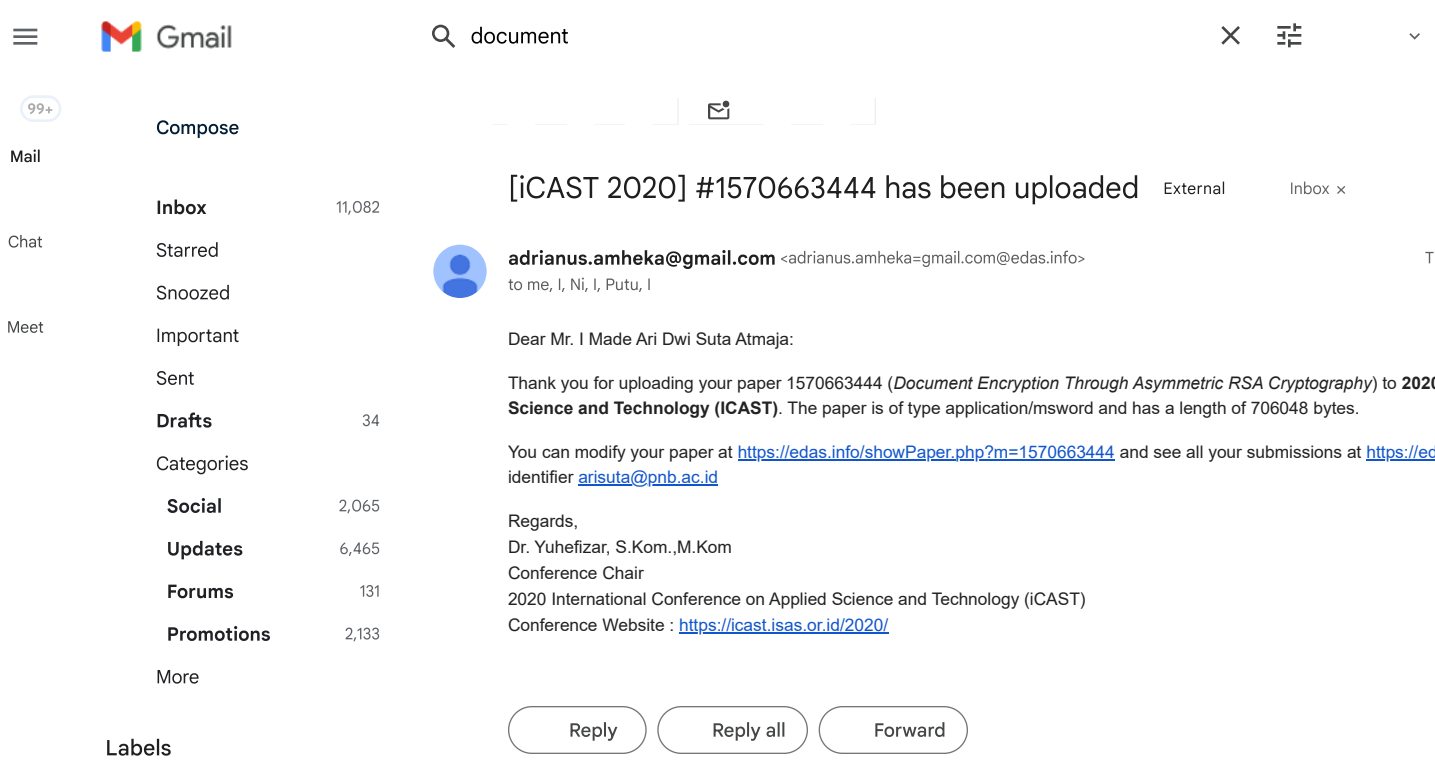

Gmail
document
99+
Mail
Chat
Meet
Compose
Inbox 11,082
Starred
Snoozed
Important
Sent
Drafts 34
Categories
Social 2,065
Updates 6,465
Forums 131
Promotions 2,133
More
Labels
[iCAST 2020] #1570663444 has been uploaded
External
Inbox ×
adrianus.amheka@gmail.com <adrianus.amheka=gmail.com@edas.info>
Thu,
to me, I, Ni, I, Putu, I
Dear Mr. I Made Ari Dwi Suta Atmaja:
Thank you for uploading your paper 1570663444 (Document Encryption Through Asymmetric RSA Cryptography) to 2020 In
Science and Technology (ICAST). The paper is of type application/msword and has a length of 706048 bytes.
You can modify your paper at https://edas.info/showPaper.php?m=1570663444 and see all your submissions at https://edas.
identifier arisuta@pnb.ac.id
Regards,
Dr. Yuhefizar, S.Kom.,M.Kom
Conference Chair
2020 International Conference on Applied Science and Technology (iCAST)
Conference Website : https://icast.isas.or.id/2020/
Reply
Reply all
Forward

