New Concept Of Security E-Documents With Hybrid Method: Biometric Signature And DSA (Digital Signature Algorithm)

Ana Wahyuni

Department of Computer Science
AKI University
Semarang, Indonesia
Email: whytio@gmail.com

Bayu Surarso, Aris Sugiharto

Department of Information System
Postgraduate Programs,
Diponegoro University
Semarang, Indonesia
Email: bayusurarso@yahoo.com,
Email: aris.sugiharto@gmail.com

***Abstract*— Exchange of electronic documents (e-documents) or documents in an e-mail on the internet has been widely used as a commercial transaction. To ensure e-document is still intact / authentic to the party verifier in transit on the network insecure one of them by giving digital signatures on e-documents. The purpose of this research is to create a new concept in the security of e-documents with a hybrid method: Biometric signatures and DSA (Digital Signature Algorithm) as one solution to the problem of key management and meet the needs non-singular signer. The input as key generator is the offline signature of one or more users for produce one or more digital signatures to a single e-document. Furthermore, e-documents, digital signatures and public key is transmitted over the internet via e-mail on verifier. Then the verifier to verify whether the results are valid or invalid.**

Keywords : signer, verifier, off-line signature, digital signatures, Biometric signatures, DSA.

I. INTRODUCTION

Exchange of electronic documents (e-documents) or documents in an e-mail on the internet has been widely used as a commercial transaction. Documents often contain important information such as contracts, financial transactions, record sales and others. Often the most important thing that is included in the document signature (handwritten) signer. Verification of a document in terms of authorization (endorser) made to the signature of a person or signer who signed the document. The document is very important in commercial transactions over the Internet such as the e-mail. To ensure that e-documents received intact / authentic means the same with e-documents submitted and the actual signer is a signatory of the e-document, one of them by giving digital signatures.

Digital signature is a cryptographic value which depends on the message and the sender / signer [4]. However, cryptographic algorithms to create digital signatures [1] allows only one digital signature to an e-document. This is inconsistent with the concept of digital signatures that depend on the sender / signer where more than one signer. Necessitating a new concept of digital signatures that can serve as an authorization of an e-document as well as the authorization signature (handwritten) some of the signer on the physical document. One method that can meet the needs of digital signatures by more than one the signer biometric offline signature. Offline signature is a signature on documents offline physical digitized by a scanner [5].

DSA (Digital Signature Algorithm) is one of public key cryptography used for authentication, data security and anti-deny device. At DSA needed a special program for generating keys and problems that arise are of user confidence in the program. In the Digital Signature Standard [1] the private key is used for a certain period and can be extended for the generation of digital signatures using the private key. Similarly also applies to public key that can be used continuously for a partner that is the private key is used to generate digital signatures. Similarly, DSA parameters can be used together in a group of users and the public. DSA parameters specified value (fixed) and can still be used or extended for some period of time. The use of parameters, the public and private keys are fixed for a certain time and extended for a period of time, is an avenue of insecurity using the DSA algorithm, because the attacker has the opportunity and time along with the increasing processor speeds. The solution of this problem is by using parameters, public key and private key that is dynamically different value for each process of making digital signatures. So it is necessary that each lock changed long before the public and privat key can be found by exhaustive search [4]. So that needs to be built by the method of application of cryptographic DSA (Digital Signature Algorithm) that can dynamically generate the key as one of the solutions in terms of key management.

In addition to key management issues, the DSA produces only one value of digital signatures on a single e-document. In fact often signer is not only one person at a single e-document. If the signer is more than one digital signature is needed more than one to one e-document. This can be overcome by the use of biometrics in particular

signatures (handwritten) of each signer. Signature (handwritten) someone called biometric signatures [6].

The use of biometric signature of each signer can be used to create digital signatures that allow more than one signer on a single e-document. While digital signatures on the DSA with input biometric signature signer can generate key pairs dynamically and allow more than one signer. So the purpose of this study establish a new concept for the security of e-documents with the hybrid method, or the incorporation of biometric signatures and DSA (Digital Signature Algorithm) as one solution to the problem of key management that can dynamically generate the key, although with the same input and meet the needs of more than one signer on a single e-document

II. DIGITAL SIGNATURE

In some cases authentication is often a necessary but not the message confidentiality. Those needs can be met by the provision of digital signatures. Public key cryptography used in digital signatures can be expressed as: E_{kd} (M) = C, D_{ke} (C) = M, where: E = encryption, D = decryption, M = Message, C = cipher, kd = private key, and ke = public key [3]. In August 1991, NIST (The National of Standards and Technology) announced the standard for digital signatures, called the Digital Signature Standard (DSS) which consists

of two components:

a. So-called digital signature algorithm DSA (Digital SignatureAlgorithm)

b. Hash function, called SHA (Secure Hash Algorithm) So the DSA for signing and SHA message digest of massage to awaken the message [4]. While the hash function used is SHA-1 [2].

