Asian Journal of Research in Computer Science

Volume 17, Issue 9, Page 112-125, 2024; Article no.AJRCOS.123574
ISSN: 2581-8260

Securing OTP-based Access in Film-sharing Platforms Using RSA Encryption and QR Codes

I Ketut Gede Suhartana [a*], I Nyoman Budhiarta Suputra [a] and Anak Agung Ngurah Gunawan [b*]

[a] Informatics Department, Faculty of Mathematics and Natural Science, Udayana University, Indonesia.
[b] Physics Department, Faculty of Mathematics and Natural Science, Udayana University, Indonesia.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/ajrcos/2024/v17i9503

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/123574

Original Research Article

Received: 14/07/2024
Accepted: 16/09/2024
Published: 21/09/2024

ABSTRACT

Login data refers to information used by individuals who have purchased or subscribed to a specific membership. Typically, this data includes an OTP code. In this research, the OTP code is utilized to grant users access to view the list of movies associated with the account that added them as a member. OTPs are particularly vulnerable to attacks, as they are often transmitted via phone numbers or email. To mitigate risks such as eavesdropping or interception, implementing robust data security systems is essential. Cryptography, the science of data security and authenticity, plays a crucial role in protecting sensitive information. Rivest-Shamir-Adleman (RSA) is one of the algorithms employed to secure data. In this research, the RSA algorithm is used to encrypt the OTP code provided to members. This encrypted OTP code is then converted into a QR code format and

Corresponding author: E-mail: ikg.suhartana@unud.ac.id, a.a.ngurahgunawan@unud.ac.id;

***Cite as:** Suhartana, I Ketut Gede, I Nyoman Budhiarta Suputra, and Anak Agung Ngurah Gunawan. 2024. "Securing OTP-Based Access in Film-Sharing Platforms Using RSA Encryption and QR Codes". Asian Journal of Research in Computer Science 17 (9):112-25. https://doi.org/10.9734/ajrcos/2024/v17i9503.*

sent to the user via email. An application of the RSA algorithm in this research has proven effective in securing data. This is supported by the results of avalanche effect testing, which showed an average security improvement of 51.9%. Based on this percentage, it can be concluded that the system provides a high level of data security, making it challenging for unauthorized individuals to breach.

Keywords: RSA; cryptography; encryption; decryption; OTP; login.

1. INTRODUCTION

The rapid development of technology has become an inseparable part of human life, allowing various activities to be carried out using technology. The internet makes it possible to manage devices from anywhere and at any time. Video broadcasts, online learning, streaming, and various other activities increasingly use the internet. It is estimated that by 2030, the number of internet-connected activities will reach 15.14 billion, perhaps even 29.42 billion, indicating the increasingly profound role of the internet in everyday life [1]. One activity that experiences a positive impact from the internet is video streaming. The launch of YouTube in 2005 became a pioneer in video streaming connected to the internet. The emergence of online video distribution platforms offers alternative options for film distribution and audience consumption [2]. This platform allows people to buy and download movies directly from home without having to buy CD from offline stores that sell movie CD or DVD. This certainly really helps people to be efficient with time. They no longer need to think about transportation costs and waste time going to the store to buy the CD or DVD of the film they want to watch. The emergence of the Covid-19 virus has encouraged the development of video streaming because activities outside the home are limited. Which inevitably results in people who are used to watching films in cinemas switching to streaming films from home. Video streaming does not immediately have a positive impact. Even though it provides many benefits in terms of efficiency and costs, video streaming also has detrimental negative impacts if not handled properly. Due to the freedom of access rights, many people abuse this, one clear example that often occurs is the number of teenagers who are not yet old enough to watch adult films freely without any restrictions. If not handled properly, this will cause quite fatal problems because it can damage the mental health of teenagers and even children who are not yet fit to watch adult films. From a case study, two teenagers suspected of being addicted to pornographic videos admitted that they enjoyed watching activities because it could arouse curiosity and create a pleasant sensation [3].

Based on this problem, the author created a family-friendly system that can provide viewing based on the access rights given. To grant access rights to the account you wish to provide, an intermediary is needed so that the system can ensure that the data is correctly provided by the sender to the right person. OTP or one time password is a dynamic password that is only valid for one login session. In general, the OTP will be a 6-digit random number, which changes continuously every time a login occurs. This OTP system can reduce the risk of unauthorized people gaining access to the account. The OTP code is usually given via SMS to the user's cellphone number. However, from the results of research on OTPs provided via SMS, several types of attacks were found to be able to intercept the OTP code provided [4]. The attacks described in the research are wireless attacks and cellphone malware. Research on A Review of One Time Password Mobile Verification by [5] explains that using OTP via SMS has weaknesses against cell phone Trojan attacks. A trojan described in the research is ZITMO (Zeus in the Mobile). Responding to this research, [6] designed a security system on the login page using OTP. In this research, researchers added a data security process by encrypting the OTP with the MD5 algorithm. However, this research has not tested the security of the OTP code which has been encrypted using the MD5 algorithm [7,8]. Therefore, the author created a login data security system using the RSA algorithm to ensure the security of the OTP code sent. The security of the OTP code in this system is tested using the avalanche effect method, namely a testing method by changing one character of the OTP code, then comparing the ciphertext of the initial OTP code and the ciphertext of the OTP code that has been changed to see how many bits are different between the two ciphertexts. The higher the percentage of avalanche effect obtained, the more difficult it is for the OTP code to be intercepted by unauthorized parties responsible [9,10].

