

Implementation of Digital Signature In Company's Reports

(paper subtitle)

Byan Sakura Kireyna Aji - 13518066
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): byansakuraka@gmail.com

Abstract — In this paperless era, the integrity of a message or a data is particularly crucial. In wide network area such as the Internet, messages must move from a node to another before it can arrive at the intended destination. There is always a risk of messages getting altered by third parties. Not only that, but it is also important to authenticate the data so that we know the information hasn't been altered. What's more to add, there could be data exchanges where the receiver would not want the senders to disown the sent transmission from the past. In order to solve these concern, digital signature can help to maintain the integrity, authentication, and non-repudiation of the data. *(Abstract)*

Keywords — Digital Signature, RSA, SHA256, data manipulation, company report

I. INTRODUCTION

As social beings, humans always need to communicate in some ways. Messages are some examples in how people communicate with each other. In the past, people use paper and pen to send messages to each other. However, the rapid improvement of technology over the years have changed the way people communicate. In the past, people can only send text to each other. Nowadays, people can send text, voice notes, images, data, tables, and so on.

The onset of the Covid-19 pandemic has increased and diversified messaging dramatically. This phenomenon was caused by the fact that people can't really see each other anymore, so everything must be done online. The pandemic has caused schools, companies, and other institutions to switch the way things were done. Some of the thing that must change because of this is reporting in companies.

Most reports need signatures to show the credentials and credibility of its content, especially the professional ones that are used in big companies.

Usually, these reports are printed then manually signed by the persons in authority to show that it has the correct and approved information. However, companies have shifted from papers and pen to digital report for better documentation and less human contact.

Undoubtedly, this move is a big step toward digitalization which is a good thing. However, when it comes to wide area such as internet, there are a lot of risks that may occur in the way these reports go. The companies need to make sure that there is something that may provide the evidence of origin, identity, and status of the electronic document.

With those concerns in mind, this essay is going to discuss about the cryptography implementation of RSA public key and hash function SHA3 as a method to validate the authenticity and integrity of the digital document by using digital signature. Digital signature is the digital equivalent of a handwritten signature or a stamped seal that offers more inherent security. It is intended to solve the problem of tampering and impersonation in digital communication.

II. THEORY

A. Digital Signature

A digital signature is a mathematical algorithm routinely used to validate the authenticity and integrity of a message [1]. Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents. In emails, the email content itself becomes part of the digital signature.

Digital signatures are significantly more secure than other forms of electronic signatures.

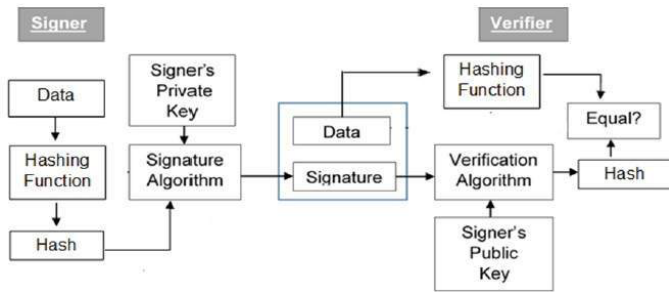


Figure II.1 Signing method using public-key cryptography

The following points explain the entire process in detail:

- Each person in this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. The signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- With the purpose of verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by private key of signer and no one else can have this key. This means the signer cannot repudiate signing the data in future.

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security. Digital signature has the ability to prove non-repudiation of message, message authentication, and data integrity.

Digital signature can prove the non-repudiation of the data since it is assumed that only the signer has the knowledge of the signature key, the signer can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

In message authentication, when the verifier validates the digital signature using public key of a sender, the verifier is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

To prove data integrity, in case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

B. RSA Algorithm

RSA Algorithm is found by three scientists from MIT in 1978 and named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman [2]. This algorithm is an asymmetric cryptography algorithm. This means that it uses a public key and a private key which are two different mathematically linked keys.