In this study developed a new concept for the security of e-documents with a hybrid method of biometric signatures and DSA. Biometric signature is defined as the process of losing the private key from a biometric sample and using a private key to sign e-documents [6]. Biometric signature is used that is signature (handwritten) offline to generate the key pair parameters and dynamically. Offline signature is used to facilitate the signing e-documents, because they do not have all the right bits for each person's signature and signature verification should not be unique but only on the validity of digital signatures. Biometric signatures are combined with offline DSA meet the needs of e-documents with more than one signer to produce not just one digital signature, but as much as its signer.

III. METHODOLOGY

Figure 1 illustrates the process flow of digital signatures with a Hybrid Method: Biometric Signature and DSA. From the results print out documents (physical documents) that have been given a signature by the signer, with the scanning process, the manual signature is taken to be processed into code strings. Of the code string is used as value parameters and SEED to generate a key pair of private key and public key. Public key is derived from the acquired private key. Key pair is used in the generation of digital signatures (signing). E-documents, the digital signature and public key then sent via the Internet as a file attachment in an e-mail. After the e-mail received verifer party, then a process of verification of the file attachment. On the results of the verification process will display the results of the verification that the message is still valid and the original e-document sent by the sender / signer actual or invalid.

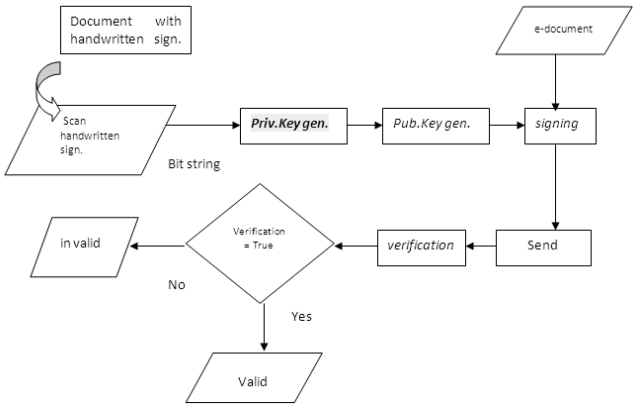

Figure 1. Digital signature Process Flow by Hybrid Method : biometric Signature and DSA

Step-by-step process of generating a key pair on digital signatures using a hybrid method: Biometric Signatures and DSA as follows :

1. The calculation of p, q and g
   a. p = 512 to 1024-bit primes
   b. q = 160 bit the prime factors of p-1
   c. g = $h^{(p-1)/q}$ mod p, where h<(p-1) and $h^{(p-1)/q}$ mod p > 1
2. Generating private key
   Calculate offline signature string code specified. Take the sting code signatures offline as SEED value to generate the private key x.
3. Generating the public key
   Calculate $y = g^x$ mod p. Value of y is p-bit public key

SEED value is used in the process of key generation, digital signature generation process and the process of verification which correspond to the steps on the Digital Signature Standard [1].

IV. RESULT

The results of this study is the software of digital signatures as the implementation of a hybrid method: a biometric signature and DSA as a new concept in solution on key management and allow more than one signer. Resulting software consists of three core processes of the

key generation process, digital signature creation and verification process.

A. Key Generation Dynamically

Figure 2 display a result of the process of creating a key with the input ttd1.jpg and 1024-bit key length.

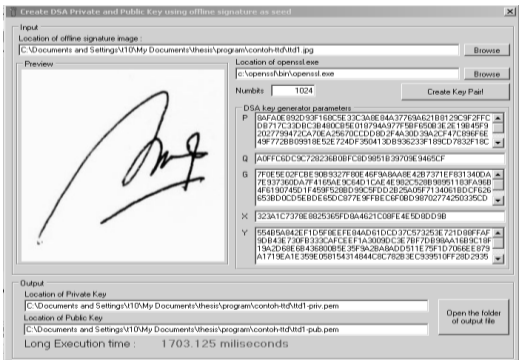

Figure 2. Example Display Making Process And Public Private Key Pair (1) of TTD1.JPG

With input ttd1.jpg generate keys in Figure 2, but it can generate another key is in Figure 3 and 4.

