives Shamir dan Adleman. Algoritma ini merupakan algoritma pertama yang memungkinkan untuk dilakukannya tanda tangan digital.

Inti dari RSA adalah pada saat pembuatan kuncinya. Tahapan pembangkitan kunci merupakan proses yang cukup mudah namun akan memakan waktu saat eksekusi programnya. Tahapannya secara singkat yaitu, mencari suatu bilangan p dan q yang merupakan bilangan prima random. Akan dihitung suatu n yang merupakan p kali q. Akan dihitung pula totien yang merupkan t=(p-1)*(q-1). Akan dipilih e sebagai kunci publik yang berada di antara 1 dan totien namun relatif prima terhadap totien. Kemudian akan dicari kunci privat d sedemikian hingga d kali e kongruen dengan 1 mod totien.

Setelah kunci didapatkan rumus enkripsi dan dekripsi merupakan sesuatu yang sederhana. Rumus enkripsi yaitu:

**Persamaan 1rumus enkripsi RSA**

$$c = m^e \bmod n$$

Rumus dekripsi yaitu:

**Persamaan 2 rumus dekripsi RSA**

$$m = c^d \bmod n.$$

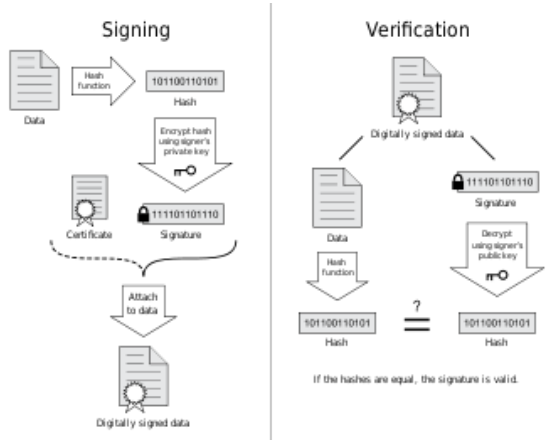
Pada implemntasinya terdapat suatu hambatan yaitu ukuran daya tampung integer ataupun integer64, yang tidak akan cukup menampung perpangkatan tersebut, melihat e dan d akan sangat besar, sehingga solusinya yaitu akan digunakan tipe bentukan bigInteger.

Implementasi algoritma ini pada tanda tangan digital berbeda dengan enkripsi dengan dekripsi pada umumnya. Pada implementasinya yang digunakan untuk melakukan enkripsi ialah kunci privat dan sebaliknya yang akan digunakan untuk melakukan dekripsi yaitu kunci publik.

Haltersebut dilakukan karena tidak semua orang dapat membuat tanda tangan digital. Hanya orang-orang tertentu yang memiliki previlages yang dapatmembuatnya. Oleh karena itu digunakan kunci privat untuk melakukan proses enkripsi. Sebaliknya, dikarenakan semua orang boleh melakukan dekripsi terhadap tanda tangan digital.

Tanda Tangan Digital pertama kali dideskripsikan oleh Whitfield Diffie dan Matin Hellman pada tahun 1976. Dan lanjutnya Ronald Shamir dan Adleman(penemu RSA), mengklaim bahwa algoritmanya tersebut dapat diimplementasikan pada skema tanda tangan digital tersebut.

Tanda tangan digital dibagi menjadi dua buah fitur yaitu pembuatan tanda tangan, dan pengecekan validitas suatu dokumen. Berikut skemanya:




**Gambar 5 skema pemrosesan tanda tangan digital**

Pada proses pembuatan tanda tangan dilakukan terlebih dahulu pembuatan hash dari berkas yang akan ditanda tangani. Setelah diperoleh hash dari berkas tersebut, hash dienkripsi menggunakan algoritma RSA dengan menggunakan kunci privat, dan hasilnya berupa berkas tanda tangan. Untuk melakukan validasi atas berkas, berkas tersebut harus di buat hashnya, setelah itu tanda tangan yang berhubungan dengan dokumen itu diambil, kemudian didekripsi dengan algoritma RSA dengan kunci publik yang berhubungan, setelah proses dekripsi seharusnya diperoleh string yang sama dengan string hash berkas tersebut jika berkas tersebut merupakan berkas yang sesuai dengan tanda tangannya,dan jika tidak sesuai maka string hash dan hasil dekripsi tanda tangan akan berbeda.

## 3. BATASAN MASALAH

Pada makalah ini masalah penulis pada penagnanan ujian dalam format ujian online dengan tipe soal isian bebas. Berkas hasil dari ujian akan berupa berkas txt yang kemudian akan diberi tanda tangan digital dengan algoritmaSHA dan RSA, kemudian ketika penyelenggara ujian akan memeriksa ujian akan dilakukan validasi apakah berkas tersebut masih valid atau sudah terjadi perubahan.