[iCAST 2020] Congratulation Your paper #1570663444 ('Document Encryption Through Asymmetric RSA Cryptography') - Conditional Accepted External Inbox

yuhefizar=pn...@edas.info Mon, Sep 7, 2020, 10:45 PM

to me, I, Ni, I, Putu, I, Adrianus, Firdaus, Udin, Hendrick, Dedi, Aliv, Anritsu, Tineke, Anang, Yuhefizar, Yulindon

Dear Mr. I Made Ari Dwi Suta Atmaja:

Congratulations - We are pleased to inform you that your manuscript #1570663444 ('Document Encryption Through Asymmetric RSA Cryptography') has now been CONDITIONAL ACCEPTED by 2020 International Conference on Applied Science and Technology (ICAST).

The evaluation of your paper and all comments from reviewers of your paper are enclosed with this message.

The reviews are below or can be found at https://edas.info/showPaper.php?m=1570663444 using your EDAS login name arisuta@pnb.ac.id.
Please follow the accepted procedures here https://icast.isas.or.id/2020/

Now we would like your cooperation with the double-check of your paper.
(1) Please ensure that manuscript is fully in English.
(2) For the copyright: Please ensure you process the copyright. The IEEE e-copyright submission can be done in EDAS electronically at 'Copyright form'.
(3) For the final paper version: Please Strictly use and follow the IEEE template (Word Format): https://www.ieee.org/conferences/publishing/templates.html
(4) Proofread your final manuscript to confirm that it will require no revision.
(5) Please ensure that number of pages of your final paper is 4-8 pages.
(6) All the manuscripts have to convert into PDF files which offered by IEEE PDF eXpress. You can use the link: http://www.pdf-express.org/. You will need the Conference ID to log in, which is: 50839X. After file conversion (become PDF file) offered by IEEE PDF eXpress successfully. You can upload PDF file paper final version in EDAS at 'Final manuscript.
(7) Please take notice that the revision of the manuscript should be submitted by September 14, 2020.
(8) Please take notice that the Final Paper should be submitted by September 28, 2020.
(9) Most importantly, please ensure the similarity score is less than 25%. You can refer to EDAS to see the similarity score of your manuscript. According to IEEE regulations, any manuscript with a similarity score of more than 25% will be dropped and should be reported to IEEE. Please make sure your final manuscript follows this rule.
If the similarity score of the final manuscript is more than 25%, the manuscript will be dropped or cancelled to be presented at iCAST 2020.
(10) IEEE reserves the right to exclude a paper from distribution after the conference (e.g. removal from IEEE Xplore) if the manuscript is not presented at the conference.

We, iCAST 2020 organizer, are now planning the detailed program and will inform you in coming weeks the information related to iCAST 2020

We are looking forward to seeing you in Padang-Indonesia via online conference, on October 24-25, 2020.

Sincerely Yours,

Regards,
Dr. Yuhefizar, S.Kom.,M.Kom
Conference Chair
2020 International Conference on Applied Science and Technology (iCAST)
Conference Website : https://icast.isas.or.id/2020/

Reviews/Comments:
======= Review 1 =======

> *** Originality: Uniqueness and originality in the presented paper
Good (4)

> *** Literature: Adequacy of references to literature
Good (4)

> *** Technical Discussion: Technical Discussion
Good (4)

> *** Contribution: Potential impact and contribution
Good (4)

> *** Comment to Author: e.g. Major reasons of your overall recommendation

The topic of this paper is good enough to present in our conference, but we suggest improving the use of a better English structure. the author also has to change the existing graphics in fig 2 into English.
The conclusion also needs some improvement.

======= Review 2 =======

> *** Originality: Uniqueness and originality in the presented paper
Average (3)

> *** Literature: Adequacy of references to literature
Average (3)

> *** Technical Discussion: Technical Discussion
Average (3)

> *** Contribution: Potential impact and contribution
Average (3)

> *** Comment to Author: e.g. Major reasons of your overall recommendation

this paper is appropriate to be accepted, however, the abstract does not explain the results obtained.

Gmail

document

99+
Mail

Chat

Meet

Compose

Inbox 11,075
Starred
Snoozed
Important
Sent
Drafts 33
Categories
Social 2,065
Updates 6,460
Forums 131
Promotions 2,132
More

Labels

I Made Ari Dwi Suta Atmaja <arisuta@pnb.ac.id> Sat, M
to Icast

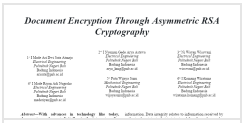
Dear Mr. Dr. Yuhefizar,

I'm sent my revised paper through this email with format .doc and .docx.