Research on OTP security using the RSA algorithm is crucial for protecting sensitive data, especially in digital authentication systems. With the increasing threat of cyber attacks, the use of RSA to encrypt OTP codes helps reduce the risk of attacks such as interception or malware.

2. METHODS

2.1 Data and Data Collection Methods

The data used in this research is a random OTP code which will be converted into a QR code. The QR code will be sent via email to users who are given access by other users. The form of the QR code will vary according to the length of the ciphertext of the OTP code obtained. The data collection method used in this research is literature study by studying journals related to the method that will be used in this research. The methods in question include the RSA algorithm, testing encryption algorithms using the avalanche effect method and application testing using the black box method.

2.2 System Development Methods

Researchers use the prototyping method as a system development method, this method was chosen because it has the advantage of a more flexible and interactive approach in software development. The prototyping method has several advantages for developers, one of which is that it allows developers to create an initial version or prototype of the application to be built. This can help developers to reduce the risk of errors.

2.3 System and Communication Requirements Analysis

Before building a system, an analysis is needed to determine the needs of the user. In this analysis, it is divided into two types, namely functional and non-functional system requirements. Functional requirements are processes or features that can be carried out by the system. Meanwhile, non-functional requirements are behaviors or those possessed by the system being built. The functional requirements of the system that will be built in this research are that the system can create OTP codes randomly, the system can encrypt the OTP code using the RSA algorithm, the system can change the form of the OTP code into a QR code, the system can send QR codes via e-mail, The system can read the QR code sent, the system can decrypt the contents of the QR code using the RSA algorithm. Meanwhile, the non-functional requirements of this application are that the system can encrypt OTP codes quickly, the system can decrypt OTP codes quickly and precisely, the system can maintain the security of messages sent, the system is easy for users to understand.

2.4 Quick Plan and Modeling Quick Design

The application that will be built in this research is the Film Bank application. In general, Film Bank is an application used to order films and add other users as members who can view the films owned by the user who added the member. This application has several features including login, register, Trending, My Film, Plus Member, Validate Member, and Account details.

1. Login

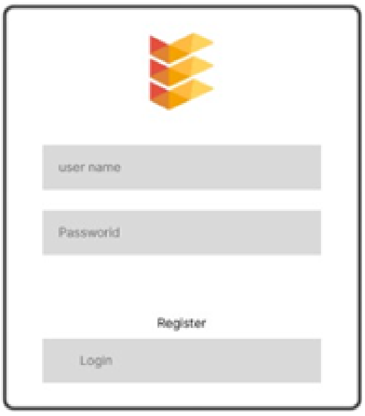


Fig. 1. Login mockup

The login feature is used for registered users to enter the Film Bank application by entering their username and password.

2. Register

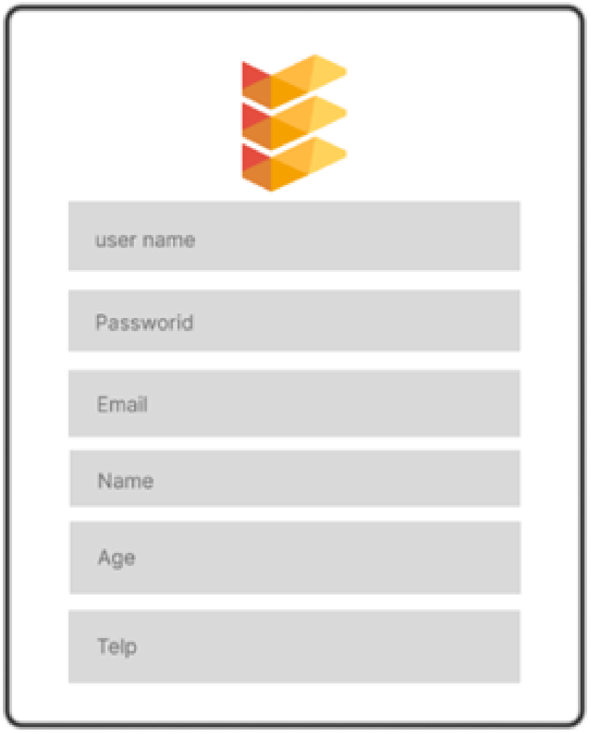


Fig. 2. Mockup register

Register feature is used for users to register their account into the film bank application.