Pada makalah ini, penulis mensimulasikan ujian online dengan membuat suatu program untuk melakukan ujian yang sifatnya lokal, namun pada intinya ia akan tetap menghasilkan berkas txt(tidak dikirim ke server). Dan proses pengecekan dilakukan secara manual dengan program kecil yang memanfaatkan fasilitas .Net berupa fungsi enkripsi SHA1.

## 4. IMPLEMENTASI

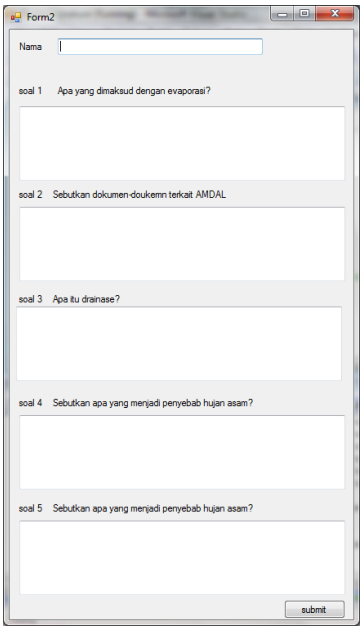
Sejauh ini penulis berhasil membuat program untuk mendukung terselenggaranya ujian online yang lebih bersih. Program yang dibuat yaitu ada dua, program dari sisi client untuk peserta mengerjakan ujiannya dan program bagi penyelenggara ujian untuk memeriksa ujian apakah berkas ujian tersebut valid. Definisi valid yaitu berkas tidak mengalami perubahan sejak file tersebut disubmit pada saat ujian diselenggarakan.

Implementasi dari fungsi SHA menggunakan library yang disediakan oleh .Net yaitu dengan kelas yang disebut SHA1. Dengan fungsi ini kita tidak perlu membuat definisi dari fungsi SHA1 itu sendiri, melainkan tinggal memanggil dan dengan fungsi computeHash, string hash dari berkas yang akan ditanda tangani akan terbentuk.

Untuk bagian RSA, penulis menggunakan kelas BigInter yang berasal dari bouncy castle. Kelas tersebut memang telah dibuat untuk menangani permaslahan RSA, hal tersebut dapat dilihat dari fungsi fungsi yang ia sediakan, mulai dari isprobable prime yang dapat digunakan untuk proses pembangkitan kunci, dan juga fungsi powmod yang berfungsi dalam mengimplementasi algoritma enkripsi dan dekripsi RSA, sehingga kita tidak perlu memangkatkan dahulu kemudian dilanjutkan dengan melakukan mod, karena telah disediakan fungsi untuk melakukan keduanya sekaligus.

Pada aplikasi untuk ujian online ini kunci yang dipakai ter integerasi sehingga akan meminimalkan bocornya private key. Penggantian key tidak dapat dilakukan dengan mudah, melainkan ia harus memiliki privatekey publickey dan n yang sebelumnya telah dipasang.

Berikut adalah tampilan program sisi peserta ujian:




**Gambar 6Tampilan program sisi peserta**

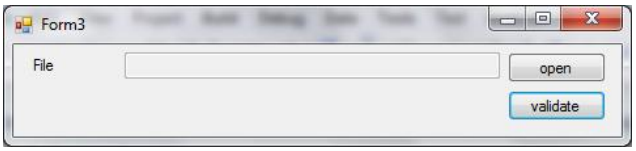
Pada program tersebut terdapat slot identitas berupa nama, dalam hal ini program menyediakan 5 buah soal beserta 5 buah slot jawaban. Tersedia pula tombol submit. Dengan ditekannya tombol submit akan dikirim file ujian peserta dengan format sebagai berikut:

```
Soal1
<<jawaban soal 1>>
Soal2
<<jawaban soal2>>
Soal3
<<jawaban soal3>>
...
SoalN
<<jawaban soalN>>
```

**Gambar 7format pesan**

Seperti yang telah disampaikan sebelumnya pada prototipe ini belum dilakukan pengiriman file, sehingga file memang disimpan secara lokal. Ketika tombol submit ditekan maka akan dihasilkan berkas dengan format seperti diatas, dan nama berkas sesuai dengan nama peserta dengan ekstensi txt. Pada saat yang bersamaan yaitu saat tombol ditekan dilakukan juga pembuatan berkastanda tangan digital dengan nama berkas sesuai dengan nama peserta dengan ekstensi .sg.