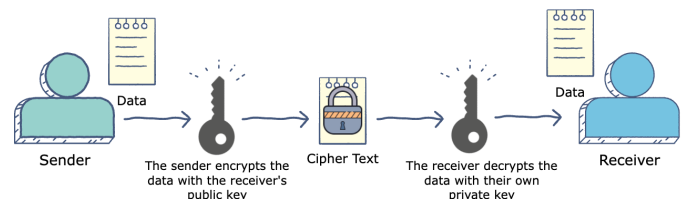


Figure II.2 The illustration how asymmetric cryptography works

The RSA algorithm is considered safe because of the difficulties in factorizing big integers to prime factors. The key generation of this algorithm is described in the following steps:

1. Select two large prime numbers, x and y . The prime numbers need to be large so that they will be difficult for someone to figure out.
2. Calculate $n = x \times y$.
3. Calculate the **totient** function;

$$\phi(n) = (x - 1)(y - 1) \quad (1)$$

4. Select an integer e , such that e is **co-prime** to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n, e) makes up the public key.
5. Calculate d such that $e \cdot d = 1 \pmod{\phi(n)}$

This algorithm also has encryption and decryption functions that is showed by the function (2) and function (3) below.

$$\text{Encryption: } E_e(m) = c = m^e \pmod n \quad (2)$$

$$\text{Decryption: } D_d(c) = m = c^d \pmod n \quad (3)$$

C. Hash Function SHA3

SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015[3]. This algorithm is a subset of a boarder cryptographic primitive family Keccak designed by Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Ban Assche.

SHA-3 uses the sponge construction, in which data is absorbed into the sponge, then the result is squeezed out. In the absorbing phase, message blocks are XORed into a subset of the state, which is then transformed using a permutation function f . In the squeeze phase, output blocks are read from the same subset of the state, alternated with the state transformation function f . The size of the part of the state that is written and read is called the rate, and the size of the part that is untouched by input/output is called the capacity. The capacity determines the

security of the scheme. The maximum-security level is half the capacity.

Generally, SHA3 Algorithm works as follow:

- Enter the input N using the pad function, yielding a padded bit string P with a length divisible by rate
- Break P into n consecutive r -bit pieces P_0, \dots, P_{n-1}
- Initialize the state S to a string of b zero bits
- Absorb the input into the state: for each block P_i :
 - Extend P_i at the end by a string of *capacity* zero bits, yielding one of length *block*
 - XOR that with state S
 - Apply the block permutation f to the result, yielding a new state S
- Initialize Z to be the empty string
- While the length of Z is less than d :
 - Append the first *rate* bits of S to Z
 - If Z is still less than d bits long, apply f to S , yielding a new state S
- Truncate Z to d bits

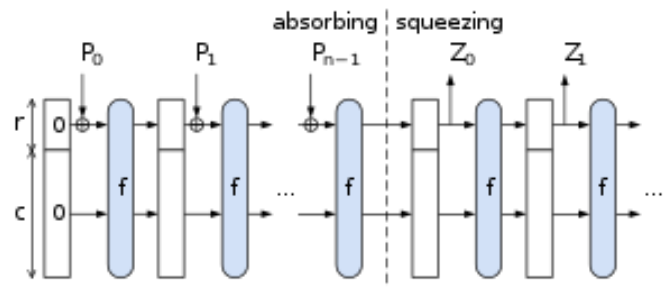


Figure II.3 The sponge construction for hash function

III. SOLUTION DESIGN AND IMPLEMENTATION

In order to solve this problem, there are several steps that can be done. Those steps are General Description, Solution Design, and Solution Implementation.

A. General Description

In order to solve the authentication problem in company's report, this essay is going to use the implementation of digital signature using the combination of hash function and public key cryptography. The use of digital signature may authenticate, prove data integrity, and provide non-repudiation of the content of the report

Hash function that is going to be used to solve this problem is SHA 3 with the consideration that SHA 3 is the standard of the hash functions. The length of the message to digest is going to be 256-bit after taking the speed of generation into account.

The public key algorithm that is going to be used is RSA public key with the consideration of its safety and popularity. The length of the key that is going to be used is 256-byte with the consideration of its safety and speed of the process.

B. Solution Design

The designated solution is consisting of two users, which is BoD and administrator. The architecture for this solution may be seen in the figure III.1.