3. Trending

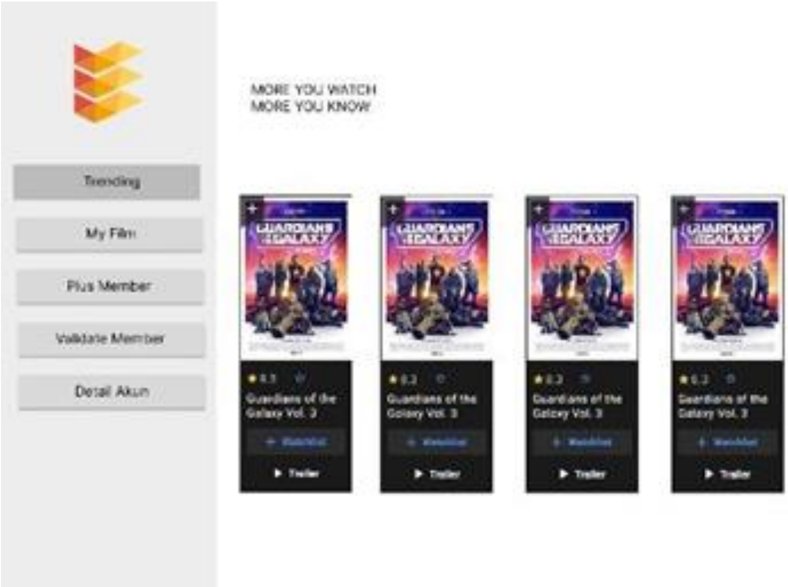

Trending
My Film
Plus Member
Validate Member
Detail Akun
MORE YOU WATCH
MORE YOU KNOW
Guardians of the Galaxy Vol. 3
Guardians of the Galaxy Vol. 3
Guardians of the Galaxy Vol. 3
Guardians of the Galaxy Vol. 3
Watchlist
Trailer

Fig. 3. Trending mockups

Trending feature is a feature that contains films that users can order.

4. MyFilm

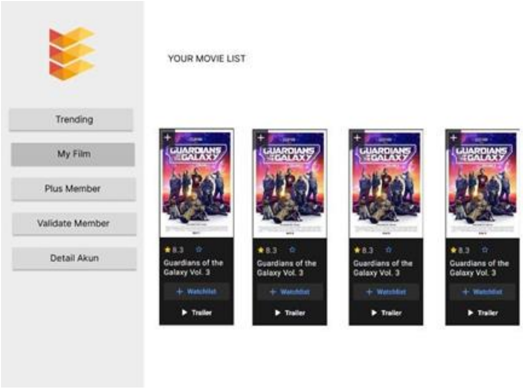


Fig. 4. Mocup my film

This feature is used to view a list of films owned by a user account.

5. Plus Member

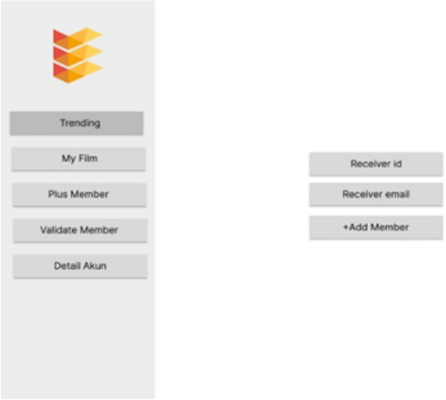


Fig. 5. Mockup plus member

Plus Member is a feature used to add members to an account that has films by entering the user's ID and email.

6. Validate Member

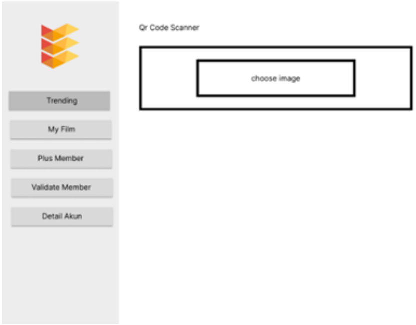
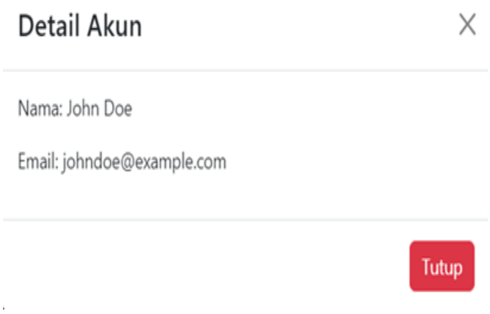


Fig. 6. Validate member mockup

In this feature, users can scan the QR code sent via the email they receive. If the scan is successful, the film owned by the account that provided the QR code will be displayed.

7. Account Details



Detail Akun

Nama: John Doe

Email: johndoe@example.com

Fig. 7. Accounts details mockup

A feature used to view information from an account.

Encryption process:

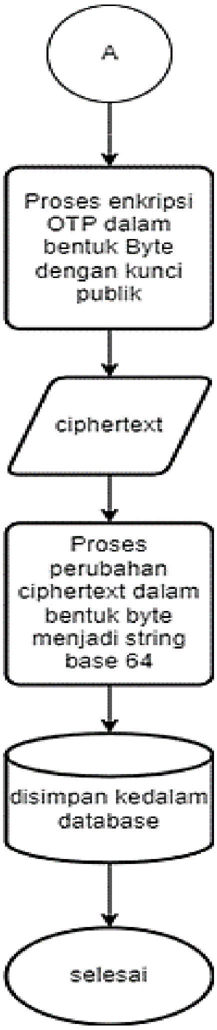
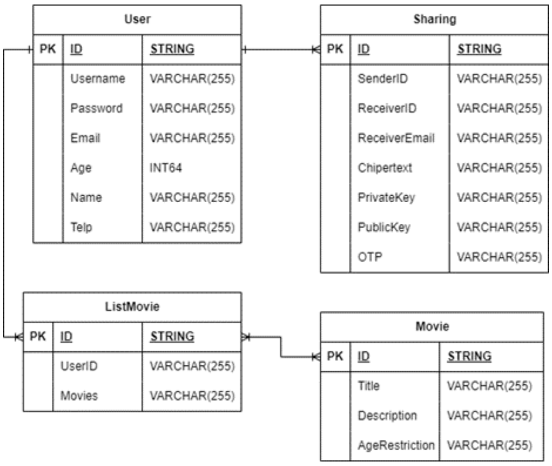

