IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 3, Ver. I (May. - June. 2018), PP 17-23
www.iosrjournals.org

Delineation of Trivial PGP Security

Mr. Nikhil Joshi[1], Mr. Gaurav Kumar[2],
Prof. Divya Premchandran Asst Professor[3],
[1]*mca Student, Bvimit Cbd Belapur, Navi Mumbai.*
[2]*mca Student, Bvimit Cbd Belapur, Navi Mumbai.*
[3]*mca Bvimit Cbd Belapur, Navi Mumbai.*
Corresponding Author:Mr. Nikhil Joshi

Abstract: *The enhanced PGP Security that we are proposing is based only for digital signatures & encryption/decryption of the messages. The algorithm that is used here consists of asymmetric algorithm as RSA 4096 & the symmetric algorithm used is AES-256(Advance Encryption standard). Also we require hashing function in order to secure the digital signature as well as messages. Hence we use Whirlpool hashing function which is open source & is based on 512 block cipher that makes the application more powerful than the previously used.*

Keywords: *-Asymmetry algorithm, AES-256, Digital Signature, Hash Function, OpenPGP , PGP, RSA 4096, Rijndael Cipher, SHA-256, Symmetric algorithm, Whirlpool.*

Date of Submission: 07-05-2018 Date of acceptance: 26-05-2018

I. Introduction

The process of creating & maintaining digitalsignature along with encryption/decryption of messages is widely known & used in PGP. Various symmetric algorithms like DES, Triple DES, Twofish & IDEA along with hashing functions like MD5, SHA-1, SHA-256 has been introduced to provide a stronger encryption technique.

The key exchange policy RSA 4096 is still considered the best asymmetric algorithm so far. Although being so strong in their encryption technique it is still slower & weaker compared to the newly concept that we are going to introduce is AES-256 & Whirlpool.

II. Literature Survey

The main purpose of introducing the concept of whirlpool hashing function is to explain that, apart from other hashing functions, whirlpool has larger cache memory which provides higher performance with greater throughput. Also with its long hash length, this provides increased protection against various attacks.

AES-256 is chosen as the symmetric algorithm for encryption purpose that is well better than its predecessors DES & 3-DES giving excellent security & protection against future attacks like (collision attacks & potential quantum computing algorithms) that would have 264 complexities with 128-bit key & could become viable in the lifetime of the data.

Few of the tools of software are where whirlpool & AES is already used are:

GoAnywhere MFT: which includes OpenPGP compliant encryption to address the privacy and integrity of data. OpenPGP is an industry standard that uses asymmetric (public key) cryptography for providing a high level of data protection, making PGP one of the most popular encryption methods used today.

Whirlpool is implemented in cryptographic programs like FreeOTFE & Trucrypt in 2005.

Also Veracrypt(a basis of Truecrypt) used whirlpool as the final version of supported hashing algorithms.

7z, Amanda Backup, PeaZip, PKZIP, RAR WinZip & UltraISO are few of the applications developed based on AES standard.

III. Digital Signature

The PGP provides authentication of messages through hashing function & asymmetric algorithm. The message is hashed using the hashing function like MD5, SHA-1 etc. to create a message digest & then encrypted using any asymmetric key algorithm like RSA, DSS or Diffie Hellman.