The design of this solution for BoD starts with BoD sending request to authorize a document. The request that is sent by the BoD will be processed first before it is received by the administrator.

Later on, after the BoD authorized the document, the administrator will check if the signature is valid before publishing the report to the company.

The design of the solution

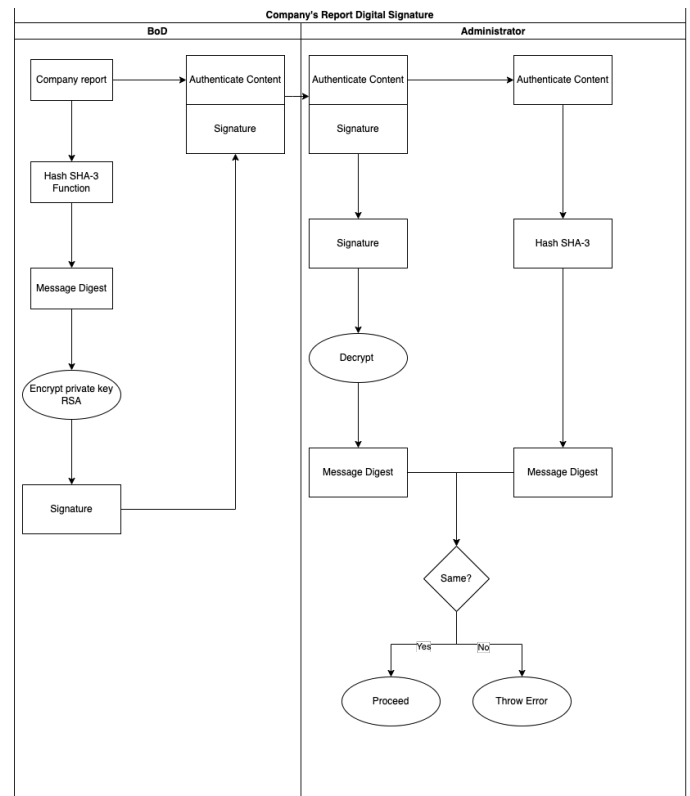


Figure III.1 Solution Architecture

C. Solution Implementation

This solution is implemented as representational state transfer application programming interface (REST API) to facilitate the authentication of a document. The part that needs to authenticate a document needs to generate a pair of public and private key first before sending authentication request. After that, public key is raised to create signature that will be attached to the report to validate the document.

There were several *endpoint* in API that will be generated, which is the key generation, signature generation, and payment.

1. Key generation

Endpoint to generate key that will receive HTTP request with POST method and document number request.

Document ID (JSON)

```
{
  "id_doc": 111
}
```

Response (JSON)

```
{
  "private_key":
    "-----BEGIN RSA PRIVATE KEY-----
    ---
    MIICXQIBAAKBgQC5CtX9aPJ60T50a
    OL6q8f/bAlbf03yc12FPhP62PxoSx/Y
    3ns0
    27d1K3aci++mcuQX/A4EcDlu1Db1j
    SYVX3kiD4651CoTSrY2VlE38DNDsWjn
    +dS4
    MrFpm0HWGCE+qKCW8i6Gpb09K+Hfq
    wixZ95sMF6ZEYdSplIGa45BYXiTdQID
    AQAB
    AoGAOnRY2z+u8btpl157pQbju2zG
    wthNUkKbxAIQcMQIWYx/lFx/GW4U7RS
    0Ovf
    3eYHdigyyWYmToONhQ58zF2npvFRI
    BxLGj/QFcR0jsNzsQQU+aSXQyoLDD+h
    fPlF
    8HlH+6njI2jFmPfvxu0HiBolsGAT6
    ItOakdPwVHase/0wcECQQDuB4mzB/hi
    4eqi
    rkKUN8hLuiirihN6SYL1IhNG+GHLh
    1c0v07SmGgIgwP/LfQwC/zhXqXEL9Gc
    Ioe5
    Yms2nGURAKAxwMzeaqi/Mw14CXX0
    X9A/NXFTvKw5o6TghtmouCNotb71L7f
    PZck
    VizoxdWnxKQrZq0Me0Rqxe7woQ6x/
    Z54JQJBANXyHIi4zz9BxH44l0tV4Egj
    Lr8Q
    wEzBK15fJGiT9ILVwUJ9+cE8j7Wm4
    xZxHZzaCZAgXGq8eHEYcFnm5msNo6EC
    QQDF
    QFH77HohqdEwKrIPr15+e29wQcu+q
    WBhG8GN/J3F4em3QvxHrB6GX3rT42Gm
    0MVH
    tSdfal+fsaWFLOiUJUaVAkBDUY/r8
    8MHwnkcJfwqozNBaWvsHCQQNCEgdDj
    qVLW
```

```
IRVGt/koUMb2X+ONUPVQ1P3i12ap+
kS1EtBr4hE2svt6
-----END RSA PRIVATE KEY-----"
"public_key":
  "-----BEGIN PUBLIC KEY-----
  MIGfMA0GCSqGSIb3DQEBAQUAA4GNA
  DCBiQKBgQC5CtX9aPJ60T50aOL6q8f/
  bAlb
  f03yc12FPhP62PxoSx/Y3ns027d1K
  3aci++mcuQX/A4EcDlu1Db1jSYVX3ki
  D465
  1CoTSrY2VlE38DNDsWjn+dS4MrFpm
  0HWGCE+qKCW8i6Gpb09K+HfqwixZ95s
  MF6Z
  EYdSplIGa45BYXiTdQIDAQAB
  -----END PUBLIC KEY-----"
```