A
Proses enkripsi OTP dalam bentuk Byte dengan kunci publik
ciphertext
Proses perubahan ciphertext dalam bentuk byte menjadi string base 64
disimpan kedalam database
selesai

Fig. 8. Encryption flowchart



User		
PK	ID	STRING
	Username	VARCHAR(255)
	Password	VARCHAR(255)
	Email	VARCHAR(255)
	Age	INT64
	Name	VARCHAR(255)
	Telp	VARCHAR(255)

Sharing		
PK	ID	STRING
	SenderID	VARCHAR(255)
	ReceiverID	VARCHAR(255)
	ReceiverEmail	VARCHAR(255)
	Chipertext	VARCHAR(255)
	PrivateKey	VARCHAR(255)
	PublicKey	VARCHAR(255)
	OTP	VARCHAR(255)

ListMovie		
PK	ID	STRING
	UserID	VARCHAR(255)
	Movies	VARCHAR(255)

Movie		
PK	ID	STRING
	Title	VARCHAR(255)
	Description	VARCHAR(255)
	AgeRestriction	VARCHAR(255)

Fig. 9. ERD film bank

The OTP code that has been generated by the system will undergo an encryption process, for example the OTP code 216322, will be converted into bytes using the ASCII code to [50,49,54,51,50,50]. Then the system creates 2 pairs of keys, namely the private key

Begin:

RSA Private Key:

MIIEpQIBAAKCAQEAs7, and the public key Begin Public Key MIIBIjANBgkqhkiG9w0BA.

The OTP bytes are then encrypted using the public key which produces a ciphertext with [109 231 117 234 215 46 80 239 124]. The ciphertext is then encoded using base64 to get ciphertext data in the form of a string (1HAzhah/FWEec1h+Vw6j34Jt6KQx)

e. ERD Application:

The design of the system flow that is built can be seen through a general program flowchart as below which shows how the overall.

3. RESULTS AND DISCUSSION

3.1 Implementation of Film Bank

The website was built using the React programming language as a display and Golang language for the programming logic of the website that has been built. The appearance of the website follows the application mock-up explained in the previous sub-chapter. The results of the mock-up implementation can be seen in the discussion below:

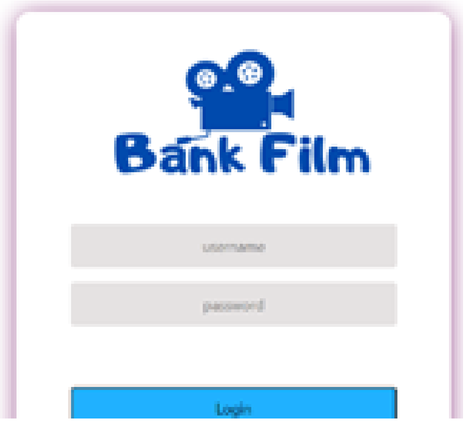


Fig. 10. Login interface

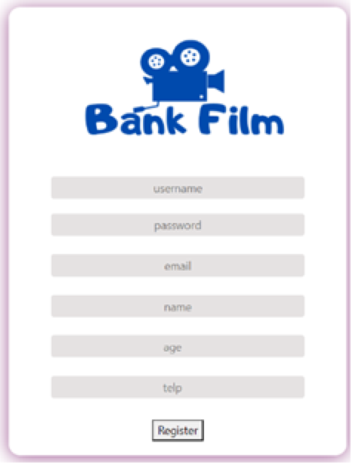
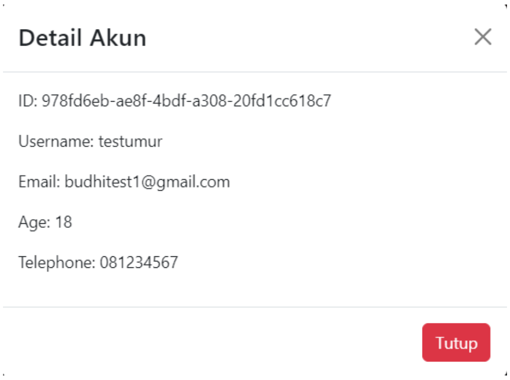


Fig. 11. Register interface



Detail Akun

ID: 978fd6eb-ae8f-4bdf-a308-20fd1cc618c7

Username: testumur

Email: budhitest1@gmail.com

Age: 18

Telephone: 081234567

Fig. 12. Interface account details

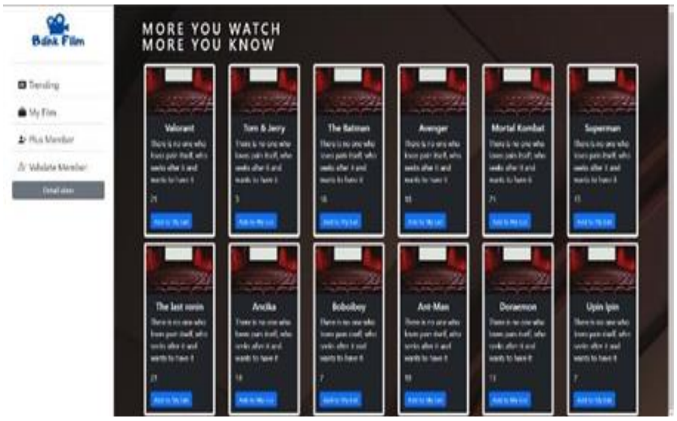


Fig. 13. Trending interfaces

The image above is the user login display, in this display the user must enter the username and password that have been registered in the system to be able to enter the Film Bank website. If the user has not registered an account, the user will not be able to enter the Film Bank website.

