Digital Rights Management on Video Files using Integration Algorithms AES and RSA Cryptography

Tuah Rus Ariandy
Department of Information System
Universitas Ahmad Dahlan Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan Yogyakarta of Indonesia

ABSTRACT

Advances in technology make it easy to distribute, copy, and share digital content. However, digital content such as video files has disadvantages in terms of secure copying and redistribution, making important video files that are still in the production process accessible by anyone. With the support of technology and the widespread use of the internet, digital content has become widely used, especially in video files. As technology develops, it becomes easier to copy, modify, and access video files. To overcome this problem, digital rights management technology needs to be developed. Digital rights management (DRM) is one of the technologies that can be used to secure and restrict access to video files, one of which is using cryptographic algorithms to encrypt video files. This study proposes that video files are encrypted using the integration of AES and RSA algorithms. The AES algorithm is used in the system to encrypt video files, and the RSA 4096-bit algorithm is used to wrap the AES 256-bit secret key. These two cryptographic algorithms are integrated into one system to encrypt video files. In this study, the DRM application developed was successfully implemented in UAD TV studios using the integration of AES and RSA cryptographic algorithms so that mp4 video files produced have access control by encrypting video files using public keys and decrypting them using private keys.

Keywords

Digital Rights Management, DRM, Cryptography, AES, RSA, Video File

1. INTRODUCTION

Advances in information technology make it easy to share, sell, and distribute digital content [1]. However, digital content has disadvantages when it comes to secure copying and redistribution, leading to rampant piracy [2]. Among all digital content, video files have attracted many researchers because of their high capacity to store important and sensitive data or information [3]. Video files are data formats that are often used in information technology to provide information to technology users because they are easily accessible using different devices anywhere, so it is necessary to have security techniques for these video files [4]. The growth of video technology and services, the total amount of video content, as well as the types of content available, have increased and diversified as technology has evolved [5]. Due to the increasing use of video, the need for video security and privacy protection has become more important. Therefore, various video encryption algorithms have been implemented to protect video content from unauthorized users [6]. With the advancement of technology and the widespread use of the internet, data has become digital. It is becoming easier and easier to copy, modify, and transform digital data into other forms. The term "digital rights management" (DRM) has been suggested to limit the use of data in digital content and to protect copyright [7].

Digital rights management systems (DRM) are techniques that make digital content accessible only to legitimate rights holders [8]. Digital rights management (DRM) is a solution to achieve the necessary security in digital content distribution systems. Under DRM protection, digital content is usually encrypted before being distributed [9]. Since the transmission of digital content over the internet is easy and fast, and the dissemination of digital content is very high, digital rights management systems are designed to limit access to the utilization, turnover, and distribution of retained digital content [10]. Digital rights management systems aim to ensure the authorized use of content [11]. When digital content is distributed over public networks, secure content access mechanisms are required. Digital rights management (DRM) systems were developed to address digital content piracy. Digital rights management systems focus on controlling the use and distribution of content [12].

Based on the description, a DRM system will be developed using symmetric and asymmetric hybrid cryptographic algorithms, which use integrated AES and RSA algorithms to encrypt video files. Video files are encrypted using AES and RSA algorithms in one system, in which the AES algorithm is used to encrypt video files. The AES key will then be wrapped with an RSA key.

2. STUDY LITERATURE

This research will use references from various sources to develop a Digital Rights Management System for video files. The system will be developed in the UAD TV Studio to control user access to the content of video files. The development of this system will use technology that has been developed previously, namely using AES and RSA cryptographic algorithm technology. This algorithm is used for the encryption process of video files

2.1 Digital Rights Management

Digital rights management (DRM) is the use of technology to control and manage access to digital content. DRM aims to protect copyright holders and prevent content from unauthorized distribution and modification [13]. DRM is gaining in importance as digital content spreads through peer-to-peer file exchanges, torrent sites, and online piracy. Most DRM systems are cryptographic software protocols. They work by cryptographically "locking" files so that only "authorized" users can access, modify, or distribute them [14].

2.2 Cryptographic Algorithms

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to alter messages in ways that are difficult to decipher. Cryptosystems use a set of procedures known as ciphers to encrypt and decrypt data to secure communications between computer systems, devices, and applications. Based on the key used, cryptographic algorithms have two types, which consist of symmetric and asymmetric encryption algorithms [15], as shown in Figure 1.

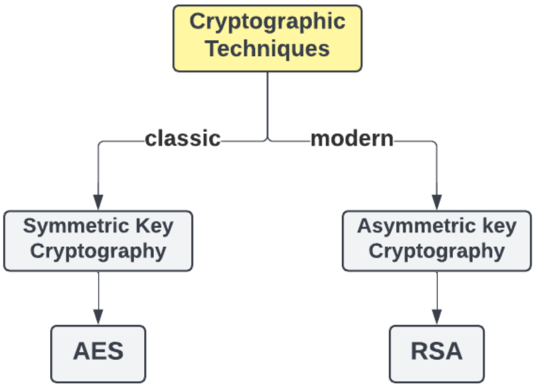


Figure 1. Types of Cryptography

2.2.1 *Symmetric Key Cryptography*

This is the simplest type of encryption that involves only one secret key to encode and decipher information. Symmetric encryption involves the use of a single key for both encryption and decryption [16]. The plaintext is read into the encryption algorithm along with the key. The key works with an algorithm to convert plaintext into ciphertext, thus encrypting the original sensitive data. The scenario of using asymmetric keys is seen in Figure 2.

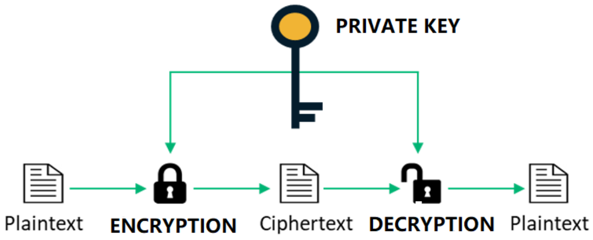


Figure 2. Symmetric Key Cryptography

Symmetric key uses only one private key to perform the encryption and decryption process on the message to be sent. This approach is the opposite of asymmetric encryption, which uses one key to encrypt and another to decrypt [17].

