Tanda Tangan Digital untuk Pengecekan Keaslian Data pada Perpustakaan Digital

Nabilah Shabrina (13508087)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18087@students.if.itb.ac.id

***Abstrak*— Buku adalah jendela ilmu merupakan pepatah yang sering kita dengar. Salah satu sarana untuk menambah ilmu adalah dengan pergi ke perpustakaan dan membaca buku di sana. Pada zaman era digital seperti sekarang ini, perpustakaan konvensional yang berisikan rak dan buku secara fisik sudah mulai berubah menjadi perpustakaan digital. Perpustakaan digital merupakan perpustakaan yang berisikan buku-buku maupun artikel dan jurnal, yang disajikan secara softcopy yang dapat diaksses oleh orang-orang dari belahan dunia mana pun di mana pun dan kapan pun. Perpustakaan seperti ini dapat menjadi solusi terhadap keengganan masyarakat untuk pergi ke perpustakaan untuk menuntut ilmu.**

Perpustakaan digital yang dapat diakses oleh orang di mana pun dan kapan pun rentan terhadap manipulasi data. Bukan tidak mungkin data-data yang terdapat di perpustakaan digital dimanipulasi oleh orang tertentu dan tentunya hal itu berakibat informasi yang terdapat pada perpustakaan digital tidak valid. Untuk mencegah hal tersebut diperlukan suatu tindakan untuk pengecekan keaslian dokumen. Salah satu cara yang dapat digunakan yaitu dengan membuat tanda tangan digital untuk setiap dokumen yang diunggah oleh perpustakaan digital. Dengan adanya tanda tangan digital tersebut, maka akan memudahkan untuk pengecekan keaslian dokumen pada perpustakaan digital.

Tanda tangan digital dapat dilakukan dengan menerapkan algoritma, salah satunya dengan algoritma SHA-1 dan RSA. Keunggulan dari algoritma tersebut adalah, algoritma SHA-1 merupakan algoritma searah yang tidak dapat diketahui teks aslinya. Algoritma RSA merupakan algoritma yang sulit dipecahkan karena harus memfaktorkan dua bilangan yang berukuran besar.

Penerapan tanda tangan digital pada perpustakaan digital diharapkan mampu mencegah adanya manipulasi data terhadap dokumen dalam perpustakaan digital sehingga peran perpustakaan dalam menyampaikan informasi yang akurat terhadap masyarakat bisa dicapai.

***Index Terms*— Tanda tangan digital, SHA-1, RSA, perpustakaan digital.**

I. PENDAHULUAN

1.1 Perpustakaan Konvensional

Secara garis besar perpustakaan berfungsi sebagai jendela ilmu yaitu sarana untuk melestarikan peradaban manusia, dengan mengumpulkan, memelihara dan menggunakan kembali koleksi-koleksi perpustakaan yang merupakan sumber informasi. Perpustakaan biasanya identik dengan dunia pendidikan. Masyarakat awam menilai perpustakaan hanya sebagai tempat dimana terdapat rak, dengan buku-buku yang berjajar, seolah-olah di samakan dengan toko buku. Maksud dari didirikan nya perpustakaan adalah menyediakan sarana atau tempat untuk menghimpun berbagai sumber informasi, untuk di koleksi secara berkesinambungan, di olah dan diproses melalui suatu rangkaian tertentu.

Dari berbagai pengertian di atas, perpustakaan adalah suatu unit kerja yang berupa tempat menyimpan koleksi bahan pustaka yang diatur secara sistematis dan dapat digunakan oleh pemakainya sebagai sumber informasi.

Ada beberapa fungsi dari perpustakaan. Ke semua fungsi ini bertujuan untuk memajukan pendidikan di Indonesia. Pertama, perpustakaan merupakan sumber segala informasi. Kedua, merupakan fasilitas pendidikan nonformal, khususnya bagi anggota masyarakat yang tidak sempat mendapatkan kesempatan pendidikan formal. Ketiga, sebagai sarana atau tempat pengembangan seni budaya bangsa, melalui buku atau majalah. Keempat, perpustakaan sekaligus memberikan hiburan bagi pembacanya karena bahan bacaan yang disimpan jenisnya beraneka ragam. Fungsi yang terakhir, merupakan penunjang yang penting artinya bagi suatu riset ilmiah, sebagai bahan acuan atau referensi.