If the user doesn't have an account, the user can register their account on the register display as shown in the image above. On the register display, users must enter their username, password, email, full name, age and telephone number to complete their account.

When the user has successfully entered the Film Bank website, the user can see detailed information from the account they have. The information that will be displayed in this detail display is, ID, username, email, age, and telephone. The account details can be seen in the image above.

The image above is the main display or first display that the user will see when the user successfully logs in. In this display there will be information regarding the film title, film description and the minimum age to watch the available films. The films contained in this display can later be added to the user's account.

The next feature is the My Film feature, which can be seen in the image above. In this view, users can see films that have been added to their account. Where the films contained in the My Film display can later be shared with other users via the plus member feature.

The Plus member view is used to add another account as a member who will get access to view films owned by the account that added the account. When a member views a film owned by the account providing access, the films that can be viewed will be adjusted to the age of the member's account. If this member's account does not meet the film's age criteria, this member's account will not be able to view the film.

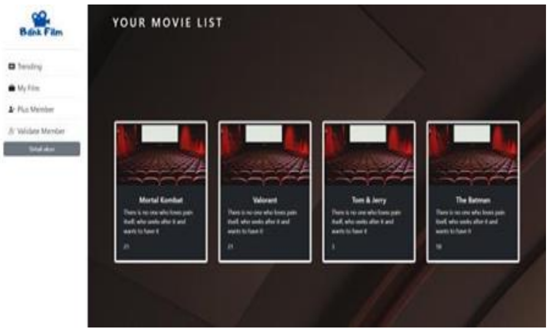


Fig. 14. My film interface

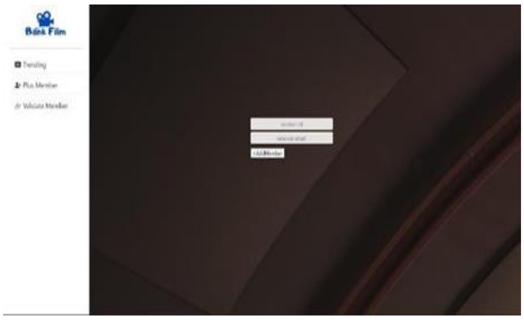
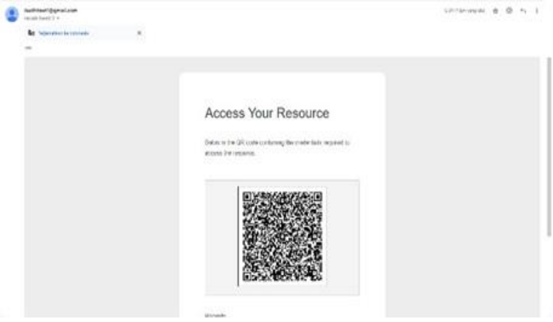


Fig. 15. Plus member interface


Access Your Resource

Below is the QR code containing the credentials required to access the resource.

Fig. 16. QR Code Via mail

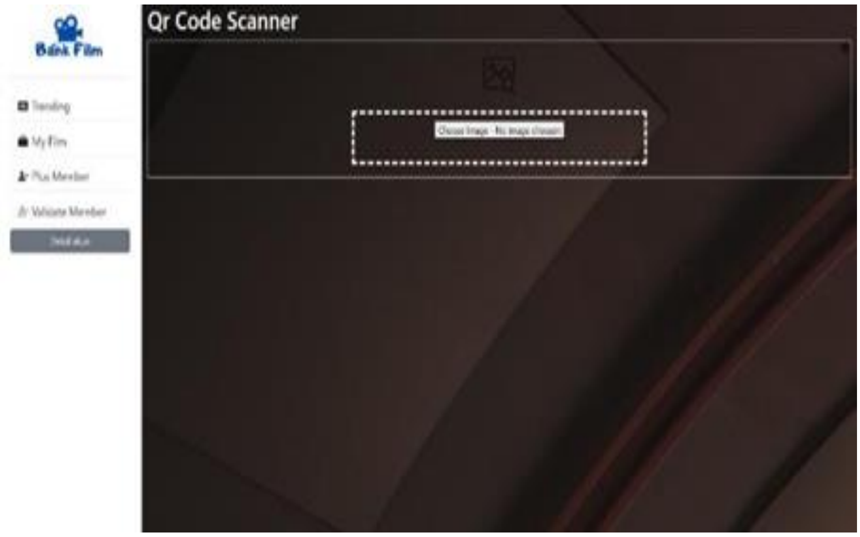
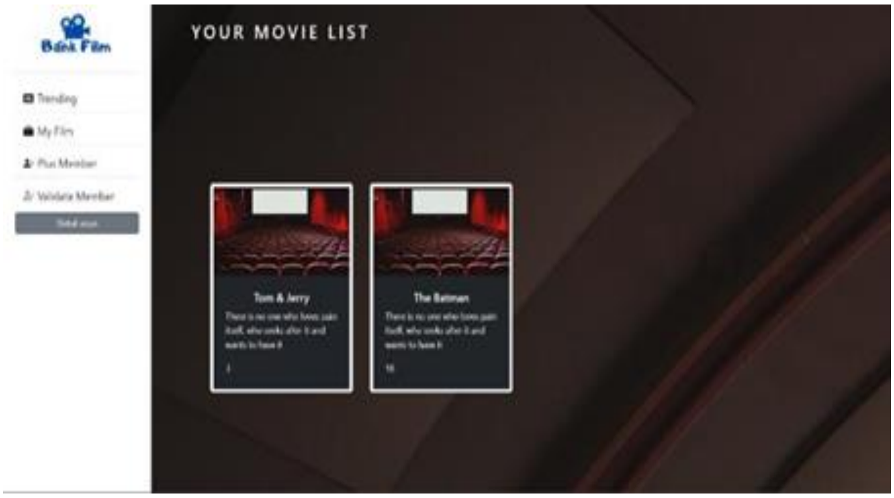