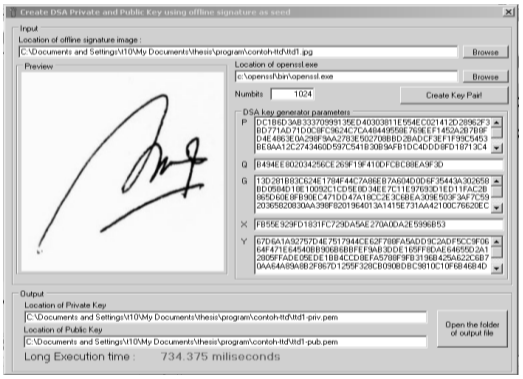

Figure 3 Private And Public Key (2) Generated From TTD1.JPG

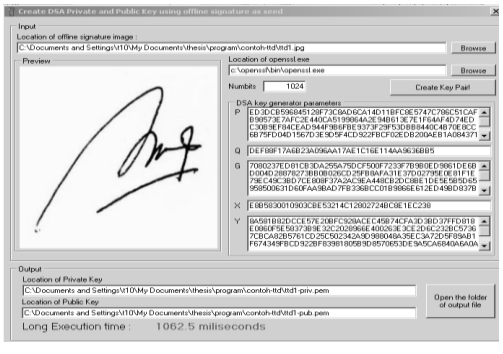

Figure 4 Private And Public Key (3) Generated From TTD1.JPG

Difference key pair (2) and (3) the resulting figure 3 and 4 are given in Table 1.

TABLE 1 THE KEY DIFFERENCE IS GENERATED BASED ON FIGURES 3 AND 4

P(2)	P(3)	Q(2)	Q(3)	G(2)	G(3)	X(2)	X(3)	Y(2)	Y(3)
DC1 …	ED3 …	B49 …	DEF …	13D …	708 …	FB5 …	E8B …	67D …	8A5 …

Based on Table 1 can be explained that of the same signature (one signature offline) with the same key length, can be used to create a different key pair so as to meet the possibility of a unique signature of a person who does not mean there are some people who have the signature of the same / similar but generated a different key. Also, results from one key to making the same input can produce more than one pair of different keys, which means whenever required can result in a different key from the same input. This suggests a new concept in the dynamic key generation, as one solution to the key management aspects. So the key is the nature of the use of disposable means that whenever a key is needed to make a pair of new / different though from the same input. This is because prime numbers are randomly generated and are available on 1024 bit numbers about 10^{305} primes [3]. The next key that is generated can be used to process digital signatures on e-documents.

B. Digital Signature by One signer

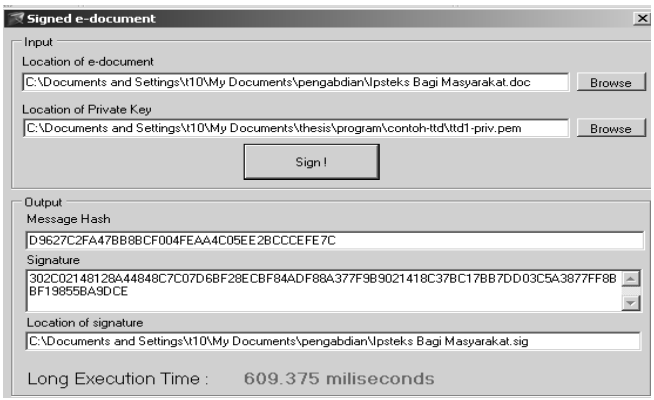

Figure 5 Results Of Digital Signature Ipsteks Bagi Masyarakat.Doc With Key TTD1-PRIV.PEM

Next e-documents, public key and the signature can be sent together or separately via the internet for example in an e-mail to the verifier. On the verifier can be a process of verification. Assumed to e-documents, public key and signature to the verifier party without any lost / stolen during the trip transmission via the Internet. Figure 6 shows the contents of some of the first page of the file "Ipsteks Bagi Masyarakat.doc" valid/ still intact which is stored in C: \ Documents and Settings \ t10 \ My Documents \ service \ Ipsteks Bagi Masyarakat.doc.