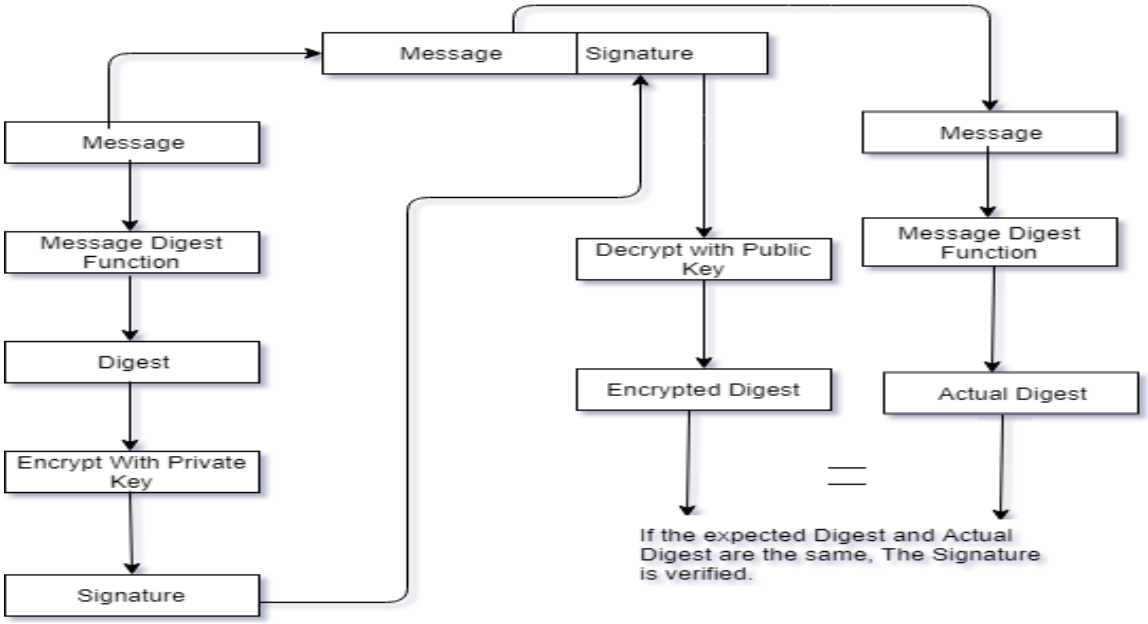

Fig.3.1 Digital Signature

The simple process that PGP follows is that, whenever the senders creates a new message, a hashing function is used togenerate the hash code of the message. Further, this hash code is encrypted with asymmetric key algorithm using the sender's private key & thus the result is pretended to the message.

Now on the receiver end, the receiver uses the asymmetric algorithm that was used by the sender & using sender's public key to decrypt & get the hash code.Further, the receiver generates a new hash code for the given message & compares it with the decrypted hash code. If the comparison between the both is true, then it accepts the message as authenticated

IV. RSA 4096

RSA is used as asymmetric key cryptography algorithm which is used in sharing information using private & public key between sender & receiver. Despite having its original version of RSA 1024 bits, it was easily attacked & seems to be somewhat breakable. So the RSA version of 2048/4096 shall be more reliable to be used.

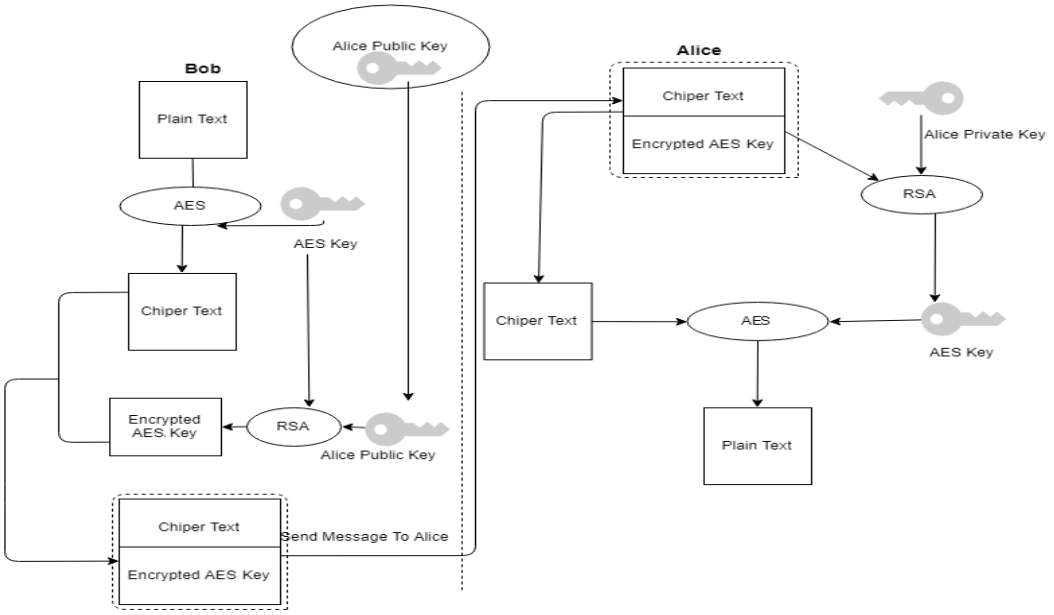

Fig.4.1 RSA 4096
Simple working process:-

Senders Side

The original message is generated by the sender along with one time random session key only valid for that particular message. Now the message is encrypted using any of symmetric key algorithm like IDEA, DES or Triple DES. RSA is then used to encrypt this session key using the receiver's public key.