Tetapi sangat disayangkan, masih jarang sekali orang yang memanfaatkan perpustakaan untuk kepentingan tersebut. Bahkan di kalangan perpustakaan perguruan tinggi sekalipun, pada kenyataanya banyak sekali mahasiswa yang tidak pernah mengunjungi perpustakaan dari awal kuliah hingga lulus. Tidak jarang mahasiswa yang mengunjungi perpustakaan hanya ketika mereka menyusun tugas akhir dan skripsi, pada proses nya pun jarang dilakukan penelitian yang benar-benar melibatkan fasilitas perpustakaan. Mahasiswa cenderung lebih menyukai mencari informasi di dunia maya.

Kondisi tersebut membutuhkan suatu solusi yang mendukung berjalannya fungsi dari perpustakan. Terciptanya iklim tersebut dapat dilakukan salah satunya dengan cara mendidik pengguna sehingga fungsi dari perpustakaan dapat dipahami dengan baik.

1.2 Perpustakaan Digital

Salah satu solusi dari permasalahan tersebut adalah dibuatkannya perpustakaan digital, sehingga mahasiswa dapat mengakses sumber-sumber bacaan dari tempat tinggal mereka. Apabila mereka membutuhkan buku secara *hardcopy*, barulah mereka pergi ke perpustakaan fisik untuk membaca buku tersebut.

Teknologi informasi dan komunikasi yang semakin canggih pada zaman ini menyebabkan perpustakaan digital selain secara ekonomi lebih murah juga memiliki beberapa keunggulan lain.

Pertama, perpustakaan digital mudah diakses oleh siapa pun dan dari mana pun asal memiliki koneksi Internet, baik menggunakan PC, laptop, maupun telepon genggam. Para pemustaka tidak perlu datang secara fisik ke pepustakaan. Cukup dengan menyalakan komputer atau telepon genggam terkoneksi internet, para pemustaka dapat melihat katalog, melakukan transaksi pemesanan dan peminjaman buku elektronik, serta mengakses dan mengunduh jurnal elektronik.

Kedua, lebih murah dari perpustakaan konvensional. Hal yang selalu menjadi kendala pada perpustakaan konvensional adalah ruang penyimpanan buku. Dengan memindai bahan pustaka ke dalam bentuk *softcopy* dan menyimpannya ke dalam basis data, maka akan semakin banyak koleksi yang dapat disimpan serta dapat menghemat pengeluaran untuk penyediaan dan pengelolaan ruang perpustakaan.

Ketiga, penghematan juga dapat dilakukan karena biaya pengiriman buku atau jurnal dari penerbit layaknya pada perpustakaan konvensional tidak diperlukan. Dari sisi pemustaka, perpustakaan digital juga amat efisien karena mencari dan mendapatkan buku tidak perlu mencarinya di rak buku, tetapi cukup dengan perangkat pencari yang disediakan atau menggunakan *Google* atau *Yahoo*.

Keempat, perpustakaan digital juga dapat menjangkau khalayak yang luas di seluruh dunia. Dengan demikian, karya ilmiah yang disajikan dalam data dapat dinikmati oleh ribuan bahkan jutaan orang di seluruh dunia. Keterbukaan itu memberi peluang dilakukannya pemanfaatan ilmu pengetahuan dan teknologi secara cepat dan terukur dan optimal, oleh siapa pun di dunia.

Kemudahan yang kini dapat dinikmati sedikit banyak dipicu oleh pemeringkatan pemanfaatan Internet untuk kepentingan pendidikan yang dikenal dengan nama Webometric yang dikeluarkan oleh sebuah laboratorium komputer berpusat di Spanyol. Karena ranking yang dihasilkan mendunia dan dibaca oleh banyak orang, setiap universitas berusaha memperbaiki rankingnya agar unggul dari universitas lain.