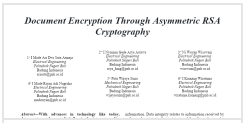
Best regards

I Made Ari Dwi Suta Atmaja
Presenter-ID Paper 1570663444

2 Attachments • Scanned by Gmail



paper icast 2020 ..



paper icast 2020 ..

Icast Conference <icast@pnp.ac.id> Sat, M
to me

Urgently required for manuscript revision of icast2020 conference

External Inbox

Icast Conference <icast@pnp.ac.id>
to arya_kmg, sriandriati, me, leo.radhitya, ayu.harry

Fri, Nov 13, 2020, 1:42 AM

Dear All Authors of iCAST2020 Conference

Thank you for your participation in the Third International Conference on Applied Science and Technology. Before continuing the process of iCAST to a publisher, as a required step from IEEE we need to make sure all of the contents on the written paper were already in English. Regarding this approach, we recommend you to check all of the entire content on your paper as below:

1. Title, author format, keywords, tables, figures and references must arrange following template.
2. The figure or graph is ideally a 300 dpi tiff and ensures all of the content in english.
3. Equation is centered using a center tab stop. Be sure the symbols in your equations have been defined or immediately following the equation. Do not use an image or a screen shoot.
4. Then ensure your manuscript already truly follow the available template.

You can submit your revised paper through this email by using Docx file format and use paper ID as the title of your file. Furthermore, the due date for this revision process is November 14, 2020. Thank you.

Best Regards

Dr. Yuhefizar

Chair of iCAST 2020

https://icast.isas.or.id/2020/

One attachment • Scanned by Gmail

PDF 1570663521(Auth…

IEEE PDF eXpress Site Services: File Received (Paper ID 6610647)

External

50839X Author Services <support@incontrolproductions.net> Mon, S
to me

Dear I Made Ari Atmaja,

PDF eXpress has received your file:

Filename: 2020 -1570663444.doc
Title: Document Encryption Through Asymmetric RSA Cryptography

Paper ID: 6610647
Received: 13 September 2020 19:06 -0800 GMT

If you submitted a PDF: PDF eXpress will compare your PDF to the latest IEEE Xplore requirements. You will receive anothe checked.

If you submitted source file(s): PDF eXpress will convert your source file(s) to PDF in accordance with the latest IEEE Xplore email when your new PDF is available.

Thank you for using PDF eXpress!

For guidance in creating Xplore-compliant PDFs, email mailto:PDFsupport@ieee.org

IEEE PDF eXpress Site Services: New PDF is ready (PaperID 6610647) External Inbox

50839X Author Services <support@incontrolproductions.net> Mon, Sep 14, 2020, 10:07 AM
to me

Dear I Made Ari Atmaja,

Your new PDF is ready for the following title:

Source Filename: 2020 -1570663444.doc
Title: Document Encryption Through Asymmetric RSA Cryptography
Paper ID: 6610647
PDF Filename: 6610647.pdf

A copy of your IEEE Xplore compatible PDF is attached to this email. You can also download it from your PDF eXpress account. The file is labeled within its document properties as being "Certified by IEEE PDF eXpress", with an exact date and time stamp. The certified file attached to this message is the file that you should submit to your conference's final paper collection site.

We recommend you check the PDF carefully. Examine each page on screen and in print to ensure everything looks as you intend.

If you are not satisfied with your PDF, you may go back to your account and submit another source file for conversion, or submit a PDF that you produce for Checking.

If there is any other issue with your PDF, you may go back to your account and Request a Manual Conversion: your submission will be sent to Technical Support for special handling.

For Paper ID: 6610647
PDF Checks: 0 of 10
Source File Conversion: 1 of 20

A Reminder: PDF eXpress is NOT the final collection site.

Thank you for using PDF eXpress!

For guidance in creating Xplore-compliant PDFs mailto:PDFsupport@ieee.org

One attachment • Scanned by Gmail

PID6610647.pdf

IEEE Copyright Transfer Confirmation for Article: Document Encryption Through Asymmetric RSA Cryptography External Inbox

ecopyright@ieee.org Mon, Sep 14, 2020, 10:26 AM

to me, arya_kmg, wisswani, maderiyan, wijayasunu, wiratama.komang

IEEE Electronic Publication Agreement Receipt
==========

Publication Title: 2020 International Conference on Applied Science and Technology (ICAST)
Article Title: Document Encryption Through Asymmetric RSA Cryptography
Author(s): Mr. I Made Ari Dwi Suta Atmaja, Mr. I Nyoman Gede Arya Astawa, Mrs. Ni Wayan Wisswani, Mr. I Made Riyan Adi Nugroho, Dr. Putu Wijaya Sunu and Mr. I Komang Wiratama
Author E-mail: arisuta@pnb.ac.id, arya_kmg@pnb.ac.id, wisswani@pnb.ac.id, maderiyan@pnb.ac.id, wijayasunu@pnb.ac.id, wiratama.komang@pnb.ac.id
eCF Paper Id: 1570663444

Dear Colleague

Congratulations! You have successfully completed the IEEE Electronic Publication Agreement. A copy of the fully executed Agreement is attached here for your records. Please save this e-mail for any future reference.

