VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

PROJECT REVIEW 1

FALL SEMESTER 2020-21

CSE3501-INFORMATION SECURITY ANAYSIS AND AUDIT

TOPIC: HYBRID CRYTOGRAPHY [RSA+DES]

SLOT: G2

TEAM MEMBERS:

LOGA RAKSHIKA . B 18BIT0430

LYDIA CHRISLIN PAUL 18BIT0439

SARADHA DEVI T 18BIT0447

SUBMITTED TO : Dr. SUMAIYA THASEEN I

DONE BY: LOGA RAKSHIKA .B

LITERATURE REVIEW:

PAPER 1: Enrichment Of Information Security By Building New Hybrid Algorithm Using Expanded Rsa, And Des Cryptosystem

1.MOTIVATION:

We all know , we are storing the data digitally on the internet. Many companies store their data on the cloud. the data may be confidential also. We need security for the data that is saved on the cloud. The security is commonly done by using most traditional encryption technique. The most important part of encryption is key generation . nowadays, hackers easily get the key with help of high end computational techniques. To provide further security with complexity they go for a concept of hybrid cryptography using rsa ans dsa algorithms.

2.ALGORITHM:

They used DES to encrypt data, then the private key is being encrypted by using our expanded RSA algorithm for more data security. The reason behind using DES symmetric algorithm is that it takes less amount of time in cryptographic operations compared to asymmetric algorithm.

Extended-prime RSA is a variation of RSA in which the modulus is the result of in excess of two particular primes. The upside of Extended-prime RSA over standard RSA lies with the expansion of numbers of prime, this will strengthen the security process . The encryption procedure is also modified to strengthen the standard of RSA.

3.PSEUDOCODE:

Key generation:

Phase 1: Let F,G,H,I represents a large prime number
Phase 2: The product n=F*G*H*I and phi (n) = (f-1) (g-1) (h-1) (i-1).
Stage 3: Select e with a definitive target that (e, phi(n)) are overall co-prime.
Stage 4: Pick out two whole figure j and k to such an extent, to the point $j=ke_2$.
Stage 5 Solve e= sqr(j/k)
Stage 6: Find d by utilizing the recipe e*d = 1 mod (phi(n)).

Encryption: $C=M^e \bmod (n)$ whose public key is (n, e).

Decryption: Use the private key (n, d) to compute calculate plaintext: $M=C^d \bmod (n)$

4.PERFORMANCE ANALYSIS:

Simple RSA	DES WITH EXPANDED RSA
Brute force attack is possible	Efficient against brute force and timing attack.
Exponent size cant be increased over 1024 bits	Exponent size increases beyond 1024 bits.

PAPER 2:] Hybrid encryption model for data security in cloud environment

1.MOTIVATION:

This system focuses on giving more security for the data that is stored on the cloud . though cloud computing offers many benefits , it has hazards at the security level also. Data threats like breaches , loss are the serious challenges. The big challenge here is that , the cloud user is not aware that his data is being used or managed by some other party. To solve this problem , they have used a combination of encryption algorithm – rsa -des-blowfish model .

2.ALGORITHM:

The encryption is done by rsa , des , blowfish algorithms. The keys generated are rsa public and private key ,blowfish secret key and des secret key. The data file is first encrypted using blowfish key , the output is encrypted with des key , then the output from that is encrypted with rsa public key.

The decryption also uses those 3 algorithms. The system uses private rsa key to decrypt the blowfish and dsa keys. 1st the decrypt the des key and the des . and that output is decrypted with blowfish decrypted key.

3.ARCHITECHTURE:

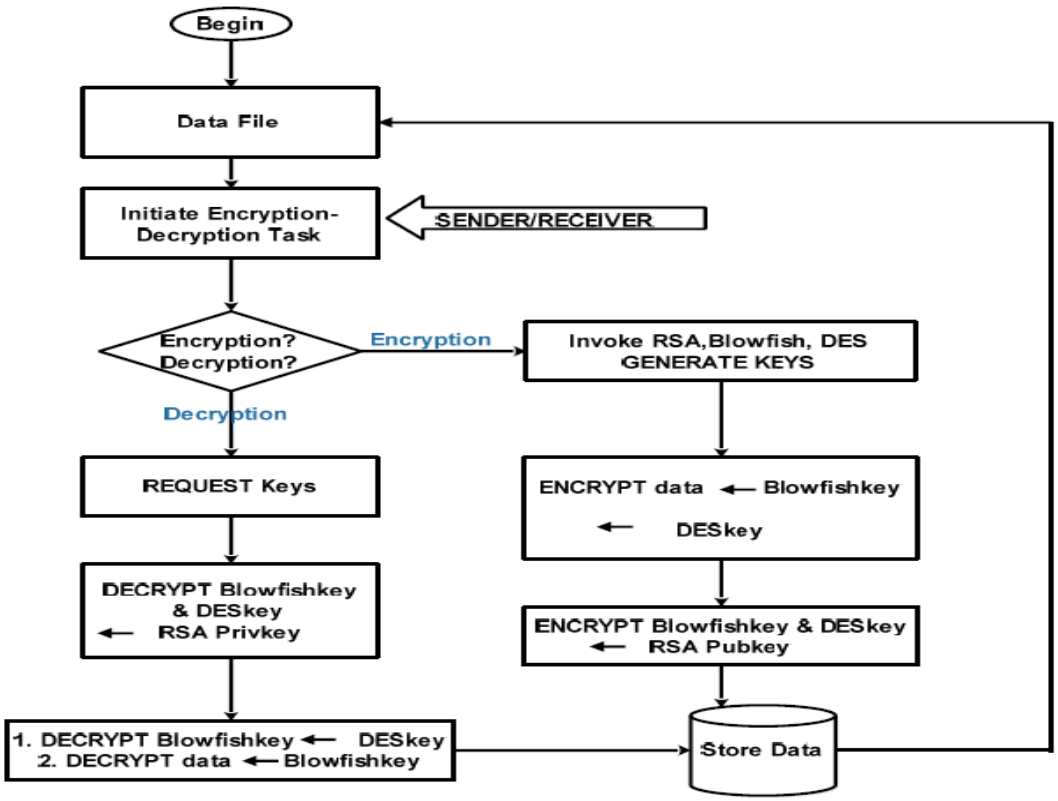


Fig. 6. A 3-tier hybrid model encryption-decryption process

4.PERFORMANCE ANALYSIS:

Factors	2 TIER RSA-BLOWFISH	3-TIER RSA-BLOWFISH-DES
Encryption decryption time	Less	Slight more than 2 tier
Change in input size	After encryption, slightly increasing in thesize of data .	Increase in data size due to double encrytion
Security	Vulnerable to attacks	Stronger encryption due to encryption of file first with blowfish before des and blowfish keys are encrypted with rsa will result in hybrid of longer keys that are hard to break

PAPER 3: Enhancing Cloud Computing Security using Cryptography & Steganography Dheyab Salman Ibrahim

1.MOTIVATION:

This paper focuses on enhancing cloud computing security using cryptography and stenography. There are lots of security issues in cloud environment . the most common issue is the unauthorized access. The attacks can be both passive and active . the drawback here is that , the user do not know where the data is kept and which machines achieve the computing jobs. Threats may be eavesdropping ,intrusion ,dos attacks , session hijacking and so on. So they try to solve this using hybrid cryptography and stenography.

2.ALGORITHM:

This system is designed in such a way that it maintains the security of the text file alone.

For encryption they first implement DES and generate perform first level encryption. After that , they implement RSA as a second level encryption. Then , they perform LSB algorithm in stenography for 3rd level security. Then , they upload a file and the cipher text is stored in database.

For decryption, they read the cipher text from database and perform all the three inverse algorithms. They get the plain text and its displayed to the user.

3.ARCHITECTURE:

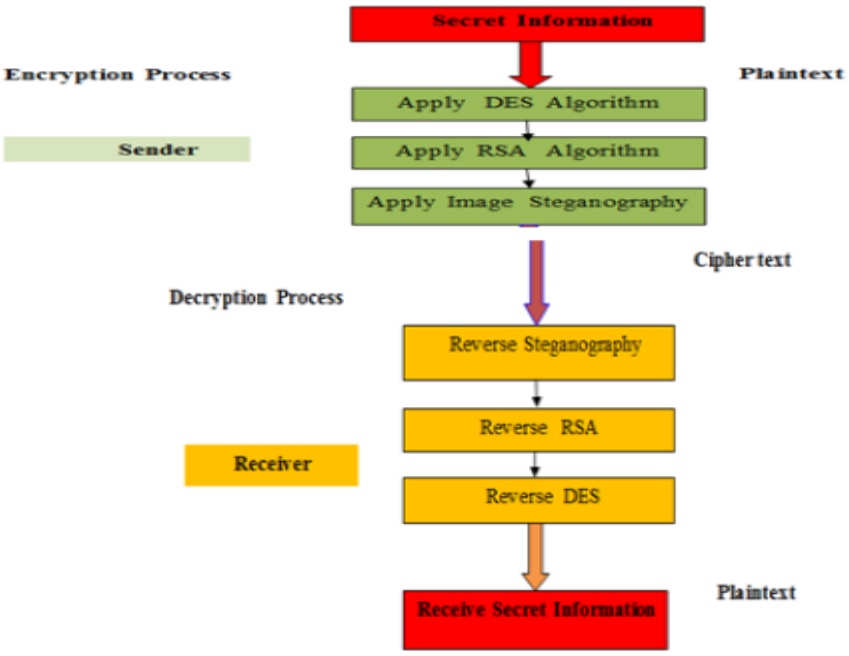


Figure (8) Overall system design

4.PERFORMANCE ANALYSIS:

Hybrid method made the system encryption and decryption stronger.this combination of symmetric and asymmetric increases the efficiency .the one who knows all the 3 key can alone access the data . by this way , this system provides the confidentiality only to the owner by default. Hence , by this way they increased the security.

Factors	Handled method
Data confidentiality	comparing it with another data encrypted by DES , AES which uses the one key to encrypt/decrypt data. Use RSA only, or LSB. In our proposed system , do not have any access to personal data in cloud, employed three levels of security**.**
Performance	Increased performance when using integrated RSA-DES rather that using single level encryption
Security	As we used stenography , the data is much more secure and provides abstraction to the owner of the data, which is not in case , if we apply only cryptography. Hence, stenography helped in proving security.

PAPER 4: Message Security Using RSA-DES Hybrid Cryptography

1.MOTIVATION:

Nowadays , most of the message are transmitted over the internet. During transmission , there are chances of integrity loss or data loss or many other network attacks . though we encrypt the message using encryption methods , the hackers are able to get the original message. To make the security far better , we use combination of cryptography.

2.ALGORITHM:

It starts with the obtaining of the first user public key. And then the fresh symmetric key is generated and we can encrypt the message using the newly formed key. With the use of first user public key we can encrypt the symmetric key and can send both of the encryption to first user.

Next process is the decryption of the message which happens when the first user uses his personal secret key to decrypt the symmetric key and with which the first user can use symmetric key to decode the encrypted information.

RSA and DES are combined together and modified . RSA is used to perform key encryption and DES is used for data encryption.

3.ARCHITECTURE:

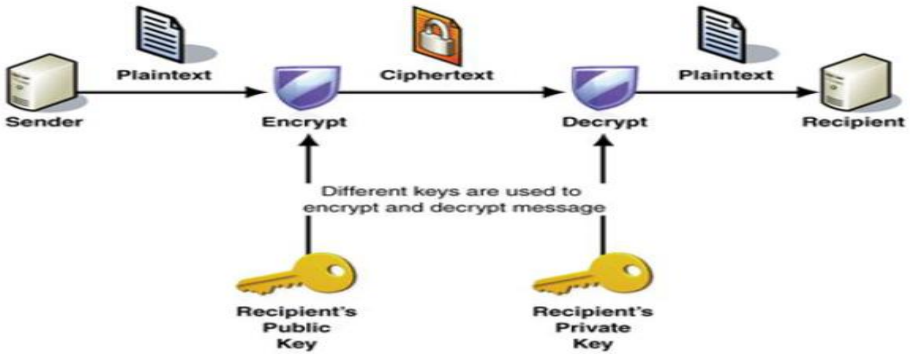


Figure 1: Asymmetric Encryption

4.PERFORMANCE ANALYSIS:

	RSA-AES		RSA-DES	
TEXT SIZE	TIME (S)	MEMORY(Kb)	TIME (S)	MEMORY(Kb)
512	303	54840	269	37614
256	295	52460	252	33580
56	264	32550	273	35589

Among the various combination of symmetric and asymmetric algorithms, RSA and DES hybrid cryptography work better in terms of time and memory consumption. The key generation time and ciphering time is very less compared to RSA-AES . Hence ,this provides enhanced security to the system .

PAPER 5: An Information Security Technique Using DES-RSA Hybrid and LSB

1.MOTIVATION:

To provide security to the data , there are various methods . one such is hiding the original data behind the picture/image. This can be achieved by cryptography and stenography. This generates secret messages such that the hackers cant see it .for the cryptography purpose , we use RSA-DES hybrid cryptography.