Persaingan itu memicu setiap universitas memperkaya aspek-aspek yang dijadikan dasar penilaian. Dampak yang paling sederhana adalah makin banyaknya perguruan tinggi yang mengunggah file berjenis PDF, .PPT atau .DOC ke dalam laman webnya. Dari sinilah akses terbuka yang memberi kemudahan bagi perpustakaan maya dimulai

1.3 Permasalahan Perpustakaan Digital

Perpustakaan digital bukan berarti tidak memiliki kelemahan. Berhubung perpustakaan digital dapat diakses oleh hampir semua orang di dunia, maka data-data tersebut rentan untuk diunduh sembarang orang. Bukan hal yang tidak mungkin bila ada seseorang yang memanipulasi dokumen tersebut. Untuk mengecek keaslian dari dokumen-dokumen asli yang terdapat pada perpustakaan digital, maka digunakan tanda tangan digital untuk pengecekan keaslian dokumen tersebut.

II. TANDA TANGAN DIGITAL

Tanda tangan digital atau *digital signature* merupakan salah satu cara untuk mengecek keaslian suatu dokumen. Salah satu cara penyusunan tanda tangan digital yaitu dengan mengkombinasikan dua buah algoritma, yaitu algoritma SHA dan RSA.

2.1 Algoritma SHA (*Secure Hash Algorithm*)

SHA adalah fungsi *hash* satu-arah yang dibuat oleh *NIST* dan digunakan bersama *DSS* (*Digital Signature Standard*). Oleh *NSA*, *SHA* dinyatakan sebagai standard fungsi *hash* satu-arah. *SHA* didasarkan pada *MD4* yang dibuat oleh Ronald L. Rivest dari *MIT*.

Algoritma *SHA* menerima masukan berupa pesan dengan ukuran maksimum 2^{64} bit (2.147.483.648 *gigabyte*) dan menghasilkan *message digest* yang panjangnya 160 bit, lebih panjang dari *message digest* yang dihasilkan oleh *MD5*.

SHA mengacu pada keluarga fungsi hash satu-arah, yaitu fungsi yang tidak bisa mengembalikan ke bentuk asal.

Enam varian dari SHA yaitu SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, dan SHA-512. Adapun SHA-0 sering diacu sebagai SHA saja.

Berikut merupakan karakteristik dari SHA-0, SHA-1, dan SHA-2:

		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Operations	Collisions found?
SHA-0									Yes
SHA-1		160	160	512	$2^{64}-1$	32	80	+,and,or, xor,rot	Theoretical attack (2^{51})[5]
SHA-2	*SHA-256/224*	256/224	256	512	$2^{64}-1$	32	64	+,and,or, xor,shr,rot	No
	SHA-512/384	512/384	512	1024	$2^{128}-1$	64	80		

Gambar 2.1.1 Perbandingan beberapa algoritma SHA

Adapun proses singkat dari SHA adalah sebagai berikut:

SHA membutuhkan 5 buah penyangga (buffer) yang masing-masing panjangnya 32 bit.

Total panjang penyangga adalah 5 x 32 = 160 bit.

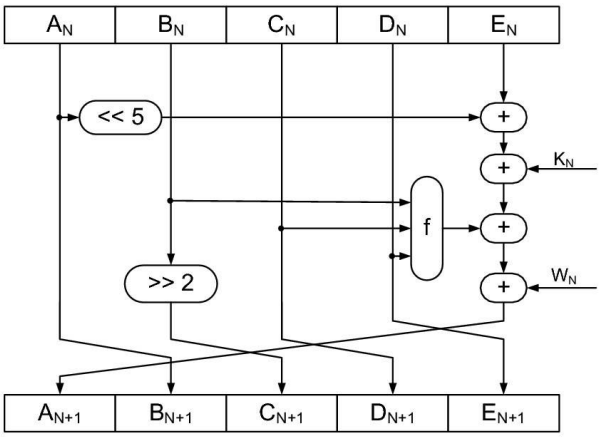
Kelima penyangga MD ini diberi nama A, B, C, D, dan E. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut:

A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
E = C3D2E1F0

Proses H_{SHA} terdiri dari 80 buah putaran (*MD5* hanya 4 putaran)
Masing-masing putaran menggunakan bilangan penambah K_t, yaitu:

Putaran $0 \le t \le 19$ K_t = 5A827999
Putaran $20 \le t \le 39$ K_t = 6ED9EBA1
Putaran $40 \le t \le 59$ K_t = 8F1BBCDC
Putaran $60 \le t \le 79$ K_t = CA62C1D6

Berikut merupakan skema operasi pada SHA-1:



Gambar 2.1.2 Skema operasi algoritma SHA-1

2.2 Algoritma RSA

Algoritma RSA merupakan algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya. Algoritma ini ditemukan oleh tiga peneliti dari MIT (Massachussets Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Algoritma RSA memiliki beberapa property yang digunakan untuk proses enkripsinya, yaitu sebagai berikut

1. p dan q bilangan prima (rahasia)
2. $n = p \cdot q$ (tidak rahasia)
3. $\phi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
   Syarat: PBB(e, $\phi(n)$) = 1
5. d (kunci dekripsi) (rahasia)
   d dihitung dari $d \equiv e^{-1} \bmod (\phi(n))$
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Setelah itu, dilakukan penurunan terhadap rumus RSA sebagai berikut

- Prinsip: Teorema Euler $a^{\phi(n)} \equiv 1 \pmod{n}$
- Syarat:
  1. a harus relatif prima terhadap n
  2. $\phi(n)$ = Toitent Euler = fungsi yang menentukan berapa banyak dari bilangan-bilangan 1, 2, 3, …, n yang relatif prima terhadap n.

Contoh: $\phi(20)$ = 8, sebab terdapat 8 buah yang relatif prima dengan 20, yaitu 1, 3, 7, 9, 11, 13, 17, 19.

Jika $n = pq$ adalah bilangan komposit dengan p dan q prima, maka $\phi(n) = \phi(p)\,\phi(q) = (p-1)(q-1)$.

Kemudian dilakukan proses sebagai berikut:

$a^{\phi(n)} \equiv 1 \pmod{n}$

$\downarrow$ (pangkatkan kedua ruas dengan k)

$a^{k\phi(n)} \equiv 1^k \pmod{n}$

$\downarrow$

$a^{k\phi(n)} \equiv 1 \pmod{n}$

$\downarrow$ (ganti a dengan m)

$m^{k\phi(n)} \equiv 1 \pmod{n}$

$\downarrow$ (kalikan kedua ruas dengan m)

$m^{k\phi(n)+1} \equiv m \pmod{n}$

Misalkan e dan d dipilih sedemikian sehingga

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

atau

$$e \cdot d = k\phi(n) + 1$$

Maka

$$m^{k\phi(n)+1} \equiv m \pmod{n}$$

$$\downarrow$$

$$m^{e \cdot d} \equiv m \pmod{n} \quad \rightarrow \quad (m^e)^d \equiv m \pmod{n}$$

- Enkripsi: $E_e(m) = c \equiv m^e \bmod n$
- Dekripsi: $D_d(c) = m \equiv c^d \bmod n$

Untuk membangkitkan kunci publik RSA, maka dilakukan langkah sebagai berikut:

1. Pilih dua bilangan prima, p dan q (rahasia)
2. Hitung $n = pq$.
3. Hitung $\phi(n) = (p-1)(q-1)$.
4. Pilih sebuah bilangan bulat e untuk kunci publik, sebut, e relatif prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi, d, dengan persamaaan $ed \equiv 1$ (**mod** $\phi(n)$) atau $d \equiv e^{-1} \bmod (\phi(n))$

Hasil dari algoritma di atas berupa sepasang kunci publik dan kunci privat:

- Kunci publik adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

Proses enkripsi dilakukan sebagai berikut:

1. Nyatakan pesan menjadi blok-blok plainteks: m_1, m_2, m_3, … (syarat: $0 < m_i < n-1$)
2. Hitung blok cipherteks c_i untuk blok plainteks p_i dengan persamaan

$$c_i = m_i^e \textbf{ mod } n$$

yang dalam hal ini, e adalah kunci publik.

Proses dekripsi dilakukan dengan menggunakan persamaan :

$$m_i = c_i^d \textbf{ mod } n,$$

yang dalam hal ini, d adalah kunci privat.