PLEASE DO NOT RESPOND TO THIS EMAIL.
For technical assistance or to search our knowledge base, please visit our support site at :

http://ieee.custhelp.com/app/answers/list/p/197,2375

One attachment • Scanned by Gmail

CopyrightReceipt…

IEEE COPYRIGHT AND CONSENT FORM

To ensure uniformity of treatment among all contributors, other forms may not be substituted for this form, nor may any wording of the form be changed. This form is intended for original material submitted to the IEEE and must accompany any such material in order to be published by the IEEE. Please read the form carefully and keep a copy for your files.

Document Encryption Through Asymmetric RSA Cryptography
Mr. I Made Ari Dwi Suta Atmaja, Mr. I Nyoman Gede Arya Astawa, Mrs. Ni Wayan Wisswani, Mr. I Made Riyan Adi Nugroho, Dr. Putu Wijaya Sunu and Mr. I Komang Wiratama
2020 International Conference on Applied Science and Technology (ICAST)

COPYRIGHT TRANSFER

The undersigned hereby assigns to The Institute of Electrical and Electronics Engineers, Incorporated (the "IEEE") all rights under copyright that may exist in and to: (a) the Work, including any revised or expanded derivative works submitted to the IEEE by the undersigned based on the Work; and (b) any associated written or multimedia components or other enhancements accompanying the Work.

GENERAL TERMS

1. The undersigned represents that he/she has the power and authority to make and execute this form.
2. The undersigned agrees to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.
3. The undersigned agrees that publication with IEEE is subject to the policies and procedures of the IEEE PSPB Operations Manual.
4. In the event the above work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, the foregoing copyright transfer shall be null and void. In this case, IEEE will retain a copy of the manuscript for internal administrative/record-keeping purposes.
5. For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.
6. The author hereby warrants that the Work and Presentation (collectively, the "Materials") are original and that he/she is the author of the Materials. To the extent the Materials incorporate text passages, figures, data or other material from the works of others, the author has obtained any necessary permissions. Where necessary, the author has obtained all third party permissions and consents to grant the license above and has provided copies of such permissions and consents to IEEE

You have indicated that you DO wish to have video/audio recordings made of your conference presentation under terms and conditions set forth in "Consent and Release."

CONSENT AND RELEASE

1. In the event the author makes a presentation based upon the Work at a conference hosted or sponsored in whole or in part by the IEEE, the author, in consideration for his/her participation in the conference, hereby grants the IEEE the unlimited, worldwide, irrevocable permission to use, distribute, publish, license, exhibit, record, digitize, broadcast, reproduce and archive, in any format or medium, whether now known or hereafter developed: (a) his/her presentation and comments at the conference; (b) any written materials or multimedia files used in connection with his/her presentation; and (c) any recorded interviews of him/her (collectively, the "Presentation"). The permission granted includes the transcription and reproduction of the Presentation for inclusion in products sold or distributed by IEEE and live or recorded broadcast of the Presentation during or after the conference.
2. In connection with the permission granted in Section 1, the author hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work or Presentation, and releases IEEE from any claim based on

right of privacy or publicity.

BY TYPING IN YOUR FULL NAME BELOW AND CLICKING THE SUBMIT BUTTON, YOU CERTIFY THAT SUCH ACTION CONSTITUTES YOUR ELECTRONIC SIGNATURE TO THIS FORM IN ACCORDANCE WITH UNITED STATES LAW, WHICH AUTHORIZES ELECTRONIC SIGNATURE BY AUTHENTICATED REQUEST FROM A USER OVER THE INTERNET AS A VALID SUBSTITUTE FOR A WRITTEN SIGNATURE.

I Made Ari Dwi Suta Atmaja — **Signature**

13-09-2020 — **Date (dd-mm-yyyy)**

Information for Authors

AUTHOR RESPONSIBILITIES

The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

RETAINED RIGHTS/TERMS AND CONDITIONS

- Authors/employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
- Authors/employers may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the author's personal use or for company use, provided that the source and the IEEE copyright notice are indicated, the copies are not used in any way that implies IEEE endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
- Although authors are permitted to re-use all or portions of the Work in other works, this does not include granting third-party requests for reprinting, republishing, or other types of re-use.The IEEE Intellectual Property Rights office must handle all such third-party requests.
- Authors whose work was performed under a grant from a government funding agency are free to fulfill any deposit mandates from that funding agency.