Fig. 17. Validate member interface



Tom & Jerry

There is no one who loves pain itself, who seeks after it and wants to have it

The Batman

There is no one who loves pain itself, who seeks after it and wants to have it

18

Fig. 18. Member film list interface implementation of the RSA algorithm

The image above is the Qr code that members get when the account is added as a member by another user. The content of the QR code is the ciphertext resulting from the encryption of the OTP code generated by the system and can be scanned via the validate member feature on the Bank Film website.

The display in the image above is the Validate member display which is used to scan the QR code sent by the access provider. If the scanned QR code matches the account data of the account added as a member. Then the member validation will be successful and the member can view films according to the age of the member's account. If the validation process is successful, the member validation display will look like the image below.

In this research there are two features that use the RSA algorithm. The function of the RSA algorithm here is to secure the access code so that it can be ensured that the access code is not obtained by unauthorized people. Features that use the RSA algorithm are the member plus and member validation features. In the plus member feature, users are required to enter the ID and email of the destination account they wish to become a member. The purpose of entering id and email is to create and send a QR code. The following is the flow of the plus member feature.

1. Generate OTP, the system will generate a 6 digit OTP code randomly with a number range from 0 to 9. The result obtained from generating this OTP code is 317073.

2. Changing the form of the OTP code into bytes, the 6 digit OTP code obtained in the previous process is then converted into bytes so that the encryption process can be carried out. Converting the OTP code using the ASCII table gets the result [51 49 55 48 55 51].
3. Generate key pair, the system generates a key pair consisting of a private key and a public key. The following are each key generated.

List of Public Key:

MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA1oBXhSPiYPf0
u1435wZqYtE0mKwZ18h4SSkkI16n
axxnpfPsHx/eQ/NnBMwAx+4LOwvX
o87Y9sVxDZd6O4NlklBJFCmruPoA 506OQ9
K3MaLQ+p69p7V1xDc3YUOnUkvV
qRCnDyY0gK81Y0wPOO+0hEjseb7
1l0dHNaWgnq5Vf/J4/FmITOtRLrSp
L4zfqDhv7O7unzFsqLkrIupAonGS2
cwD62k/QyJTkaZSKCmcJtClfLElpB bx
RJh5UcAzGRMosxoZsNiX5j7nuhxi8
oK5vHUi+768jYzND5lxHP/Lf4woSM
szQW+BhjYpw7H8T3J9FifP32bPYkr
di5Ef5M+J+QIDAQAB

List Of Private Key:

MIIEpQIBAAKCAQEA1oBXhSPiYPf0
u1435wZqYtE0mKwZ18h4SSkkI16n
axxnpfPsHx/eQ/NnBMwAx+4LOwvX
o87Y9sVxDZd6O4NlklBJFCmruPoA
506OQ9K3MaLQ+p69p7V1xDc3YU
OnUkvVqRCnDyY0gK81Y0wPOO+0
hEjseb71l0dHNaWgnq5Vf/J4/FmIT
OtRLrSpL4zfqDhv7O7unzFsqLkrIup
AonGS2cwD62k/QyJTkaZSKCmcJtC
lfLElpBbxRJh5UcAzGRMosxoZsNiX
5j7nuhxi8oK5vHUi+768jYzND5lxHP
/Lf4woSMszQW+BhjYpw7H8T3J9Fif
P32bPYkrdi5Ef5M+J+QIDAQABAoIB
AQC/SGZD0bNP++6fpC6/86Wth5ia
yWamWhyCSZDzhbZQu1zmzfXz74
xbFlT5Hx9XKz2So0Xiy1QKBBqEH2
AecFeEudnhhCOh6jgiDZiqfN9nASX
RSPwh8Z0apI7bSuSMbBoWEUaZK
N3LH/PBIBO3F3PoP8u56gPCqwqi
mZf5ycdvN15QBVJOJnVjEb2NY9Id
WW2g6cqyOYiIpfxhdl3bQLyOx2/Ov
foy47NoPEZ13mXKggNgK5Mbv3gaI
7HD9dpIvATaOLgq46HT2Lg/u0mD7
NW4jwh6kgCVXGjZnq8I+YVSyD5W
JJHeMYSGQNjniCxLbwJmIQa1ybxy
3FcttjxTelAxAoGBAOFgVlI+eZ9WjaT
iRZ2JIeDXQVpPNshbckP4l2VfZvGc
TXOX0WmwY4ZOGJ9wk1XnNWYu8
JhRc+l6898QcRy0R6qTn4Z8pfZ3AL
kWEAyftvbA+gc8UvhGAn7FMkH4p
3xDHalPP/oMLxzwVCTXygyZDj/tMlc
9VLJ83wtnyAXqVqPVAoGBAPOluJG
ctbA1SntOaCcD4kQ9ojWvFptfuqK/
NCGkdSW2ZEZZwvV9KxCdwBqeOt
ha4Red+C97P7B+YGWR54fnN9Q2i
e0n49EC/CBVKQ25CSzupKj8Esis/A
gVHSqvLWKin1Tz2G5lJPpFdnEdOU
+GeUYl2NMUPyRGQPoDhcaJ4/OV
AoGBANLeFiXhOl4w11o8MzJQShh
ajlT25KTVmrWp88zvVBwfSAAtPcwL
MzNIApW6+L9ZEodGx+lb3H3Jgj9k
3NAkhSE9+fYUzhsqAM0rrVyCWufI
aqc2c9LDfjYqPvmmst361dfBxHQp
zjLfUXsfQ3ZCBikdvwoM4iAV4YKEW
YvfU6z5AoGBAMoPouznyOo0l+uB
D/FjUDAF6VOaPCZpErBL3+ESsbCv
/aM2Z/ANeTyThzDMDsNFQy3B7YT7
MsudUzaI9ToJMIzHGkXa8h1x20S5
O43M6eYgl+ApBS71/yJ42DKBCyOk
+HyMqe6L5UnFd7/BW7kvLb5WPu
Z3ARKFTPfLGhOYYbqtAoGATXbUys
7C25yZxHkHdgmxBOTgWjfs/hG7ER
lxwDHfdFy8w0SV2IUQzyYa6aHh8i+
CzNdQWKx0d9CMOu91h7UoQncV
NnzL4SGDoKQHLVI/Q+9JFUHbz+IX
QmFDlhPv9TwA2ZVaSHwZh+QS6d
VSfAlHVVDUXh1pV/TuYSRtSYUYoO Y=