III. TANDA TANGAN DIGITAL PADA PERPUSTAKAAN DIGITAL

Salah satu syarat sebelum mengunggah dokumen ke perpustakaan digital, dilakukan terlebih dahulu pemberian tanda tangan digital pada dokumen tersebut.

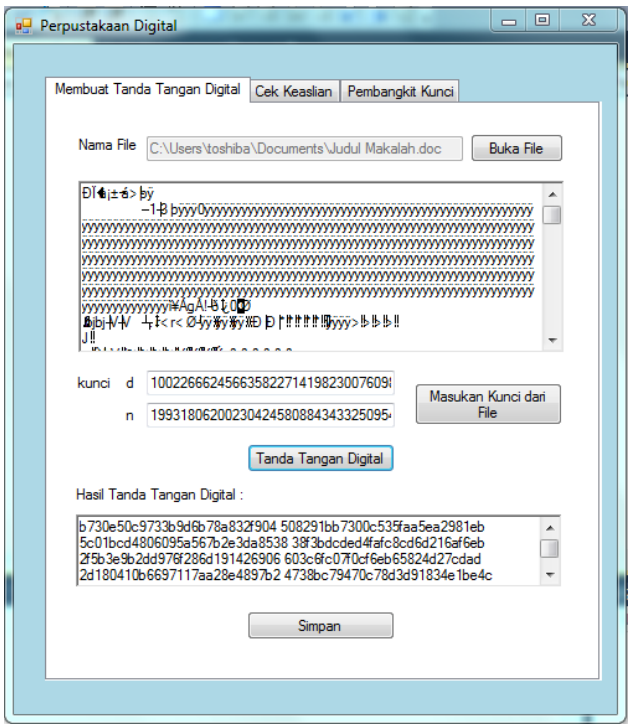
Tanda tangan digital pada dokumen dilakukan dengan menerapkan algoritma RSA dan SHA-1 di dalam program.

Secara garis besar, algoritma untuk pemberian tanda tangan digital adalah sebagai berikut:

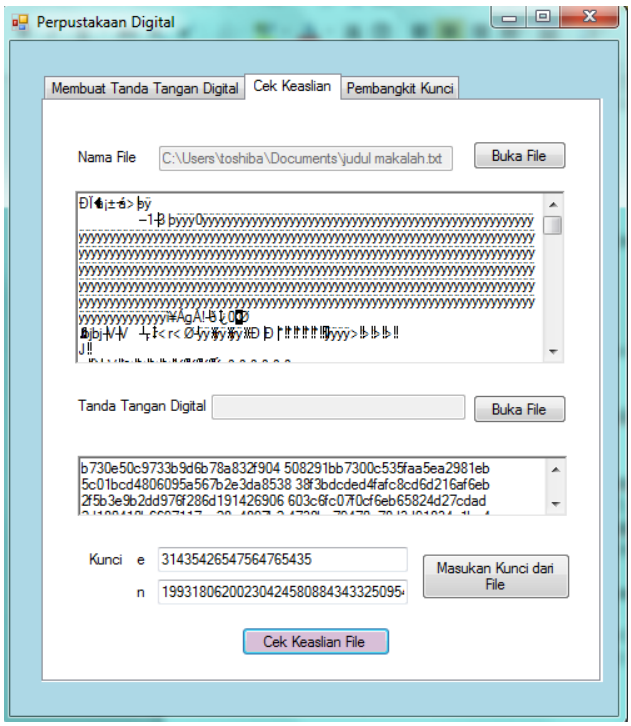
```
//variabel global

byte[] isifile;
string filename;
byte[] signature;
String hasilRSA;
byte[] hasilSHA;
bool compareDS;


//algoritma untuk membuat tanda tangan digital

hasilSHA = program.SHAmessage(isifile);
hasilRSA = Enkripsi(hasilSHA, KeyD.Text,
KeyN.Text);
signature = StrToByteArray(hasilRSA);

//algoritma untuk mengecek keaslian dokumen

hasilSHA = program.SHAmessage(isifile);
hasilRSA = Dekripsi(signatureText.Text,
LoadKeyE.Text, LoadKeyN.Text);
compareDS=compare(hasilRSA, hasil SHA);
```

Pertama, teks asli akan diubah menjadi suatu *message digest* dengan panjang tertentu oleh algoritma SHA-1, kemudian hasilnya akan dienkripsi oleh algoritma RSA dengan menggunakan kunci privat. Kunci yang digunakan pada algoritma RSA memiliki format big integer yang panjangnya bisa mencapai 256 bit. Kunci yang panjang ini akan menghasilkan tanda tangan digital yang panjang pula. Semakin panjang kunci, semakin panjang tanda tangan digital yang dihasilkan.