Receiver Side

On the receiver end, the receiver uses same asymmetric algorithm with its own private key to decrypt & recover the session key & then session key is used to decrypt the message.

RSA is basically used to encrypt the session key as it is not feasible to encrypt the entire message. For message encryption, several symmetric key algorithmsare used.

V. Whirlpool

Whirlpool is a hash designed after the Square block cipher, and is in family of block cipher functions. It takes a message of any length less than 2^256 bits and returns a 512-bit message digest.Although whirlpool being built based on AES, it can only be used as hashing function.

The complete digest is created in following steps:

1. Padding: Message is padded in odd multiple of 256 bits.
2. Message length: The length of the existing unpadded message is appended to the message.
3. Hash matrix initialization: The result of hash is stored in 8*8 matrix.
4. Block cipher: The block cipher processes the message in 512-bit blocks.

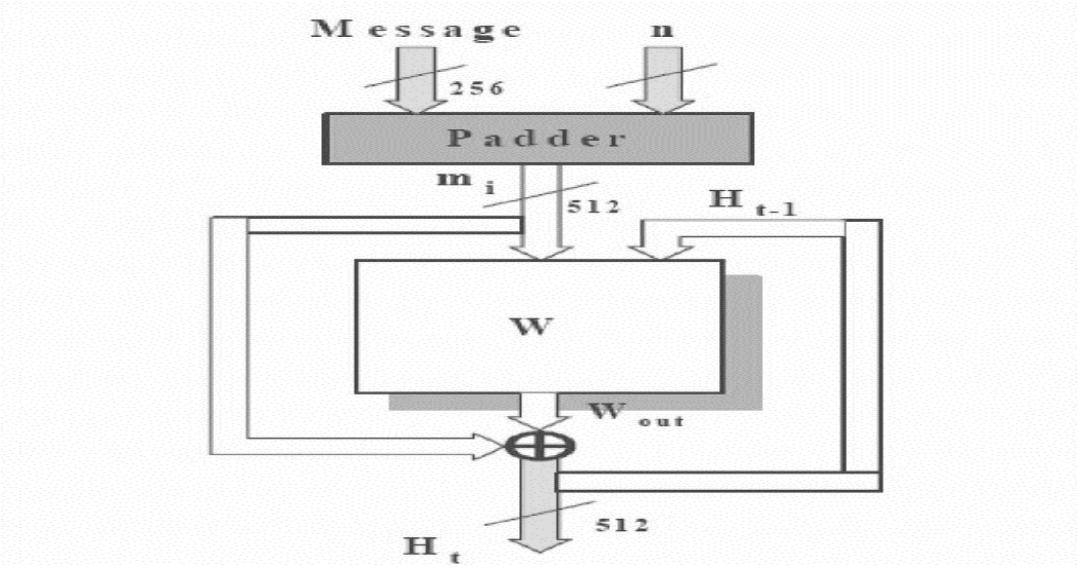

Fig 5.1. Generation of Whirlpool Digest

Structure:

The encryption algorithm 512-bit key as input & 512-bit plaintext blocks& produces 512-bit cipher text as output.

It consists of four form of functions or transformation:

1. Add key
2. Substitute bytes
3. Shift columns
4. Mix rows

There are in total 10 rounds that Whirlpool cipher performs all above functions for every round.

The algorithm can be expressed as:

W (K) = (O RF(Kr)) * AK(Ko)