OTP byte encryption, OTP bytes are encrypted using the public key. The encryption results of the OTP bytes will produce a ciphertext of the ASCII code byte type. The ciphertext obtained from the encryption process is

```
[212 112 51 133 168 127 21 97 30
115 88 126 87 14 163 223 130 109
232 164 49 203 201 231 88 61 40 33
54 113 0 126 16 153 118 18 134 150
39 92 77 158 93 103 231 240 234 200
22 158 193 68 112 84 221 235 90 220
67 122 61 240 158 54 111 94 210 72
24 121 205 174 78 191 122 230 158
148 71 48 73 220 74 45 39 75 17 112
86 125 40 16 222 230 128 57 185 225
196 60 234 228 110 184 34 231 38
199 43 182 126 40 1 124 30 173 248
74 74 24 141 110 172 172 163 207
209 252 56 74 252 98 205 72 216 252
199 4 41 193 216 85 251 32 206 6 86
189 137 166 135 229 11 243 172 155
97 215 132 107 75 232 64 97 47 75
208 26 7 226 217 26 150 90 219 131
15 82 76 125 163 173 14 58 246 91
155 38 196 219 207 171 254 67 135
82 172 73 127 100 252 155 115 205
229 255 142 56 208 201 193 168 214
45 31 79 30 173 181 151 173 3 219
44 214 156 1 109 102 82 63 41 100
153 87 242 163 70 128 27 241 56 87
170 159 168 230 95 174 22 81 170
125 59 185 98]
```

Encode the ciphertext into base64, the ciphertext resulting from the encryption is then encoded using base64 which aims to change the form of the ciphertext into text or string form so that it can be stored in the database. The encoded result of the ciphertext above is:

1HAzhah/FWEec1h+Vw6j34Jt6Kqxy
8nnWD0oITZxAH4QmXYShpYnXE2
eXWfn8OrIFp7BRHBU3eta3EN6PfC
eNm9e0kgYec2uTr965p6UrzBJ3Eot
J0sRcFZ9KBDe5oA5ueHEPOrkbrgi5
ybHK7Z+KAF8H
q34SkoYjW6srKPP0fw4SvxizUjY/Mc
EKcHYVfsgzgZWvYmmh+UL86ybYd
eEa0voQGEvS9AaB+LZGpZa24MP
Ukx9o60OovZbmybE28+r/kOHUqxJ
f2T8m3PN5f+OONDJwajWLR9PHq 21l60D
2yzWnAFtZlI/KWSZV/KjRoAb8ThXq
p+o5l+uFlGqfTu5Yg==

The ID from the member addition process and the ciphertext that has been converted to base64 will be converted into a QR code. A QR code in the form of a file with the extension PNG will be sent directly to the user's email which has been added previously to the plus member display. The following is a QR code sent via email.

The second feature that uses the RSA algorithm is the validate member feature. This feature uses the decryption process of the RSA algorithm. In this feature, members are required to scan the QR code sent via email. If the scan process is successful, the data obtained is the member addition ID and the ciphertext resulting from the OTP code encryption. The OTP code will be checked first. If the OTP code has not expired, the system will decode using base64 the ciphertext obtained from the scanned QR code. The decoded ciphertext is then decrypted using the private key. The result obtained from this decryption process is 317073. This result is the same as the plaintext or initial OTP code created by the system. This means that the decryption process was successful and the user who validated it is a member who was given access by another user.

Avalanche effect testing: The purpose of this test is to assess how well the encryption system can convert small changes in input into large and random changes in the resulting output. The way this test works is by observing how significant the output changes are resulting from changes in the given input bits. The more unpredictable the resulting input and output patterns, the more difficult it is for attackers to hack or attack the encryption system. The following are the test results of several OTP codes.