AUTHOR ONLINE USE

- **Personal Servers**. Authors and/or their employers shall have the right to post the accepted version of IEEE-copyrighted articles on their own personal servers or the servers of their institutions or employers without permission from IEEE, provided that the posted version includes a prominently displayed IEEE copyright notice and, when published, a full citation to the original IEEE publication, including a link to the article abstract in IEEE Xplore. Authors shall not post the final, published versions of their papers.
- **Classroom or Internal Training Use.** An author is expressly permitted to post any portion of the accepted version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.
- **Electronic Preprints.** Before submitting an article to an IEEE publication, authors frequently post their manuscripts to their own web site, their employer's site, or to another server that invites constructive comment from colleagues. Upon submission of an article to IEEE, an author is required to transfer copyright in the article to IEEE, and the author must update any

previously posted version of the article with a prominently displayed IEEE copyright notice. Upon publication of an article by the IEEE, the author must replace any previously posted electronic versions of the article with either (1) the full citation to the IEEE work with a Digital Object Identifier (DOI) or link to the article abstract in IEEE Xplore, or (2) the accepted version only (not the IEEE-published version), including the IEEE copyright notice and full citation, with a link to the final, published article in IEEE Xplore.

Questions about the submission of the form or manuscript must be sent to the publication's editor.
Please direct all questions about IEEE copyright policy to:
IEEE Intellectual Property Rights Office, copyrights@ieee.org, +1-732-562-3966

Document Encryption Through Asymmetric RSA Cryptography

1st I Made Ari Dwi Suta Atmaja
Electrical Engineering
Politeknik Negeri Bali
Badung Indonesia
arisuta@pnb.ac.id

2nd I Nyoman Gede Arya Astawa
Electrical Engineering
Politeknik Negeri Bali
Badung Indonesia
arya_kmg@pnb.ac.id

3rd Ni Wayan Wisswani
Electrical Engineering
Politeknik Negeri Bali
Badung Indonesia
wisswani@pnb.ac.id

4th I Made Riyan Adi Nugroho
Electrical Engineering
Politeknik Negeri Bali
Badung Indonesia
maderiyan@pnb.ac.id

5th Putu Wijaya Sunu
Mechanical Engineering
Politeknik Negeri Bali
Badung Indonesia
wijayasunu@pnb.ac.id

6th I Komang Wiratama
Electrical Engineering
Politeknik Negeri Bali
Badung Indonesia
wiratama.komang@pnb.ac.id

2020 International Conference on Applied Science and Technology (iCAST) | 978-1-7281-9567-4/20/$31.00 ©2020 IEEE | DOI: 10.1109/iCAST51016.2020.9557723

***Abstract*—With advances in technology like today, documents can be sent digitally via the internet media. An important problem faced in sending digital documents is that often documents sent can be accessed by parties who do not have the authority over these documents. The solution to this problem is to secure digital documents before transmission. One of the methods to secure data is cryptography. Cryptography with asymmetric keys is the strongest data security technique to use. One of the most widely used asymmetric cryptography is the RSA (Rivest-Shamir-Adleman) algorithm. The type of document that is encrypted is the most commonly attached document when sent e-mails. The document types are .docx, .pptx, .xlsx, .pdf, .jpg and .mp4. In the encryption process, a public key and a private key will be generated which can be sent separately by sending encrypted digital documents. The decryption process for digital documents is carried out from the receiving end of the document using a private key generated in the encryption process. The encryption result has a size larger than the original file size because it has been encoded in another form according to the RSA algorithm. The longer and bigger the input size, the longer it will take required for encryption.**

Keywords--Cryptography, Encryption, Decryption, Document.

I. INTRODUCTION

The advancement of information technology today has provided many benefits in everyday life, both for individuals and organizations. Technological advances are characterized by easy and fast access to information. Each individual can exchange information in seconds even though the distance is quite far. This convenience is of course accompanied by challenges, namely the security of information exchanged. The easier access to information is, the less secure it will be. Information security includes 3 main aspects, namely: confidentiality, data integrity, and availability [1]. Confidentiality is related to the assurance that information can only be accessed by those who have authority over the information. Data integrity relates to information received by authorized recipients that is intact and free from changes by unauthorized parties. Availability, namely the assurance of system services for authorized parties.