2.2.1 *Asymmetric Key Cryptography*

Asymmetric encryption works with any pair of keys. The beginning of asymmetric encryption involves the creation of a pair of keys, one of which is the public key, and the other is the private key. The public key can be accessed by anyone, while the private key must be kept secret from everyone except the creator of the key [18]. This is because encryption occurs with the public key while decryption occurs with the private key. The recipient of sensitive data will provide the sender with their public key, which will be used to encrypt the data. This ensures that only the recipient can decrypt the data with their own private key [19]. The usage scenario of asymmetric cryptographic keys is shown in Figure 3.

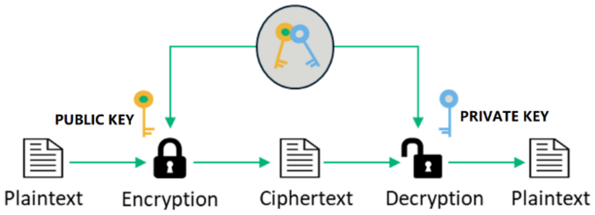


Figure 3. Asymmetric Key Cryptography

In the process of sending a message, encrypt and decrypt the message using a similar key pair. In asymmetric key cryptography, messages are encrypted using the public key, and the private key is used for decryption [20].

2.3 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is an encryption algorithm established by the National Institute of Science and Technology (NIST) in 2001 [21]. The cipher used in AES is a block cipher of the Rijndael cipher family. When AES was created, three different Rijndael block ciphers were chosen to be used to make AES more secure [22]. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. All three ciphers used are 128 bits, but the keys used are each of different sizes: 128, 192, and 256 bits. It is considered a symmetrical block cipher since only one key is used in the encryption process [23].

2.4 Rivest–Shamir–Adleman (RSA)

The RSA algorithm is a type of asymmetric cryptographic algorithm that uses two different but mathematically interconnected keys, two RSA keys consisting of a public and a private key. As the name suggests, the public key is shared publicly, while the private key is confidential and should not be shared with anyone. In the process of using the public key, the public key is used to encrypt the message while the private key is used to decrypt the message [24]. The two keys are interconnected and cannot be separated, meaning that the message is encrypted with the public key, and the message can only be decrypted with its private key pair. The safety of RSA depends on the practical difficulty of factoring the product of two large primes. The RSA algorithm has a slow process if used to encrypt large data. Therefore, the RSA algorithm is not recommended to encrypt large data directly. The RSA algorithm is more commonly used to transmit shared keys for symmetric key cryptography, which is then used for mass encryption-decryption processes [25].

2.5 Rivest–Shamir–Adleman (RSA)

The RSA algorithm is a type of asymmetric cryptographic algorithm that uses two different but mathematically interconnected keys, two RSA keys consisting of a public and a private key. As the name suggests, the public key is shared publicly, while the private key is confidential and should not be shared with anyone. In the process of using the public key, the public key is used to encrypt the message while the private key is used to decrypt the message [24]. The two keys are interconnected and cannot be separated, meaning that the message is encrypted with the public key, and the message.

3. METHODOLOGY

3.1 Requirement Analysis

The initial stage before creating and designing the system to be built requires data and useful information to be a reference for how the system will be made. Data collection and information in the UAD TV Studio is carried out by observation and interviews. Based on information obtained at this time, the UAD TV studio has not applied DRM to video files produced, therefore the video file DRM application is built to secure and control access to video files produced by UAD TV. The concept of the DRM system to be built is shown in Figure 4.

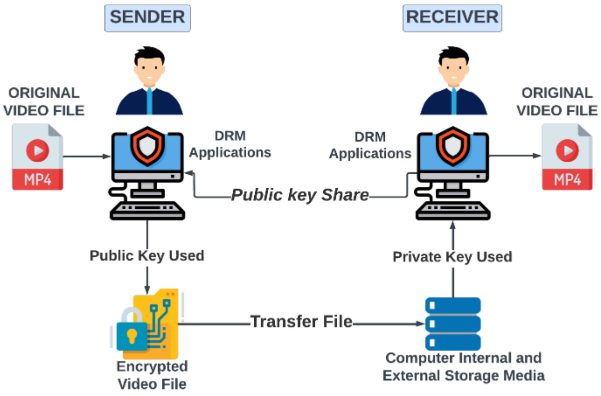


Figure 4. DRM Application Concept

Based on Figure 4, the concept of the DRM application that will be used by UAD TV studio, first the receiver will create a public key and an RSA private key by generating a key. After that, the public key will be sent or disseminated to the user who will send the video file. The public key will be used by the sender to encrypt the video file, while the private key is held and used by the receiver to decrypt the video file that has been decrypted using the public key.

3.2 System Design

The design of the application system created will integrate AES and RSA cryptographic algorithms as an implementation of digital rights management (DRM) using cryptography on security in mp4 video files produced by UAD TV studio. Video files are encrypted using AES and RSA algorithms in one system, wherein the AES algorithm is used to encrypt video files while the RSA algorithm is used to encrypt AES secret key. AES and RSA key wrapping occurs when the video file encryption process starts.

The basic concept is that video files are encrypted with the AES-GCM 256-bit algorithm using a unique disposable secret key, and then the AES key used to encrypt video files is encrypted again using the RSA-OAEP 4096-bit algorithm. This key wrapping algorithm is a hybrid encryption scheme consisting of asymmetric key wrapping and symmetric key wrapping operations as described below:

- ➔ The public key from the import job is used with RSAES-OAEP 4096-bit, using the SHA-512 digest algorithm, to encrypt a one-time-use AES-GCM-256 key. The one-time-use AES-GCM 256 key is generated at the time the wrapping is performed.
- ➔ The one-time-use AES-256 key from step 1 is used to encrypt the target key material using AES Key Wrap with Padding.

The wrapped key material for import is a single byte array consisting of the results of step 1, followed by the results of step 2. In other words, the results of steps 1 and 2 are concatenated together to form the wrapped key material.

3.3 System Modelling

System modeling is the process of developing abstract models of a system. System modeling is needed so that this application can run according to its function, which is to produce encrypted video files with the integration of AES and RSA algorithms. This system modeling is made so that the system can be built in accordance with what is required by the UAD TV studio. This system modeling discusses the encryption process of AES and RSA algorithms. Modeling system is shown in Figure 5.