Figure 6. Pieces Home Page File Ipteks Bagi Masyarakat.DOC (FILE AUTHENTIC / LEGAL)

Figure 6 Display Pieces Home Page File Ipteks Bagi Masyarakat.doc (File Authentic / Legal)

Figure 7 shows the results of verification of valid e-documents / whole / genuine and legitimate signer. Based on the figure 7, if e-document is still intact / original signer and the signer is in fact (signature and public key is valid) then the verification result is "Valid".

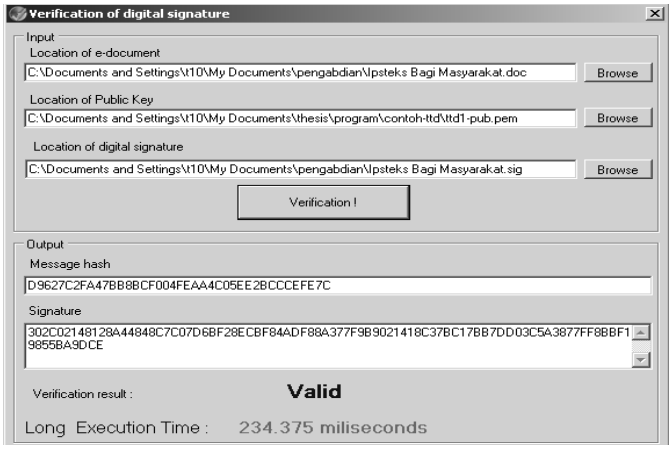

Figure 7 Result Verification With E-Documents, Public Key And Signature Of Legal

Figure 8 shows the contents of e-documents "Ipsteks Bagi Masyarakat.doc" invalid / not authentic by being given an additional one space on the title of "Usulan (double spaced) Program .." files are stored in C: \ Documents and Settings \ t10 \ My Documents \ simulasi \ Ipsteks Bagi Masyarakat.doc.

Figure 8 Display Pieces Home Page File Ipsteks For Masyarakat.Doc Non Authentic / Unauthorized

Figure 9 shows the results of the verification file "Ipsteks Bagi Masyarakat.doc unauthorized stored in C: \ Documents and Settings \ t10 \ My Documents \ simulasi \ Ipsteks Bagi Masyarakat.doc with a valid signature that is stored in C: \ Documents and Settings \ t10 \ My Documents \ service \ Ipsteks Bagi Masyarakat.sig and valid public key (ttd1-pub.pem). Changes in e-document will cause the message digest is different. This is what causes the results of verification "Invalid". Changes have been done on some of the contents of e-documents include the addition or subtraction of characters (letters / words, spaces) or images, color replacement character or image, or image replacement character size, character or image deletion and replacement of the character or image position.

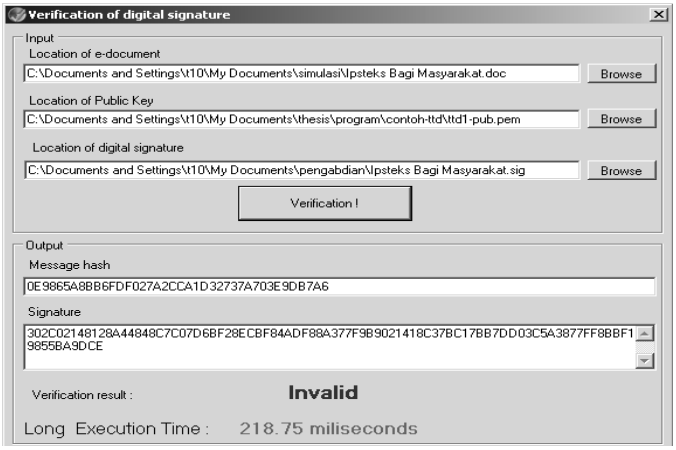

FIGURE 9 RESULTS VERIFICATION AGAINST UNAUTHORIZED E-DOCUMENTS

The results of verification with 18 combinations of possibilities that occur include e-documents valid / invalid, public key valid / invalid / corrupted and the signature is valid / invalid / broken only give the results of verification 'valid' for e-documents, public key and signature valid , in addition to the verification result 'invalid'. Public key or signature corrupted/ broken is assumed to be the replacement of damaged contents / editing a public key or signature is valid. While the file type of e-documents that have been given a signature of files with extensions: php, mp3, pptx, ppt, html, pdf, txt, bmp, sys, docx, doc, xlsx, xls, zip, exe, jpg.