Contoh antarmuka program adalah sebagai berikut:



Gambar 3.1 Antarmuka pembuatan tanda tangan digital



Gambar 3.2 Antarmuka pengecekan keaslian dokumen

Setelah dilakukan pembuatan tanda tangan digital, hasil tanda tangan digital yang telah didapat disimpan di suatu tempat. Kemudian akan dicocokkan dengan dokumen aslinya bila terdapat keraguan terhadap keaslian dokumen tersebut.

Cara mencocokkannya adalah sebagai berikut. Pertama, dokumen yang dicurigai keasliannya dibuat message digest dengan algoritma SHA-1. Setelah itu tanda tangan digital yang disimpan, didekripsi dengan kunci publik algoritma RSA. Kedua hasil tersebut dibandingkan. Bila hasilnya sama, maka dapat disimpulkan dokumen tersebut merupakan dokumen yang asli.

Berikut ini merupakan contoh antarmuka program untuk mengecek keaslian dokumen.

Bila keluar pesan asli, maka dokumen tersebut benar-benar asli milik perpustakaan digital. Namun bila terdapat perubahan dalam dokumen, maka akan keluar pesan tidak asli. Perubahan sekecil apa pun pada dokumen akan mengeluarkan pesan tidak asli.

IV. ANALISIS

Pengecekan keaslian data menggunakan tanda tangan digital, yang berisi algoritma SHA-1 dan algoritma RSA memiliki beberapa keuntungan. Algoritma SHA-1 merupakan algoritma satu arah, atau algoritma yang tidak mempunyai cara untuk mendekripsi sehingga tidak bisa dikembalikan ke teks awal. Perubahan sedikit pada teks asal akan mengakibatkan perubahan yang berarti pada hasil algoritma SHA-1 sehingga bisa dikatakan algoritma ini memiliki kesensitifan yang tinggi terhadap perubahan teks sekecil apa pun. Sedangkan algoritma RSA merupakan salah satu algoritma yang sulit dipecahkan karena algoritma ini menggunakan dua bilangan yang besar dalam pembuatan kuncinya. Pemfaktoran dua bilangan besar ini sangat sulit untuk dilakukan.

Cara ini cukup aman untuk pengecekan keaslian data, asalkan data yang berisi tanda tangan digital tetap ada.

V. KONTRIBUSI TERHADAP MASYARAKAT

Dengan diterapkannya tanda tangan digital pada setiap dokumen yang terdapat dalam perpustakaan digital, maka akan meningkatkan keamanan data pada perpustakaan digital. Keberadaan perpustakaan digital ini sangat penting bagi masyarakat, supaya masyarakat gemar membaca, dan memudahkan masyarakat untuk mendapatkan informasi yang akurat di mana pun dan kapan pun.

VI. KESIMPULAN

Penerapan tanda tangan digital pada dokumen yang terdapat pada perpustakaan digital dapat menjadi salah satu cara mengecek keaslian data tersebut bila suatu saat terjadi manipulasi dokumen.

Tanda tangan digital yang mengandung algoritma RSA dan SHA-1 cukup efektif untuk digunakan. Cara ini cenderung aman untuk diterapkan karena sulit dipecahkan oleh kriptanalisis.

REFERENCES

[1] http://perpustakaan.upi.edu/

[2]http://www.isgtw.org/feature/isgtw-feature-secure-enough-re-assessment-worlds-most-used-hash-function

[3] Slide IF 3058, Kritpografi, Rinaldi Munir

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Mei 2011

Nabilah Shabrina (13508087)