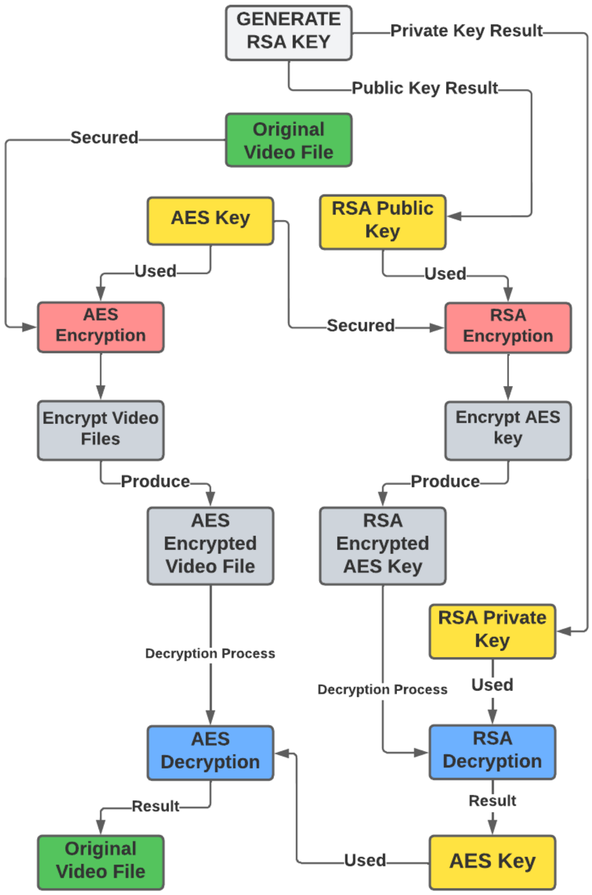


Figure 5. DRM Application Concept

Based on the system modeling in Figure 5, before the key exchange process, the sender and receiver of the video file agree to create public and private keys. The public key is shared with the sender, and when the public key holder wants to send the video file to the receiver, the public key will be used for encryption. The video file encryption process involves several encryption processes, consisting of video file encryption by the AES algorithm and AES private key encryption by the RSA algorithm. The video file can only be opened or decrypted with the RSA private key pair owned.

3.4 Coding System

Coding the system is the process of writing program codes that will be used so that the system can run and function according to the design of the system in the application. At this stage, the system will be built using several programming languages, while the main programming languages used to build the system so that applications can run are JavaScript, CSS, and HTML, this application will use web application security protocols using JavaScript to perform basic cryptographic operations in web applications.

3.5 Testing and Evaluation

The system has been completed and implemented;the next stage is testing. Testing this application aims to ensure whether the system can run properly and is worth using.this testing includes how the application can secure mp4 video files with the AES-GCM 256-bit encryption algorithm and RSA-OAEP 4096-bit encryption. After the test is completed, the evaluation will be carried out as a reference for improvement if there are shortcomings or problems when running the application.

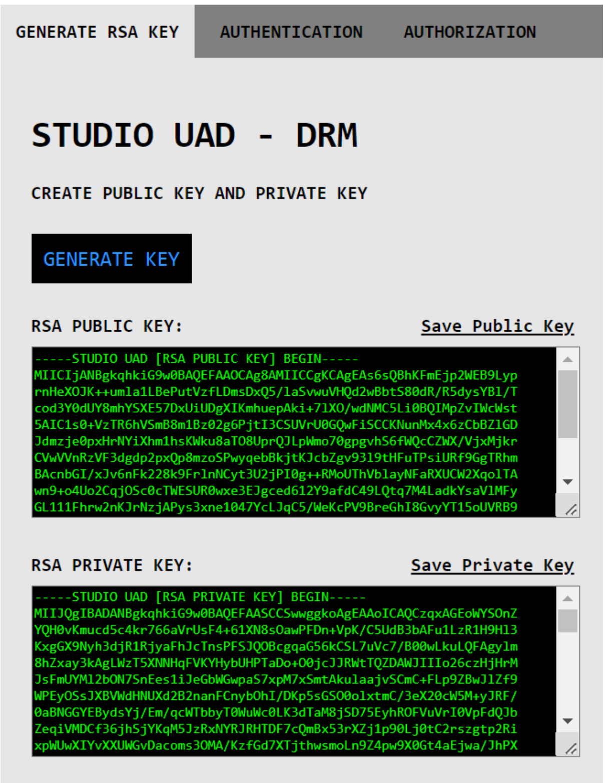
4. RESULT AND DISCUSSION

4.1 Display and Implementation of Application Usage

In this section, the DRM (Digital Rights Management) application already has a user interface and features that are ready to test the application's functionality when generating keys, encrypting, and decrypting mp4 video files.

4.1.1 RSA Key Generator User Interface

In this section, the display and menu of the RSA key generator page are displayed. The output results at this stage are public and private keys. The following display and testing of the RSA key generator function can be seen in Figure 6.



```
-----STUDIO UAD [RSA PUBLIC KEY] BEGIN-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAs6sQBhKFmEjp2WEB9Lyp
rnHeXOJK++umla1LBePutVzfLDmsDxQ5/laSvwuVHQd2wBbtS80dR/R5dysYBl/T
cod3Y0dUY8mhYSXE57DxUiUDgXIKmhuepAki+71XO/wdNMC5Li0BQIMpZvIWcWst
5AIC1s0+VzTR6hVSmB8m1Bz02g6PjtI3CSUVrU0GQwFiSCCKNunMx4x6zCbBZlGD
Jdmzje0pxHrNYiXhm1hsKWku8aTO8UprQJLpWmo70gpgvhS6fWQcCZWX/VjxMjkr
CVwVVnRzVF3dgdp2pxQp8mzoSPwyqebBkjtKJcbZgv9319tHFuTPsiURf9GgTRhm
BAcnbGI/xJv6nFk228k9FrlnNCyt3U2jPI0g++RMoUThVblayNFaRXUCW2XqolTA
wn9+o4Uo2CqjOSc0cTWESUR0wxe3EJgced612Y9afdC49LQtq7M4LadkYsaVlMFy
GL111Fhrw2nKJrNzjAPys3xne1047YcLJqC5/WeKcPV9BreGhI8GvyYT15oUVRB9
```