C. Digital Signature by More than One signer

In some cases, often signing / signer of a document or e-documents is two or more people. It is necessary to further strengthen the importance of e-document. On the other side of the digital signatures of more than one to one e-document further strengthen the security of the contents of e-document authenticity and validity of the signer. This is a new concept which allows more than one digital signature according to many e-signer on a single document. If done

giving a digital signature by the two-signer, e-document that is required is an e-document files (*.*) and a copy of the file the e-document (copy of *.*). If the signer is more than two such n it is necessary to file a copy of the e-document as much as (n-1). This is done because the signature of each signer will be created and stored by the system automatically according to the e-document file name, so the signature of each signer is saved with different file names.

In this simulation example there are two signer. As the input is offline signer and signature details. Details are only examples, so it can be replaced number of the document, signer's name or other information indicating authorization (endorser) on the physical document. Figure 10 shows the results of a signer 1 key generation and figure 11 shows the results of making key signer 2. Figure 12 shows the digital signature of the signer 1 and Figure 13 shows the digital signature of the signer 2. As an example of e-documents to be given a digital signature is 1.php.

Then e-documents, the digital signature signer 1 and signer 2, a signer's 1 and 2 public key sent via e-mail. E-mail will be accepted by the verifier who will verify the authenticity of the e-document and the authenticity of the signer. In an e-mail marked as a digital signature file with a key partner. Once accepted and downloaded the attachment file verifier, it can be a process of verification. The verification process is carried out on each of the signature and signer's public key.