2. Signature Generation

Endpoint to generate signature by accepting HTTP request using POST method

Request (JSON)

```
{
  "id_doc": 111
}
```

Response (JSON)

```
{
  "signature":
    "12e96bab82254324631451
    9b5c7bwjhdwgdqh9828973u332800"
}
```

3. Authentication

Endpoint to authenticate if the document is valid

Request (JSON)

```
{
```

```

    "id_doc": 111
    "encrypted_signature" :
    "Mjwhduywgue932ujkQJQHUSqisho
    ihqs8
    gwidiumgjwnswioedy8newydhJjijimg
    sqhguiihJUGYGm NGYUGDY hjoij"
  }

```

Success Response

```

{
  "id_doc": 111
  "status" : "approved"
}

```

Failure Response

```

{
  "id_doc": 111
  "status" : "failed"
}

```

IV. TESTING AND DISCUSSION

A. Testing

There were two experiments that were done to test the validity of the document using valid signature and invalid signature

The experiment is showed in the table below:

id_doc	1
public_key	<p>-----BEGIN PUBLIC KEY-----</p> <p>MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy poKMkdxNFQSNt2YPD70r8J4Uj 7NDZWni+RJ1 VIA16r65DGfwgZ 6OWd2/XN4Yt1ypBIEWHn+Hvg fygEzC+KumwtCmWnanJhQXNS 4X6eZVKG/n0taivA6Yt82VjGKO QT3zQpjB5IjS3iPCOkoMruGD29l TjVwAXWNYXUZEjo5ycxUIFpq MXuj2iOwBmkELIOMSqipRLft/ R8hKMC6GWzCHV8+HvD7pA</p>