The study of data security is cryptography. According to Rodriguez-Henriquez, cryptography is a discipline that studies mathematical techniques related to information security, such as providing security services in the form of confidentiality, data integrity, authentication, and non-repudiation (cannot be denied) [2]. Until now, various cryptographic algorithms has founded to secure data. Cryptographic algorithms have been classified into 2 based on the key, namely the symmetric key algorithm and the asymmetric key. The symmetric key only uses a secret key that is the same between the sender of the message and the recipient of the message. The message is encrypted (encoded) and decrypted (decoded) with a secret key so that both the sender and receiver will share a secret key. In an asymmetric key, the sender and receiver use different keys [3]. If a message is confidential and only has the right to be known by the recipient, then the recipient will give the public key that has been generated from the private key to the sender. The sender then encrypts the information with that public key. When the recipient receives an encrypted message, the recipient will decrypt it using his private key. The use of this asymmetric key is very widely used today because the recipient does not need to give the secret key to other parties so that only the recipient knows the key.

Nowadays, the use of asymmetric keys is becoming more and more common. Various asymmetric key algorithms have been widely known, among which the most widely used is Rivest-Shamir-Adleman (RSA). Various studies on the RSA algorithm have been carried out, including Chandel and Patel conducting a literature review to encrypt image data, and it was found that RSA is good for doing it [4]. Parkin 2003 conducted a study to use RSA as a digital signature in e-commerce transactions [5]. Shen in 2009 carried out an object-based implementation to accelerate the RSA algorithm [6].

In this study, the implementation of RSA was carried out in document form information. This algorithm is implemented to be able to secure data in documents so that they are safe from unauthorized.

II. RESEARCH METHOD

The data in this study were document text files in the .docx, .xlsx, .pdf format, .ppt, .jpg and also .mp4. The document file will be tested with the built application, they will decode with the RSA encryption algorithm. The results of each encryption will be saved into a text file with text

978-1-7281-9567-4/20/$31.00 ©2020 IEEE

format. When the end-user receives the file and will do the decryption, the opposite of the encryption algorithm used previously. For each encrypted text file, the encryption time will be calculated based on the length of the key used and the file size formed after the encryption process.

In the system design process, it is necessary to make the system process flow itself. The document security system application created has an architecture as shown in Figure 1 below:

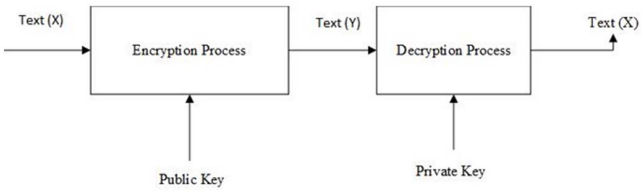


Fig. 1. Asymmetric Key Encryption Application Architecture

In Figure 1, there are 2 users, namely A as the sender and B as the recipient of the message. A has previously been told the private key B. The X text document data which will be referred to as plaintext is input into the system. The system will encrypt X using the RSA algorithm to produce a private key. The encryption result is a ciphertext named Y. B as the recipient will decrypt Y using an existing private key and obtain a text X which has the same content as the plaintext sent by A

For more specific, the process of encryption and decryption of documents is described in the following flowchart:

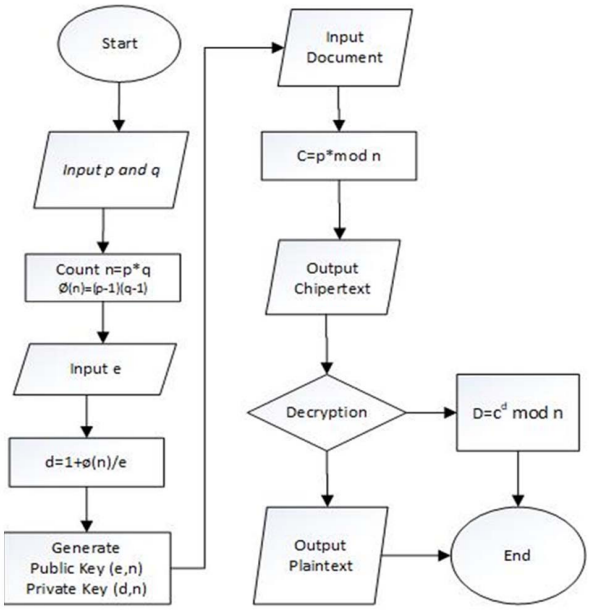


Fig. 2. Flowchart of RSA Asymmetric Key Encryption Application

The process of encryption and decryption of documents following the flow chart in Figure 2 is explained as follows:

1. Key Forming Process:

a. Choose two prime numbers p and q, (try p> q)

b. Calculate n = p x q

c. Calculate Φ (n) = (p-1) x (q-1)

d. Choose a public key that is relatively prime with Φ (n)

e. Calculate the private key with SK = 1 + Φ (n) / PK

2. Encryption Process:

a. Change the plaintext into ASCII code

b. ASCII characters are stored in blocks of bytes.

c. Multiply each block to get the ciphertext with the formula: C = p ^ e mod n

3. Decryption Process:

a. Change the plaintext into ASCII code

b. ASCII characters are stored in blocks of bytes.

c. Multiply each block to get the plaintext with the formula: P = c ^ d mod n

The data used are 6 types of files with different formats and for file size, there are no restrictions.