Program untuk mengecek validitas berkas ujian yaitu:




**Gambar 8tampilan program sisi penyelenggara ujian**

Program tersebut akan mengecek berkas ujian dengan cara membuka berkas ujian,kemudian program akan mencari nama berkas tanda tangan yang bersesuaian,kemudian program akan menampilkan pesan berupa messagebox, apakah berkas tersebut adalah berkas yang masih valid atau tidak, yang artinya apakah berkas tersebut telah diubah atau belum.

## 5. ANALISIS dan PENGUJIAN

Saat melakukan pengujian dilakukan kepada berkas dengan ukuran 2,14kb. Berkas tersebut berisi jawaban untuk 5 soal ujian bertipe isian bebas dengan kira kira jawaban persoal sepanjang 54 kata.

Saat dilakukan pengujian dengan membuat tanda tangan terhadapnya dan melakukan validasi, waktu yang dibutuhkan sangatlah kecil yaitu hanya `00:00:00.0030001`. waktu tersebut merupakan waktu yang diperoleh jika digunakan kelas SHA1 yang dibawa oleh .NET, dan sebagai perbandingan ketika digunakan kelas SHA buatan penulis pada program ini waktu eksekusi berkas yang sama menjadi : `00:00:00.5710326`.

Terlihat bahwa waktu yang diperlukan sangatlah berbeda, namun keduanya menawarkan waktu yang cukup kecil untuk setiap berkas. Berikut adalah tabel perkiraan waktu ketika diadakan penandatanganan untuk suatu ujian

| Jumlah peserta | Waktu(sha .net) (s) | Waktu(s) |
|---|---|---|
| 50 | 0,15 | 28,55163 |
| 500 | 1,5 | 285,5263 |
| 1000 | 3 | 571,0326 |
| 5000 | 15 | 2855,163 |

Dilihat dari tabel tersebut nampaklah perbedaan yang cukup jauh ketika dilaksanakan ujian dengan jumlah peserta yang banyak. Oleh karena itu penulis memilih untuk menggunakan fungsi SHA yang telah disediakan oleh .NET.

```
SHA sha = new SHA();
RSA rsa = new RSA();
SHA1 sha2 = new
SHA1CryptoServiceProvider();
String hash =
BitConverter.ToString(sha2.ComputeHash(
File.ReadAllBytes(signer_file.Text))).R
eplace("-", "").ToLower();
```

**Gambar 9penggunaan kelas SHA bawaan .NET**

Analisis penulis akan perbedaan yang jauh tersebut diduga karena fungsi SHA memang merupakan proses yang panjang, ditambah lagi SHA yang penulis buat tidak menggunakan fasilitas-fasilitas yang disediakan .NET seperti kelas bitarray yang pada dasarnya telah memiliki primitif-primitif fungsi seperti penambahan dan perkalian dan operator and atau or. Penulis saat membuat kelas SHA-1 membuat tipe bitarray sendiri dengan menggunakan array of boolean,sehingga primitif primitif yang dibutuhkan pun didefinisikan sendiri. Mungkin dikarenakan haltersebut SHA buatan penulis menjadi tidak se-effisien SHA yang telah disediakan oleh .NET.

Saat penulis menguji kevalidan suatu berkas dengan cara mengubah karakternya sebanyak satu buah, saat dilakukan validasi program dapat mendeteksinya dengan mengeluarkan pesan bahwa berkas yang bersangkutan tidka cocok dengan tanda tangan digitalnya, sehingga ketika terjadi kecurangan akan dapat diketahui.

## 6. Kesimpulan

Beberapa kesimpulan yang penulis dapat:

- MD5 tidak sesuai untukdigunakan pada aplikasi yang berhubungan dengan SSL atau digital signature
- SHA 1 merupakan fungsi hash yang relatif tidak ada celah, dikarenakan pada laporan penemuan celah keamannya harus menggunakan banyak komputer(kompleksitas algoritma pembobolnya tinggi)
- Dengan bantuan library .NET eksekusi program menjadi sangat cepat, dengan demikian sangat mungkin bila program ini diimplementasi untuk ujian online yang menggunakan format isian bebas.

## REFERENSI


[1] http://www.rsa.com/rsalabs/node.asp?id=2125
[2] ^ a b Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126.doi:10.1145/359340.359342
[3] http://msdn.microsoft.com/en-us/library/system.security.cryptography.sha1.aspx
[4] http://www.w3.org/PICS/DSig/SHA1_1_0.html
[5] http://www.youdzone.com/signature.html


## PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan bahwa makalah ini dibuat tanpa ada unsur plagiasi,

Mohammad Dimas,13507059
Bandung, 16 Mei 2010