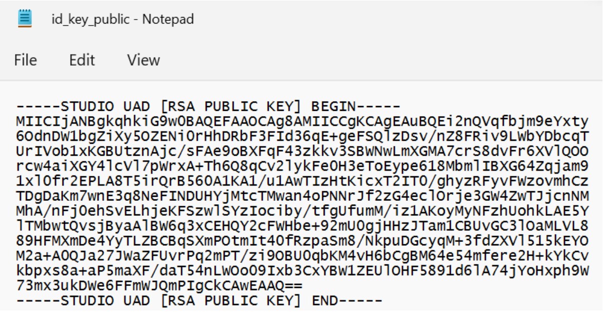
```
-----STUDIO UAD [RSA PRIVATE KEY] BEGIN-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwggkoAgEAAoICAQCzqxAGEoWYSOnZ
YQH0vKmucd5c4kr766aVrUsF4+61XN8sOawPFDn+VpK/C5UdB3bAFu1LzR1H9H13
KxgGX9Nyh3djR1RjyaFhJcTnsPFSJQOBcgqaG56kCSL7uVc7/B00wLkuLQFAgylm
8hZxay3kAgLWzT5XNNHqFVKYHybUHPTaDo+O0jcJJRWtTQZDAWJIIIo26czHjHrM
JsFmUYMl2bON7SnEes1iJeGbWGwpaS7xpM7xSmtAkulaajvSCmC+FLp9ZBwJlZf9
WPEyOSsJXBVWdHNUXd2B2nanFCnybOhI/DKp5sGSO0olxtmC/3eX20cW5M+yJRF/
0aBNGGYEBydsYj/Em/qcWTbbyT0WuWc0LK3dTaM8jSD75EyhROFVuVrI0VpFdQJb
ZeqiVMDCf36jhSjYKqM5JzRxNYRJRHTDF7cQmBx53rXZj1p90Lj0tC2rszgtp2Ri
xpWUwXIYvXXUWGvDacoms3OMA/KzfGd7XTjthwsmoLn9Z4pw9X0Gt4aEjwa/JhPX
```

Figure 6. RSA Key Generator Page View

Based on Figure 6 of the key generator feature testing results, the application managed to provide a response and output in the form of 2 keys, namely the public key and private key RSA 4096 bit. With an RSA key length of 4096 bits. This key is used for the encryption and decryption of the video file's content. The public and private key files will be automatically saved in.txt format on the computer's local storage. The private key is confidential, and this public key will be shared or published. These are the public and private keys, as shown in Figure 7 and Figure 8.

4.1.1.1 RSA Public key

Public key cryptography, also known as asymmetric cryptography, is a system that uses key pairs to encrypt and authenticate information. One of the keys in a pair is a public key that can be widely distributed without affecting security. The RSA public key is used for the encryption process of video files,this public key is non-confidential. This public key is an RSA-OAEP key with a length of 4096-bit. The RSA public key is shown in Figure 7.



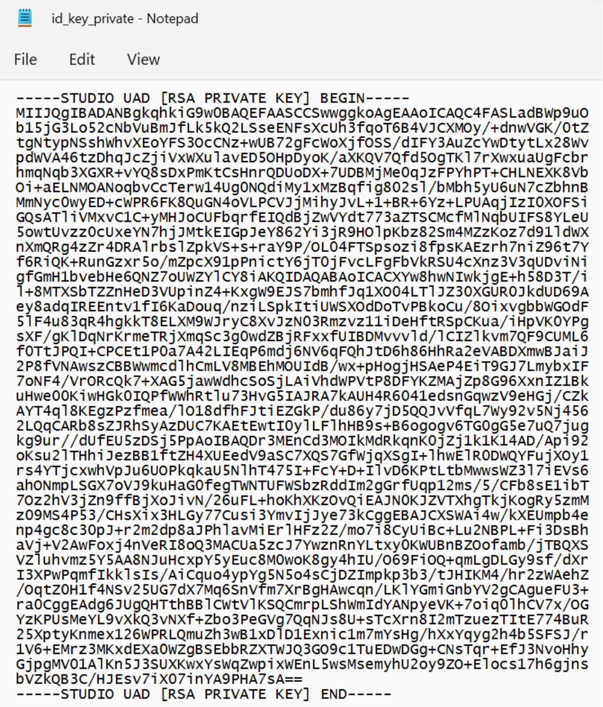
```
-----STUDIO UAD [RSA PUBLIC KEY] BEGIN-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAuBQEi2nQVqfbjm9eYxty
6OdnDW1bgZiXy5OZENiOrHhDRbF3FId36qE+geFSQlzDsv/nZ8FRiv9LWbYDbcqT
UrIVob1xKGBUtznAjc/sFAe9oBXFqF43zkkv3SBWNwLmXGMA7crS8dvFr6XVlQOO
rcw4aiXGY4lcVl7pWrxA+Th6Q8qCv2lykFeOH3eToEype618MbmlIBXG64Zqjam9
1xl0fr2EPLA8T5irQrB56OA1KA1/u1AwTIzHtKicxT2ITO/ghyzRFyvFWzovmhCz
TDgDaKm7wnE3q8NeFINDUHYjMtcTMwan4oPNNrJf2zG4eclOrje3GW4ZwTJjcnNM
MhA/nFjOehSvELhjeKFSzwlSYzIociby/tfgUfumM/iz1AKoyMyNFzhUohkLAE5Y
lTMbwtQvsjByaAlBW6q3xCEHQY2cFWHbe+92mUOgjHHzJTam1CBUvGC3lOaMLVL8
89HFMXmDe4YyTLZBCBqSXmPOtmIt40fRzpaSm8/NkpuDGcyqM+3fdZXVl515kEYO
M2a+AOQJa27JWaZFUvrPq2mPT/zi9OBUOqbKM4vH6bCgBM64e54mfere2H+kYkCv
kbpxs8a+aP5maXF/daT54nLWOo09Ixb3CxYBW1ZEUlOHF5891d6lA74jYoHxph9W
73mx3ukDWe6FFmWJQmPIgCkCAwEAAQ==
-----STUDIO UAD [RSA PUBLIC KEY] END-----
```

Figure 7. RSA Public Key

The RSA public key is non-confidential and public keys can be shared with everyone in the system. Once the sender has the public key, he uses it to encrypt his video file.