	<p>MJIYb+qfKt4vO5Buf8NjWIFDPej prahERhf2edoGfzYaRIYBACbHt X9d2+JFMrbNTbyMjEnz+t163pP PF2Jds/4tfGLEZt1XRSc/iRCcAfN rk6Es8LqIFDDQIDAQAB</p> <p>-----END PUBLIC KEY-----</p>
private_key	<p>-----BEGIN PRIVATE KEY-----</p> <p>MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBCkgwggSkAgEAA oIBAQDKmgoyR3E0VBI23Zg8P vSvwnhSPs0NlaeL5EnVUGDXqvr kMZ/CBno5Z3b9c3hi3XKkEgRY ef4e+B/KATML4q6bC0KZadqcm FBc1Lhfp5IUob+fS1qK8Dpi3zZ WMYo5BPfNCmMHkiNLeI8I6Sg yu4YPb2VONXABdY1hdRkSOjn JzFSUWmoxe6PaI7AGaQQsg4xK qOIEsW39HyEowLoZbMldXz4e8 PukAwmVhv6p8q3i87kG5/w2Na UUM96OmtqERGF/Z52gZ/NhpG VgEAJse1f13b4kUyts1NvIyMSfP 63Xrek88XY12z/i18YsRm3VdGw L+JEJwB82uToSzwuogUMNAGM BAAECggEAQU5X/Q8EUY7L9 D2HpdvROZpg+Hnf1QIpaLFkj0u Ik/w8NTQ9v+ggm8JbG6WN56hk HLjmB7MDE+59KLssPieKitWd WSBC5HIAZjv3VnYKuboNr4Y1 oFWBLH+w3yXG3UxZqBEyDK 2xjNFGoeOuHnRN6UnKCOS2vv GqagC53SNBn2cXVVNyDlbq+A nUzt2IXuH9Z9guqbok+9BKenMj 2aD/4V21SIYAEkm/UOOQ1vDlh uv6WrRljTUMXXddmhv7BCEff QvfgDvBXiOmbomLySgEAvqs6F H9G2pCsFX5vDhJDFwlfZRgaO1 nIqdAtQ216M8ahNR7UHetX5I17k uIoTC6TQKBgQD67npSJoJSBIP UoZgnJe+LxINbbpmT+scBWSpkI RPyLPgYKarMve3u4GlbTVmmq oKSp18fP/UdOQ+ohp49LAjzNGH zglwgn2zQzi6T8L9SJ/RBvNGbgz osm3BexrwiPBc4P0FSgp7l6oaZy UGPteFNW89pjwOQeZF0ITqUI7 ZgYwKBgQDOsag2K/K/buyE/m Mznkugt+jb9uAowTFUdMPP9M YZ9zG15jUgtGZA6K5GGtvkPK1 jCIKO+RrPvF03BObTBw/SUNi/T 6GfeaDF1CHAd7B4y50FRNIRac/</p>

	VhkL73ISVYSO23ybEC2IQHsBz pqviFJuAdbCTMBmLJhsjV3yCg2 5RzwKBgBNT+yglv1EB+AWQz N93FJR3doa8Zif30QxRiepcgeTN ge6ahwVuO72Cm5rkwlsMFzKkjf 8iNgciNgqNE/MySR4ykrjm+aGp pgAPYZcTnCj/2tiVaq/H09tLvcQP Gr6oUkGK3cU1OngLMIL39YzU PZ5vy/IdifC+7G1GcVSny4xxAoG BALG7bmt2ivw1w8fwfxkJyvpeai uLM+GXjnWTGjWdwyLcvrAtTg 3bUfoKmqDJw7+UtXts++c5KObs kDMZUeqwLdipkFehf9cD3U1/Ra 6cvPCCFXIMZJpvJDnlg2/VFGK G7xD2/fyh1ScLam2IKIDza2ugx7 8pIy3WDIvtVLFdluVdAoGBAO8 dZ6OXLc+LS7VL6Ju10WWFxa DTkzMaE+Az14cONPWkQkq2zJ R3PP2q+xmzqKd0SmbwTSarO+ h28BJjooBU/ZsZ5dawPWmtQwJ6 c6dL1cl+V15z/SEi9PF8/KzK5diK oJbjWdz58/igZh0qVPp6sg2i+AuP 7dAG0V0xpexgoiB -----END PRIVATE KEY-----
Valid signature	s+y1jM+hylp2pVzUaNemlpMDdf GxLliay89OpBgP9nzXkfvMyOJw JJRSqPAu2L3xNA4BO09iWZSn8 CYlgiRNxsIqzjUtCVkAya3qFON UGAPSh/yvDS2aWuyjjL2UZY8A gCmz1P2gMhQdqnm+LBEHPv7r 4Y+OLQqouL/mhPvCtk7VMkC/R jy9QcErHQi+UOZFR12HpuQB2l6 lTnEBIVacdXCZQNDP838eJvsd3 y6tfUZkPV91mKtB3v4SMIZKUz N3o+KKNzTxFWQLRgy38Q/ZY hr0HmbaGHcKLgK2L8v9IZM3j+ K3nHPxgiiUYE11cSutz7r9YVn/u 2JDPt08e/+Hmw==
Invalid Signature	s+y1jM+hylp2pVzUaNemlpMDdf GxLliay89OpBgP9nzXkfvMyOJw JJRSqPAu2L3xNA4BO09iWZSn8 CYlgiRNxsIqzjUtCVkAya3qFON UGAPSh/yvDS2aWuyjjL2UZY8A gCmz1P2gMhQdqnm+kaijsduwhd 7r4Y+OLQqouL/mhPvCtk7VMkC /Rjy9QcErHQi+UOZFR12HpuQB 2l6lTnEBIVacdXCZQNDP838eJvs d3y6tfUZkPV91mKtB3v4SMIZK UzN3o+KKNzTxFWQLRgy38Q/