2.ALGORITHM:

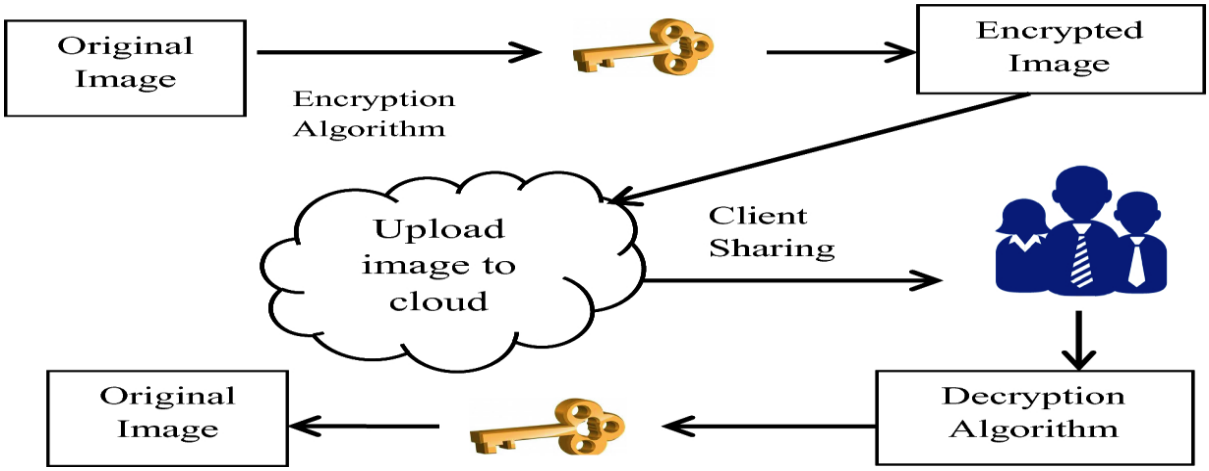
The system is designed by using RSA ,DES, LSB.

We encrypt the message using DES algorithm . then we choose 2 prime numbers for RSA key generation. We encrypt the DES key using public key of RSA . the cipher text obtained from DES and RSA is shuffled among themselves to represent a hybrid of ciphertexts.

After obtaining the hybrid of cipher text, it is hidden inside a image using LSB algorithm/technique. Then , its ready for transmission.

For decryption , we decrypt using keys of LSB and extract DES,RSA keys and we perform decryption.

3.ARCHITECTURE:



4.PERFORMANCE ANALYSIS:

Factors	DES	RSA	DES+RSA
RESPONSE TIME	FAST	SLOW	FAST
SECURITY	WEAK	HIGH	HIGH
SCALABILITY	WEAK	WEAK	STRONG
PRACTICALIBILITY	WEAK	WEAK	STRONG

The system is strong because , no one can identify the secret behind the cryptography and it is difficult to break through. This system avoids brute force attacks .it is more secured than the existing system . the feature of using stenography adds more security to the data .

REFERENCES:

[1] Enrichment Of Information Security By Building New Hybrid Algorithm Using Expanded Rsa, And Des Cryptosystem Abdulganiyu A.[1*], Hammawa M.B.[2] and Owolabi O.[2] (2018)
http://www.lajans.com.ng/articles/LAJANS%203(1)183%20-%20190.pdf

[2] Hybrid encryption model for data security in cloud environment.(2018)
K.Ntshable ,B.Isong ,T.Moemi,N.Dladlu,N.Gasela
Department of computer science,north-west university,Mafikeng , South Africa
https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/GCC3304.pdf

[3] Enhancing Cloud Computing Security using Cryptography & Steganography
Dheyab Salman Ibrahim(2019)
https://pdfs.semanticscholar.org/508c/c5d25fcf03a9debddec2107f9cd532e89e7e.pdf

[4] Message Security Using RSA-DES Hybrid Cryptography
Dr. Sheetalrani R. Kawale *Assistant Professor, Dept. of Comp. Sci., KSAWU, Vijayapura, Karnataka, India Corresponding Author: Dr. Sheetalrani R Kawale*

http://www.iosrjournals.org/iosr-jce/papers/Vol21-issue2/Series-2/B2102020710.pdf

[5] An Information Security Technique Using DES-RSA Hybrid and LSB
1 Sandeep Singh, 2Aman Singh 1Department of Computer Science Engineering, Lovely Professional University, Phagwara, Punjab, India 2Assistant Professor, Department of Computer Science Engineering, Lovely Professional University, Phagwara, Punjab, India
https://www.researchgate.net/publication/278329872_An_Information_Security_Technique_Using_DES-RSA_Hybrid_and_LSB