4.1.1.2 RSA Private key

The RSA private key is used for the decryption of encrypted video files. This private key is an RSA-OAEP key with a length of 4096-bit. The RSA private key is shown in Figure 8.



```
-----STUDIO UAD [RSA PRIVATE KEY] BEGIN-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQC4FASLadBWp9uO
b15jG3Lo52cNbVuBmJfLk5kQ2LSseENFsXcUh3fqoT6B4VJCXMOy/+dnwVGK/OtZ
tgNtypNSshWhvXEoYFS3OcCNz+wUB72gFcWoXjfOSS/dIFY3AuZcYwDtytLx28Wv
pdWVA46tzDhqJcZjiVxWXulavED5OHpDyoK/aXKQV7Qfd5OgTKl7rXwxuaUgFcbr
hmqNqb3XGXR+vYQ8sDxPmKtCsHnrQDUoDX+7UDBMjMeOqJzFPYhPT+CHLNEXK8Vb
Oi+aELNMOANoqbvCcTerw14UgONQdiMy1xMzBqfig8O2sl/bMbh5yU6uN7cZbhnB
MmNycOwyED+cWPR6FK8QuGN4oVLPCVJjMihyJvL+1+BR+6Yz+LPUAqjIzIOXOFSi
GQsATliVMxvC1C+yMHJoCUFbqrfEIQdBjZwVYdt773aZTSCMcfMlNqbUIFS8YLeU
5owtUvzzOcUxeYN7hjJMtkEIGpJeY862Yi3jR9HOlpKbz82Sm4MZzKoz7d91ldWX
nXmQRg4zZr4DRAlrbslZpkVS+s+raY9P/OLO4FTSpsozi8fpsKAEzrh7niZ96t7Y
f6RiQK+RunGzxr5o/mZpcX91pPnictY6jTOjFvcLFgFbVkRSU4cXnz3V3qUDviNi
gfGmH1bvebHe6QNZ7oUWZYlCY8iAKQIDAQABAoICACXYw8hwNIwkjgE+h58D3T/i
l+8MTXSbTZZnHeD3VUpinZ4+KxgW9EJS7bmhfJq1XOO4LTlJZ3OXGUROJkdUD69A
ey8adqIREEntv1fI6KaDouq/nziLSpkItiUWSXOdDoTvPBkoCu/8OixvgbbWGOdF
5lF4u83qR4hgkkT8ELXM9WJryC8XvJzNO3Rmzvz11iDeHftRSpCKua/iHpVKOYPg
sXF/gKlDqNrKrmeTRjXmqSc3gOwdZBjRFxxfUIBDMvvvld/lCIZlkvm7QF9CUML6
fOTtJPQI+CPCEt1POa7A42LIEqP6mdj6NV6qFQhJtD6h86HhRa2eVABDXmwBJaiJ
2P8fVNAwszCBBWwmcdlhCmLV8MBEhMOUIdB/wx+pHogjHSAeP4EiT9GJ7LmybxIF
7oNF4/VrORcQk7+XAG5jawWdhcSoSjLAiVhdWPVtP8DFYKZMAjZp8G96XxnIZ1Bk
uHweOOKiwHGkOIQPfWWhRtlu73HvG5IAJRA7kAUH4R6041edsnGqwzV9eHGj/CZk
AYT4ql8KEgzPzfmea/lO18dfhFJtiEZGkP/du86y7jD5QQJvVfqL7Wy92v5Nj456
2LQqCARb8sZJRhSyAzDUC7KAEtEwtIOylLFlhHB9s+B6ogogv6TGOgG5e7uQ7jug
kg9ur//dUfEU5zDSj5PpAoIBAQDr3MEnCd3MOIkMdRkqnKOjZj1k1K14AD/Api92
oKsu2lTHhiJezBB1ftZH4XUEedV9aSC7XQS7GfWjqXSgI+lhwElRODWQYFujXOy1
rs4YTjcxwhVpJu6UOPkqkaU5NlhT475I+FcY+D+IlvD6KPtLtbMwwsWZ3l7iEVs6
ahONmpLSGX7oVJ9kuHaGOfegTWNTUFWSbzRddIm2gGrfUqp12ms/5/CFb8sE1ibT
7Oz2hV3jZn9ffBjXoJivN/26uFL+hoKhXKzOvQiEAJNOKJZVTXhgTkjKogRy5zmM
zO9MS4P53/CHsXix3HLGy77Cusi3YmvIjJye73kCggEBAJCXSWAi4w/kXEUmpb4e
np4gc8c3OpJ+r2m2dp8aJPhlavMiErlHFz2Z/mo7i8CyUiBc+Lu2NBPL+Fi3DsBh
aVj+V2AwFoxj4nVeRI8oQ3MACUa5zcJ7YwznRnYLtxyOKWUBnBZOofamb/jTBQXS
VZluhvmz5Y5AA8NJuHcxpY5yEuc8MOwoK8gy4hIU/O69FiOQ+qmLgDLGy9sf/dXr
I3XPwPqmfIkklsIs/AiCquo4ypYg5N5o4sCjDZImpkp3b3/tJHIKM4/hr2zWAehZ
/OqtZOH1f4NSv25UG7dX7Mq6SnVfm7XrBgHAwcqn/LKlYGmiGnbYV2gCAgueFU3+
raOCggEAdg6JUgQHTthBBlCWtVlKSQCmrpLShWmIdYANpyeVK+7oiqOlhCV7x/OG
YzKPUsMeYL9vXkQ3vNXf+Zbo3PeGVg7QqNJs8U+sTcXrn8I2mTzuezTItE774BuR
25XptyKnmex126WPRLQmuZh3wB1xDlD1Exnic1m7mYsHg/hXxYqyg2h4b5SFSJ/r
1V6+EMrz3MKxdEXaOWZgBSEbbRZXTWJQ3GO9c1TuEDwDGg+CNsTqr+EfJ3NvoHhy
GjpgMVO1AlKn5J3SUXKwxYsWqZwpixWEnL5wsMsemyhU2oy9ZO+Elocs17h6gjns
bVZkQB3C/HJEsv7iXO7inYA9PHA7sA==
-----STUDIO UAD [RSA PRIVATE KEY] END-----
```