ZYhr0HmbaGHcKLgK2L8v9IZM 3j+K3nHPxgiiUYE11cSutz7r9YV n/u2JDPt08e/+Hmw==

1. Valid Signature

In this experiment, a request to approve a document is sent using valid signature

Request

{ "doc_id": 111 "encrypted_signature": "qr0KFJW718C+s+s+w+C18htkL6WxdrW Pa8YYHZjMVffJ3YaW/5HcI4HbpM1Z1b mhuqYFn+PQXkqg0cOEIj8zCbSRbTEIZ WqAXFEI2D4gvTfhMerfxkfa77Yh9UEQ 8ub9AKAxYe6JfR0pLRw99N7nBjWbd36 ZVfQnxbddkyDKWf6tFnuZMDz8iEmRLZ S2eXDXKqyBo2yW0ySHGCzrpvS6T5Wd7 hDMtTocDQtz/LQH2PJKU8VepWir6SuZ dEcL5uGktDxRu1NyS8SBQbrYGTeeTE EYcW8N5r4CwzGwohVDui5dQMtcieUwQ aDTz+jHQ/3BCBwcBJk9s4KdJgy2D3NB kA=="
--

Response

{ "doc_id": 111 "status": "approved"
--

2. Invalid Signature

In this experiment, a request to approve a document is sent using invalid signature

Request

{ "doc_id": 212

```
“encrypted_signature”:  
“R0VyUq9juNILv3wwzEW0BuPm3cjrEZ  
zYK6zMxOp27hB/Vkw2sMGM3Mv0X8usa  
9nd0Ioi901r3B77sGX231QngB10sZPf  
I6A0/7hwEFzYkcyFHxxPwNX2skL8J0z  
BncMSMT0jRNIk/l17orhNuazvuFNcS6  
VKpODUKj2Kym8sdiHy3ENwOHLwbETKB  
uSKMySrqryU3MKUxSNemhkchWnb0YZb  
So0w2amTu60zRezfd3WvvjM53A02Ffd  
dELTA9kCIhDKX7eiSMza7pM6FJ+AMGc  
GIO8aM9FEWEHpql1uvTTrny9VCG+3re  
PAPQJ9MezdJbpMNo9/xmqi9HsjtMbbz  
Zw==”  
}
```

Response

```
{  
  “id_doc”: 212  
  “status” : “failed”  
}
```

mengucapkan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T. yang telah memberikan kesempatan dan wawasan mengenai ilmu kriptografi dengan jelas sehingga penulis dapat menyelesaikan penulisan karya tulis ini.


REFERENCES

- [1] R. Munir, "Tanda Tangan Digital," Teknik Informatika STEI - ITB, Bandung.
- [2] Smart, Nigel (February 19, 2008). "Dr Clifford Cocks CB". Bristol University. Retrieved August 14, 2011.
- [3] NIST (August 2015). "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions" (PDF). doi:10.6028/NIST.FIPS.202. Retrieved February 29, 2020.

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, 20 December 2021



Byan Sakura Kirayna Aji - 13518066

ACKNOWLEDGMENT (*Heading 5*)

Penulis ingin mengucapkan puji syukur kepada Tuhan Yang Maha Esa, karena telah diberikan kemudahan dalam menyelesaikan karya tulis ini. Selain itu, penulis juga ingin