Table 1. Avalanche effect testing

OTP code	Average Avalanche Effect
317070	58.59%
317077	57.03%
317071	49.61%
317078	49.22%
917073	48.83%
317003	48.44%
317003	50.78%
387073	41.02%
347973	54.30%
317072	61.72%

The Table 1 is the test results of the OTP code 317073. The step for testing the avalanche effect is to change one bit of the plaintext or in this research, namely the OTP code. Next, a comparison of the ciphertext bits from the first plaintext and the ciphertext bits from the changed plaintext is carried out. After getting the comparison results in the form of the number of different bits from the two ciphertexts, then the number of different bits is multiplied by the length of the ciphertext multiplied by 100%. From 10 tests carried out with randomly changed OTP codes, it was found that the average percentage obtained from the avalanche effect test results was 51.9%. From the average obtained, it can be said that the system is good at securing messages. Because a change of 50% can result in problems that are quite difficult for irresponsible parties to solve.

Black-box testing: Black-Box testing here focuses on the functional specifications and external behavior of the software. In this functionality test, the system's capabilities will be tested by carrying out processes defined in the analysis of the needs and features provided by the application being built.

Table 2. Functional specifications and external behavior of the software

No	Scenario	Description	Expected results	Test result
1	Login	Login with the registered username and password	Users can enter the system	Users can enter the system
		Login with the wrong username or password	Users cannot enter the system and get an indication that the username or password is incorrect.	Users cannot enter the system and get an indication that the username or password is incorrect.
2	Registration	Users register	User has successfully registered	User has successfully registered
3	Added My Movies	Users add trending available films to the my films list	The film data has been successfully added to the user's My Film list	The film data has been successfully added to the user's My Film list
4	View the My Films list	Users see a list of films in My Film	Users can see a list of films they own in the My Film feature	Users can see a list of films they own in the My Film feature
5	Adding members	User adds user ID and user email	Users who have been successfully added as members	Users who have been successfully added as members
		User added wrong ID and email	Users get a notification that ID and Email are not available	Users don't get unavailable notifications
6	Member validation	Users validate by scanning the QR code file	Users are directed to the My Films feature with a list of films from the sender's account	Users are directed to the My Films feature with a list of films from the sender's account

4. CONCLUSION

Based on the results obtained from this research, it can be concluded that the Film Bank application design is able to implement the RSA cryptographic algorithm in securing user login data in the form of an OTP code. From the results of the research carried out, it can be seen that the system can carry out the encryption process well starting from the process of creating a 6 digit OTP code, creating a public key and a private key. After the system encrypts the OTP code, the system can change the form of the encryption results into a QR code that is ready to be sent to the recipient via e-mail. The system can also carry out the decryption process well as evidenced by the success of the system re-decrypting the ciphertext sent via e-mail and getting the same results as the OTP code sent by the user for the first time.

The quality of the system in carrying out encryption can be said to be of good quality which is the result of the avalanche effect test carried out on the OTP code obtained. In this test, the OTP code used was 317073. From 10 experiments carried out by changing one random character from the OTP code used, an average avalanche effect of 51.9% was obtained. In a literature study regarding the avalanche effect, it is explained that an avalanche effect system above 45% can be categorized as a good system, because it has caused problems that are quite difficult for attackers to solve. The functional quality of the system that has been built can also be categorized as good looking at the results of the black-box testing that has been carried out.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Changsong W, Kerry L, Marta RF. Film distribution by video streaming platforms across Southeast Asia during COVID-19. Media, Culture and Society. 2021;43(8): 1542–1552.
2. Diana DI. Case study of pornography addiction in adolescents. Motiva Journal of Psychology. 2018;1(2):56. Available:https://doi.org/10.31293/mv.v1i2.3688
3. Fauzi A, Maulita Y, Pardede AM. Hybrid cryptosystem analysis of RSA and triple dec algorithms. Kaputama Information Engineering Journal (JTIK). 2017;1(2).
4. Harahap MK, Khairina N. Analysis of the one time pad algorithm with the transposition cipher algorithm as text message security. Informatics Engineering Journal & Research. 2018; April 1:58–62.
5. Sulaiman A, Krisnadi I. Security management using access control based on roles in the organization; 2016.
6. Suntoro A. Wiretapping and the existence of the corruption crime commission supervisory board. Indonesian Journal of Legislation. 2020;17(1):25. Available:https://doi.org/10.54629/jli.v17i1.627
7. Susanto AE. Text message security with encryption and decryption method using RSA algorithm (Rivest Shamir Adleman) based on android. 2023;3(2):1–16.
8. Sylfania DY, Juniawan FP, Laurentinus L, Hengki H. Securing E-complaint messages for academic community facilities and performance using the RSA algorithm. Journal of Information Technology and Computer Science. 2022;9(6): 1203. Available:https://doi.org/10.25126/jtiik.2022965388
9. Tampubolon A. Implementation of a combination of the RSA algorithm and DES algorithm in text message security applications. SAINTIKOM Journal (Journal of Information and Computer Management Science). 2021;20(1): 38.
10. Wiyono N, Hardjianto M. Email security using the RSA algorithm and mobile-based SHA-1 digital signature. Ipsikom. 2016; 4(2):1–11.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the publisher and/or the editor(s). This publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/123574