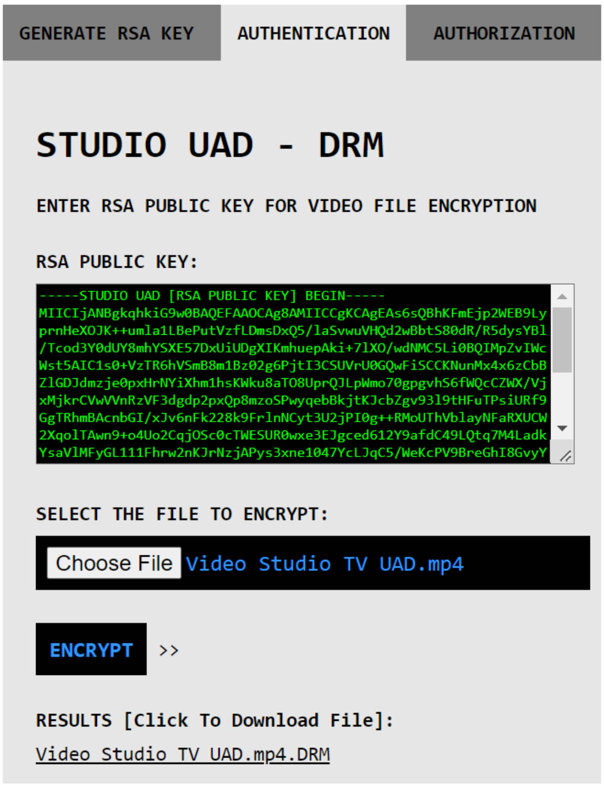
Figure 8. RSA Private Key

As shown in Figure 8, the RSA private key is longer than the RSA public key. This is because the RSA public key consists of a modulus and another value called the "public exponent," which is usually quite short. So, the public key will require relatively few additional bytes for encoding. This does not apply to the private key, which includes the modulus and the public exponent (like the public key) but also the "private exponent". The consequence is that the encoded private key is expected to become longer. This private key is confidential and should not be shared with anyone else.

On thisapplication, when a 4096-bit RSA-OAEP algorithm key is generated, the RSA public key and private key are encoded from the ArrayBuffer to base64, base64 to PEM, or vice versa, and displayed in PEM (Privacy-Enhanced Mail) format. This key will later be used during the RSA and AES wrap key and unwrap key processes. The public key is used for encryption and the private key is used for data decryption.

4.1.2 File Encrypt User Interface

In this section, the display and menu of the video file encryption page are displayed.The encryption page is part of the DRM application that will be used to process the encryption of video files. This page consists of several functions that can be executed. The output at this stage is the encrypted video file. The following display and encryption testing is shown in Figure 9.



STUDIO UAD - DRM

ENTER RSA PUBLIC KEY FOR VIDEO FILE ENCRYPTION

RSA PUBLIC KEY:

```
-----STUDIO UAD [RSA PUBLIC KEY] BEGIN-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAs6sQBhKFmEjp2WEB9Ly
prnHeXOJK++umla1LBePutVzfLDmsDxQ5/laSvwuVHQd2wBbtS80dR/R5dysYBl
/Tcod3Y0dUY8mhYSXE57DxUiUDgXIKmhuepAki+7lXO/wdNMC5Li0BQIMpZvIWc
Wst5AIC1s0+VzTR6hVSmB8m1Bz02g6PjtI3CSUVrU0GQwFiSCCKNunMx4x6zCbB
ZlGDJdmzje0pxHrNYiXhm1hsKWku8aTO8UprQJLpWmo70gpgvhS6fWQcCZWX/Vj
xMjkrCVwVVnRzVF3dgdp2pxQp8mzoSPwyqebBkjtKJcbZgv93l9tHFuTPsiURf9
GgTRhmBAcnbGI/xJv6nFk228k9FrlnNCyt3U2jPI0g++RMoUThVblayNFaRXUCW
2XqolTAwn9+o4Uo2CqjOSc0cTWESUR0wxe3EJgced612Y9afdC49LQtq7M4Ladk
YsaVlMFyGL111Fhrw2nKJrNzjAPys3xne1047YcLJqC5/WeKcPV9BreGhI8GvyY
```

SELECT THE FILE TO ENCRYPT:

Video Studio TV UAD.mp4

RESULTS [Click To Download File]:

Video Studio TV UAD.mp4.DRM

Figure 9. Encrypt File Page

To perform the encryption process, the first stage is to enter the public key into the application form. After that, select the file from the local storage by clicking the "Select File" button. The next step is to click the "encrypt" button to start the video file encryption process.File changes also occur,files that could previously be opened with a media player can now no longer be opened with any software. Mp4 video files that have been encrypted using this combination of AES and RSA can only be opened or decrypted with their private key pair.

The result of the encrypted video file is shown in Figure 10.

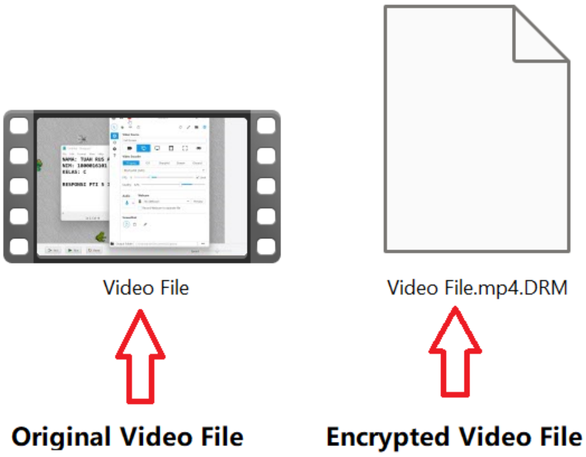
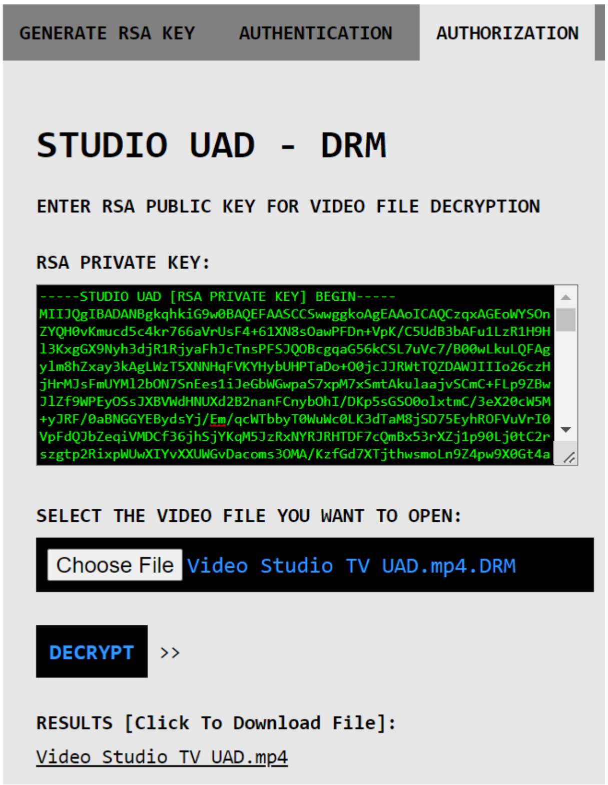


Figure 10. Results After and Before the File is Encrypted

Based on the output of the video file before and after decryption, there are changes that occur in the mp4 video file, including the extension of the file, the file extension before and after the video file is decrypted.