TABLE I. TYPES OF TEST DOCUMENTS

No	File Type	File Size (KB/MB)	RSA	
			Encryption Time (s)	Decryption Time (s)
1	File 1.docx	Size 1		
2	File 2.pptx	Size 2		
3	File 3.xlsx	Size 3		
4	File 4.pdf	Size 4		
5	File 5.jpg	Size 5		
6	File 6.mp4	Size 6		

Table 1 above shows the file types that will be used for testing. In the testing process, the time spent in the encryption and decryption process will be calculated for each type of document. System testing will be carried out using several types of documents and videos that are most often transmitted through the internet. The file formats such as *.docx, *.pptx, *.xlsx, *.pdf, *.jpg and *.mp4. This decryption encryption application goal that the document has security so it can't be accessed by unauthorized people.

III. RESULT AND DISCUSSION

The results obtained from this study is a document encryption application with the RSA method. This application was built using the programming language used in building this information system is PHP using the Code Igniter Framework where the storage process is carried out directly into the user's computer internal storage. The results of the research are as follows:

A. Result

The results of this application have been implemented and can be accessed online through the page: https://rsacryptography.com. The following is a view of the

document encryption application based on the RSA Asymmetric method, on this page, there are 2 main menus, namely Encryption, and Decryption.

Fig. 3. Main Page of RSA Asymmetric Encryption Application

For menu 1, namely the encryption process, the document to be encrypted is input into the system and then the encryption process will be carried out. After the encryption process is running, the system will generate information from the document that has been encrypted in the form of the original file name, file type, the resulting private and public key, the name of the encryption file, and the time it takes in the encryption process. As seen in Figure 3 below:

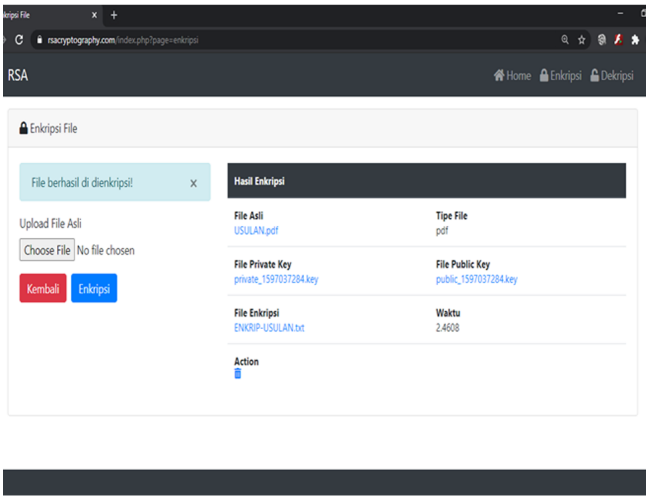


Fig. 4. RSA Asymmetric Key Document Encryption Process

All encrypted files are saved in .txt format. This format is the easiest file format to transmit or send on the internet. After the encryption process is carried out, the document and private key can be downloaded for further use in the decryption process. Encryption files that have been downloaded will be stored directly into the internal storage of the computer used by the user.

The encryption-decryption process produces 2 keys. namely Public Key and Private Key. The Public Key can be known by others. While the private key can only be known by the recipient of the encryption file, where later the private key will be used to decrypt the received document. The private key is generated differently for each encryption process. So each key will not be the same as one another. Private key files can also be downloaded directly and stored in the internal storage of the computer

An example of the results of the private key generated from the encryption process is shown in Figure 5 below :

Fig. 5. Private Key of RSA Asymmetric Encryption Application

Likewise, the generated public key will be different for each time the encryption process is performed. For an example of the results of the public key generated from the encryption process is shown in Figure 6 below :

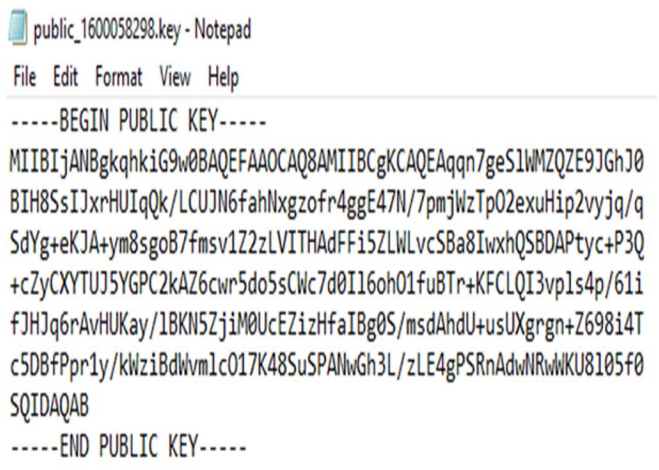


Fig. 6. Private Key of RSA Asymmetric Encryption Application

In the decryption process, the private key plays a very important role so that the document can be successfully decrypted back into the original document. Each file decryption process uses his private key. in other words each document has its private key, so only the corresponding private key can decrypt the document itself. The decryption process is shown in Figure 7 below:

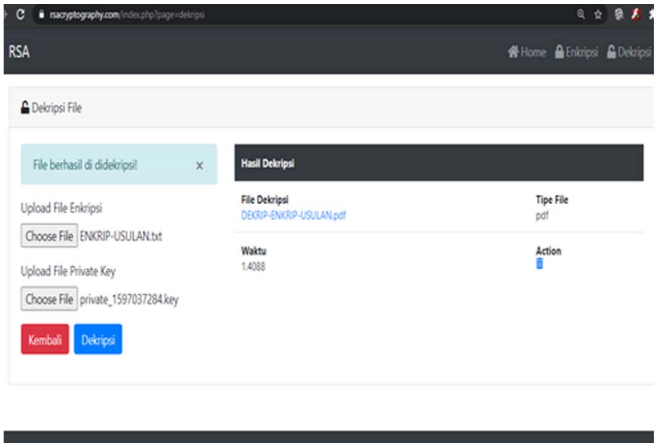


Fig. 7. RSA Asymmetric Key Document Decryption Process

B. Result Evaluation Process

The test carried out is the description test of the 6 types of documents that are most commonly transmitted via internet media. All document types have been successfully encrypted and decrypted. When the encryption file is opened, the original information has been encoded according to the RSA encryption result. The insured message information is shown in Figure 8 below:

Fig. 8. Contents of RSA Encrypted Document Files

All types of documents are tested by obtaining the results as shown in Table II below:

TABLE II. RESULTS OF TESTING ALL TYPES OF DOCUMENTS

No	File Type	File Size (KB)	RSA		Status
			Encryption Time (s)	Decryption Time (s)	
1	Enkripsi.docx	284	0.2808	0.2386	Succeed
2	JSA.pptx	535	0.5034	0.4411	Succeed
3	Rab.xlsx	102	0.1018	0.1131	Succeed
4	Usulan.pdf	1.662	1.5733	1.3877	Succeed
5	Flowchart.jpg	23	0.0274	0.0343	Succeed
6	Video.mp4	1.878	1.7106	1.5132	Succeed

From the testing that has been completed, all types of documents running properly encrypted and decrypted. From the test results, it is also seen that the larger the document size will affect the time in the encryption and decryption process. In this system, there are no restrictions on the size of the documents to be encrypted but in general, in the process of sending documents through the internet, each application has different restrictions. So it is still recommended that the size of the document file to be encrypted can adjust to the application that will be used to transmit the encrypted results. Decryption and encryption with a shorter time is necessary so that the process becomes effective and efficient

IV. CONCLUSION

The conclusion of this research is application software can perform process encryption, decryption, and verification with success, thus providing security that is an aspect of confidentiality and data authentication. In all processes handled by the RSA algorithm, the key size is directly proportional to the processing time/speed. The average Encryption time is faster compared to the decryption time. The encryption result has a size larger than the original file size because it has been encoded in another form according to the RSA algorithm. The longer and bigger the input size, the longer it will take required for encryption.

ACKNOWLEDGMENTS

The authors would like to thank the department of research and community service center of Politeknik Negeri Bali and the Ministry of Research and Technology of Higher Education of the Republic of Indonesia for the financing of this research.

REFERENCES

[1] Stalling, W. 2011. Cryptography and Network Security. Prentice-Hall: New York.

[2] Dwi Liestyowati 2020. Public Key Cryptography. Journal of Physics: Conference Series 1477 052062

[3] Rodriguez-Henriquez, F.; Saqib, N.A; Díaz Pérez, A; Koc, C.K 2007. Cryptography Algorithms on Reconfigurable Hardware. Springer.

[4] Chandel, GS, Patel, P. 2013. A Review: Image Encryption with RSA and RGB Randomized Histograms. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, 4397-4401

[5] Park, JM. 2003. Constructing Fair-exchange Protocols for E-commerce via Distributed Computation of RSA Signatures. Proceedings of the Twenty-second Annual Symposium on Principles of Distributed Computing: New York. 172-181

[6] Shen, G, Liu, B, Zheng, X. 2009. Research on Fast Implementation of RSA with Java. Proceedings of the 2009 International Symposium on Web Information Systems and Applications: Nanchang. 186-189