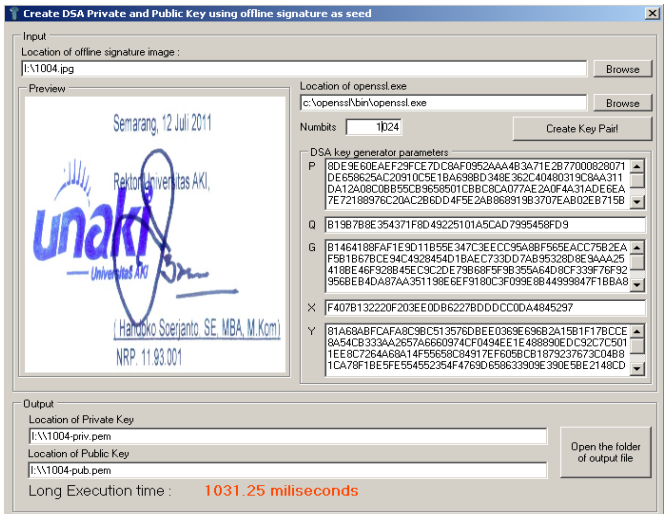

Figure 10 Example Preparation Of Key By The Signer 1

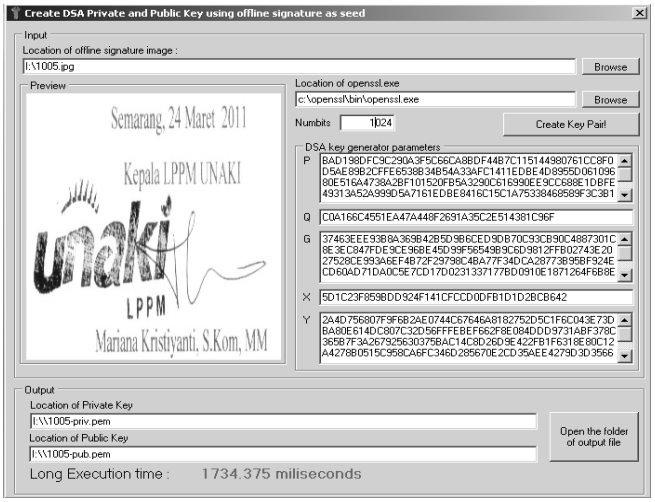

Figure 11 Example Preparation Of Key By The Signer 2

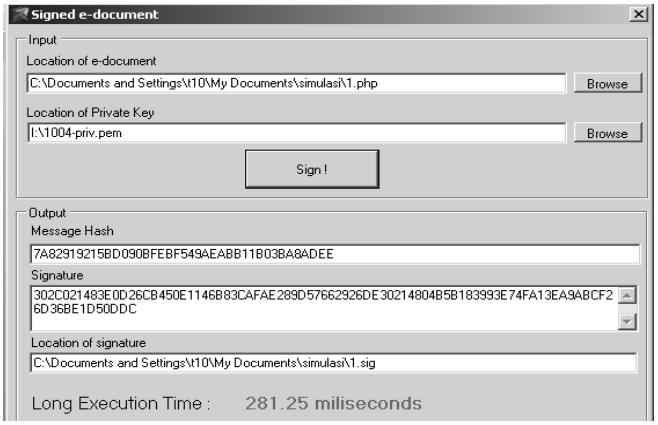

FIGURE 12 EXAMPLE PREPARATION OF DIGITAL SIGNATURE BY THE SIGNER 1

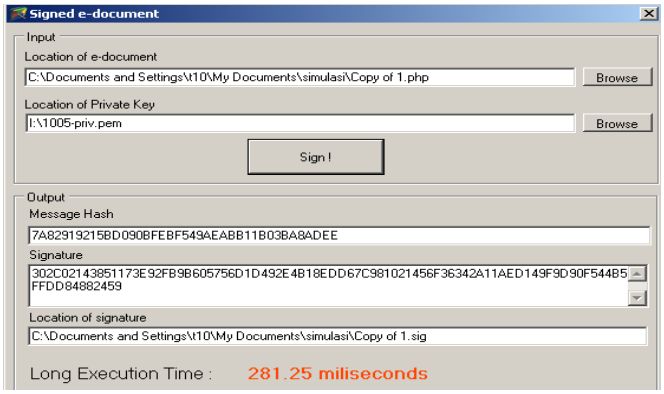

Figure 13 Example Preparation Of Digital Signature By The Signer 2

D. Long Time Execution

On the hardware specifications of the Pentium (R) Dual Core CPU 2:00 GHz T4200@2.00 GHz, 1.87 GB of RAM, get a long execution time that has been tested on key manufacturing processes with a minimum time of 687.5 milliseconds, maximum 3031.25 milliseconds and average 1317.729 milliseconds. While the long execution time on the process of making digital signatures 218.75 milliseconds minimum, maximum 296.875 milliseconds and an average of 265.625 milliseconds. While the long execution time on the verification process with a minimum time of 203.125 milliseconds, 671.875 milliseconds and the maximum average of 261.719 milliseconds. Execution time of a maximum of three processes 3031.25 milliseconds, the minimum time of 218.75 milliseconds and an average of 615.024 milliseconds or 1.025 minutes. So the user just waiting to get the process of key generation, signature and verification for an average of 1.025 minutes.

V. CONCLUSION

Biometric signatures offline user manual can be used to create a private key. The resulting private key, public key is used to make partner. Key length between 512 to 1024 bits according to security standards issued by the FIPS (Federal Information Processing Standard). From one input online signature can generate more than one pair of keys. This shows a dynamic key generation as a new concept on the use of keys for one-time use.

Digital signatures can satisfy the needs non-singular signer. This is a new concept in the application of digital signatures that meet the authorization requirements of e-documents with more than one signer.

The security Biometric signatures and DSA implementation in this study are based on an e-document if signed by the signer will be verified n times. If all valid n-value verification means have been through n layers of security in terms of verification. Conversely, if one or more of the verification result is not valid then the verifier can find out if an e-document received is not authentic or one or more of the signer is not the person who actually signed the e-document. In addition to the security key is generated on the difficulty of factoring large prime numbers look particularly at 1024 bits and 1024 bits are available on the number of primes of about 10^{305}.

E-dokumen transmission security with hybrid methods: biometric signatures and DSA are :

- Secrecy (confidentiality) signature by the verifier can only decrypt with public key private key pairs on the signer.
- The integrity or the authenticity (integrity) of the transmitted e-documents, secured with SHA-1 hash of an e-document.
- Assurance of the identity and validity (authenticity) n with n signer generated the signature and verification results, where n = 1,2,3,....

REFERENCES

[1] FIPS PUB 186-3. 2009. Digital Signature Standard (DSS). http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf. Date accessed 3 Mei 2011

[2] FIPS PUB 183-3. 2008. Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf. Date accessed 3 Mei 2011

[3] Kurniawan, Y. 2004. Kriptografi Keamanan Internet dan Jaringan Telekomunikasi, Informatika, Bandung.

[4] Munir, R. 2006. Kriptografi. Informatika, Bandung.

[5] Najmul, A.K.M. 2006. Handwritten Signature Verification Using P-Tree, Asian journal of information Technologi 5 (3)

[6] Pawan, K.J.;& Siyal, M. Y. 2001. Novel biometric digital signature for internet based applications. Information Management & Computer Security, Emerald journal 9 (5).