4.1.3 File Decrypt User Interface

In this section, the display and menu of the video file decryption page are displayed. The output result at this stage is the decrypted video file. The following display and decryption testing is shown in Figure 11.



STUDIO UAD - DRM

ENTER RSA PUBLIC KEY FOR VIDEO FILE DECRYPTION

RSA PRIVATE KEY:

```
-----STUDIO UAD [RSA PRIVATE KEY] BEGIN-----
MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQCzqxAGEoWYSOn
ZYQH0vKmucd5c4kr766aVrUsF4+61XN8sOawPFDn+VpK/C5UdB3bAFu1LzR1H9H
l3KxgGX9Nyh3djR1RjyaFhJcTnsPFSJQOBcgqaG56kCSL7uVc7/B00wLkuLQFAg
ylm8hZxay3kAgLWzT5XNNHqFVKYHybUHPTaDo+O0jcJJRWtTQZDAWJIIIo26czH
jHrMJsFmUYMl2bON7SnEes1iJeGbWGwpaS7xpM7xSmtAkulaajvSCmC+FLp9ZBw
JlZf9WPEyOSsJXBVWdHNUXd2B2nanFCnybOhI/DKp5sGSO0olxtmC/3eX20cW5M
+yJRF/0aBNGGYEBydsYj/Em/qcWTbbyT0WuWc0LK3dTaM8jSD75EyhROFVuVrI0
VpFdQJbZeqiVMDCf36jhSjYKqM5JzRxNYRJRHTDF7cQmBx53rXZj1p90Lj0tC2r
szgtp2RixpWUwXIYvXXUWGvDacoms3OMA/KzfGd7XTjthwsmoLn9Z4pw9X0Gt4a
```

SELECT THE VIDEO FILE YOU WANT TO OPEN:

Video Studio TV UAD.mp4.DRM

RESULTS [Click To Download File]:

Video Studio TV UAD.mp4

Figure 11. Decrypt File Page

To perform the decryption process, the first step is to enter the private key into the application form. After that, select the file from the local storage by clicking the "Select File" button. The next step is to click the "decrypt" button to start the decryption process of the encrypted video file. After that, its contents can be accessed using a common media player.

4.2 Application Functional Testing Results

This test aims to ensure that the application works according to the design of the system. This test was carried out directly at the UAD TV Studio by several members on duty, namely as senders and receivers of studio-produced video files. The testing process is carried out by executing several functions of the application, among which are generating public and private keys and encryption and decryption of mp4 video files. The instrument used to perform this test is black box testing. The black box test results are shown in the table.

4.2.1 Test Results Generate a Key

In this section, the function of the application in generating the RSA public and private keys will be tested. This test is done with several stages of application testing by looking at the response results in the form of input and output. The test results are shown in Table 1.

Table 1. Test Results Generate a Key

No	Test List	Description	Results
1	Click the “Generate Key” button to generate a key.	The system will display the output of public and private keys.	Valid
2	Click the "Save Public Key" button.	The system will save the public key file in local storage.	Valid
3	Click the "Save private key" button.	The system will save the private key file in local storage.	Valid

Based on the test results in Table 1. The function of generating keys runs as expected and provides a response in the form of public and private key outputs that will be used for encryption and decryption processes at a later stage.

4.2.2 Test Results Encrypt Video File

In this section the encryption function of video files will be tested, this test is done with several stages of application testing by looking at the response results in the form of input and output, the test results are shown in Table 2.

Table 2. Test Results Encrypt Video File

No	Test List	Description	Results
1	Click the button to search for the video file to encrypt.	The system will display a search form for video files that will be encrypted.	Valid
2	Fill in the form with the public key.	The system will use the public key to authenticate the video file.	Valid
3	Click the "encrypt" button.	The system will process the encryption of the video file.	Valid
4	Click the "Save File" button.	The system will save the encrypted video file in local storage.	Valid

Based on the test results in Table 2, the video file encryption function succeeds as expected and gives a response in the form of an encrypted video file output. The first process is to provide input in the form of mp4 video files stored on local storage. After that, provide input in the form of a public key for encryption. After providing input in the form of mp4 video files and a public key, then give the command to run the encryption program by clicking "encryption". After the program is run, the system will automatically respond in the form of output in the form of encrypted mp4 video files.This video file can only be decrypted with its private key pair.

4.2.3 Test Results Decrypt Video File

In this section the decryption function of encrypted video files will be tested, this test is carried out with several stages of testing, namely by looking at the response results in the form of input and output. The input is a private key, and the output is a decrypted video file. The test results are shown in Table 3.

Table 3. Test Results Decrypt Video File

No	Test List	Description	Results
1	Click the button to search for the video file to decrypt.	The system will display a search form for video files that will be decrypted.	Valid
2	Fill in the form with the private key.	The system will use the private key for authorization of the video file.	Valid
3	Click the "decrypt" button.	The system will process the decryption of the encrypted video file.	Valid
4	Click the "Save File" button.	The system will save the already decrypted video file in local storage.	Valid

The decryption function on the encrypted video file succeeds as expected and gives a response in the form of the decrypted video file. Based on the results on the three test tables, the system can run several features of the DRM application to generate keys, encrypt and decrypt mp4 video files produced by UAD TV Studio. The number of black box testing tables tested was 3 tables, with each test being done twice. All the results of the black box test table tested were found to be free of errors when testing its use by the studio crew, so that the Digital Rights Management (DRM) application can be implemented in mp4 video files produced or managed by UAD TV Studio.

5. CONCLUSION

The DRM (Digital Rights Management) application developed at UAD TV Studio is successfully implemented by running several processes, namely the process of generating public and private keys, storing public and private keys, encrypting video files using public keys, storing encrypted video files, decrypting video files using private keys, and storing MP4 video files that have been decrypted in local storage. RSA-OAEP 4096 bit and AES-GCM 256-bit algorithms with key wrapping mechanism for the encryption process of video files produced to have digital rights management successfully implemented and can be used to grant access rights to video files produced or managed by UAD TV studios.In future work, I will work on encryption of video streaming using other modern cryptographic algorithms such as ECC, which have better performance in terms of speed and security for data transfer encryption.

6. REFERENCES

[1] S. Rana and D. Mishra, “Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems,” Security and Privacy, vol. 4, no. 1, Jan. 2021, doi: 10.1002/spy2.133.

[2] H. Zhao, Y. Liu, Y. Wang, and Y. Huang, “Hiding Data into Blockchain-based Digital Video for Security Protection,” in Proceedings - 2020 3rd International Conference on Smart BlockChain, SmartBlock 2020, Oct. 2020, pp. 23–28. doi: 10.1109/SmartBlock52591.2020.00012.

[3] R. J. Mstafa, Y. M. Younis, H. I. Hussein, and M. Atto, “A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector,” IEEE Access, vol. 8, pp. 161825–161837, 2020, doi: 10.1109/ACCESS.2020.3021356.

[4] A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon, and W. El-Shafai, “A Novel Hybrid Cryptosystem for Secure Streaming of High Efficiency H.265 Compressed Videos in IoT Multimedia Applications,” IEEE Access, vol. 8, pp. 128548–128573, 2020, doi: 10.1109/ACCESS.2020.3008644.

[5] M. K. Lee and E. S. Jang, “Cryptanalysis of Start Code-Based Encryption Method for HEVC,” IEEE Access, vol. 9, pp. 92568–92577, 2021, doi: 10.1109/ACCESS.2021.3092005.

[6] . Xu, “Commutative Encryption and Data Hiding in HEVC Video Compression,” IEEE Access, vol. 7, pp. 66028–66041, 2019, doi: 10.1109/ACCESS.2019.2916484.

[7] E. Adali, Akdeniz Üniversitesi, and Institute of Electrical and Electronics Engineers , 2. UluslararasıBilgisayarBilimleriveMühendisliğiKonferansı = 2nd International Conference on Computer Science and Engineering : Antalya - Türkiye 5-8 Ekim (October) 2017.

[8] H. Jiaming and Z. Hongbin, “Digital right management model based on cryptography and digital watermarking,” in Proceedings - International Conference on Computer Science and Software Engineering, CSSE 2008, 2008, vol. 3, pp. 656–660. doi: 10.1109/CSSE.2008.1000.

[9] A. C. Prihandoko and H. Ghodosi, “Oblivious Content Distribution System to Advantage Digital Rights Management.”

[10] D. Mishra and S. Rana, “Authenticated content distribution framework for digital rights management systems with smart card revocation,” International Journal of Communication Systems, vol. 33, no. 9, Jun. 2020, doi: 10.1002/dac.4388.

[11] S. Rana and D. Mishra, “Cryptanalysis and improvement of biometric based content distribution framework for digital rights management systems,” Security and Privacy, vol. 4, no. 1, Jan. 2021, doi: 10.1002/spy2.133.

[12] C. T. Yen, H. T. Laiw, N. W. Lo, T. C. Liu, and J. Stu, “Transparent digital rights management system with superdistribution,” in Proceedings - 2010 International Conference on Broadband, Wireless Computing Communication and Applications, BWCCA 2010, 2010, pp. 435–440. doi: 10.1109/BWCCA.2010.110.

[13] E. Becker, W. Buhse, D. Günnewig, and N. Rump, “LNCS 2770 - Digital Rights Management (Frontmatter Pages).”

[14] J. Gao, H. Yu, X. Zhu, and X. Li, “Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption,” IEEE Systems Journal, vol. 15, no. 4, pp. 5233–5244, Dec. 2021, doi: 10.1109/JSYST.2021.3064356.

[15] K. Pavani and P. Sriramya, “Enhancing public key cryptography using RSA, RSA-CRT and N-Prime RSA with multiple keys,” in Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021, Feb. 2021, pp. 661–667. doi: 10.1109/ICICV50876.2021.9388621.

[16] A. Baksi, “Computer Architecture and Design Methodologies Classical and Physical Security of Symmetric Key Cryptographic Algorithms.”

[17] M. Islam, M. Shah, Z. Khan, T. Mahmood, and M. J. Khan, “A New Symmetric Key Encryption Algorithm Using Images as Secret Keys,” in Proceedings - 2015 13th International Conference on Frontiers of Information Technology, FIT 2015, Feb. 2016, pp. 1–5. doi: 10.1109/FIT.2015.12.

[18] W. Easttom, *Modern Cryptography*. Springer International Publishing, 2021. doi: 10.1007/978-3-030-63115-4.

[19] N. Kabir and S. Kamal, “Secure Mobile Sensor Data Transfer using Asymmetric Cryptography Algorithms,” Oct. 2020. doi: 10.1109/ICCWS48432.2020.9292392.

[20] A. Siddiqa and S. Ahmed, “Scalable Asymmetric Security Mechanism for Internet of Things,” 2020. [Online]. Available: www.ijacsa.thesai.org

[21] J. Vincenttrijmen, “Information Security and Cryptography TheeDesignoffRijndaelTheeAdvanced Encryption Standard (AES) Second Edition.”

[22] Z. Lu and H. Mohamed, “A Complex Encryption System Design Implemented by AES,” Journal of Information Security, vol. 12, no. 02, pp. 177–187, 2021, doi: 10.4236/jis.2021.122009.

[23] Y. Yuan, Y. Yang, L. Wu, and X. Zhang, “A High-Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation.”

[24] C. H. Hsia, S. J. Lou, H. H. Chang, and D. Xuan, “Novel Hybrid Public/Private Key Cryptography Based on Perfect Gaussian Integer Sequences,” IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3121252.

[25] L. Zhang, B. Li, and X. Zhao, “Reconfigurable Hardware Implementation of AES-RSA Hybrid Encryption and Decryption,” in 2020 IEEE 5th International Conference on Signal and Image Processing, ICSIP 2020, Oct. 2020, pp. 970–974. doi: 10.1109/ICSIP49896.2020.9339251.