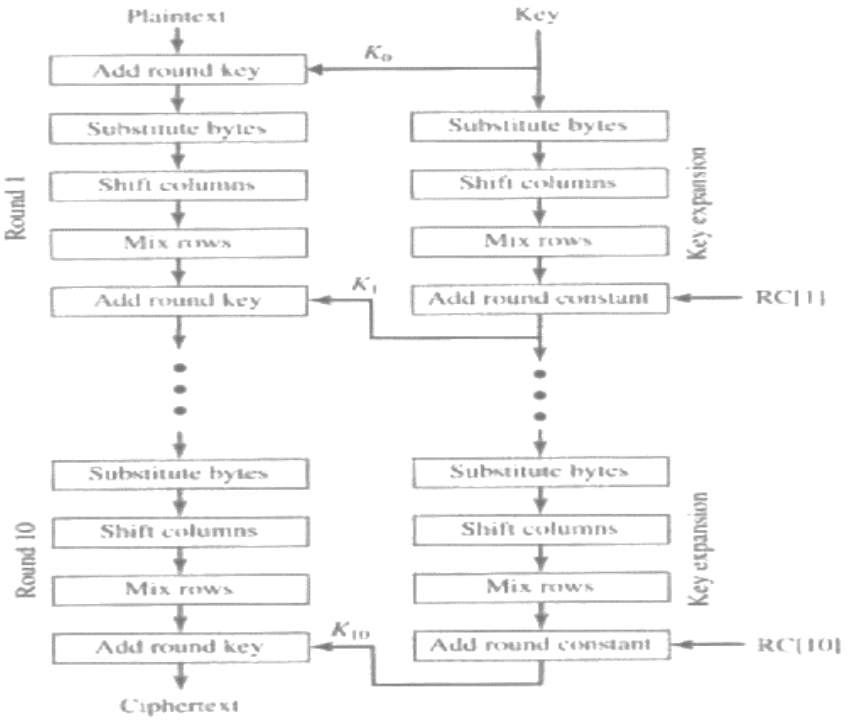

Fig.5.2 Whirlpool Cipher

As seen in the diagram above, at first time, key is used as input to initial AK function. For rest of the rounds from round 2 till 10 previous hash value is used as key i.e. output of first round is used as key for next round & so on.

VI. AES-256

The Rijndael cipher -- a mash of the Belgian creators' last names Daemen and Rijmen -- was selected as the proposed algorithm for AES in October 2000 and published by NIST as U.S. FIPS PUB 197.

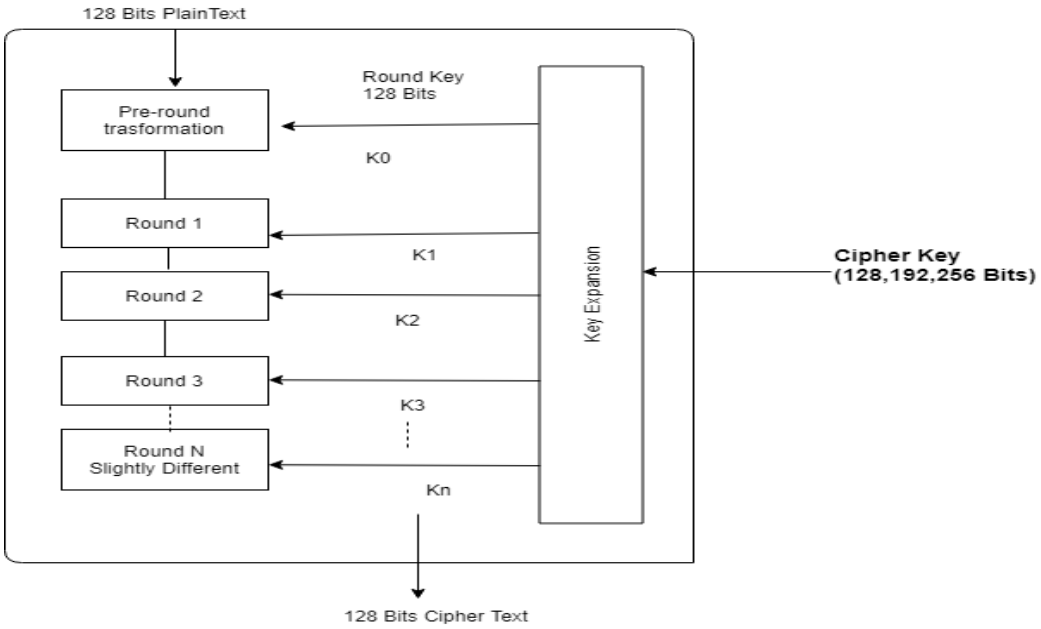

Fig. 6.1 AES Structure

AES is considered to be stronger than its predecessors – DES/Triple DES as it uses longer key lengths & also has faster encryption technique with low latency & higher throughput. It is considerably used in firewalls & routers & in protocols such as SSL, TLS & can be used in many modern applications.

There are series of linked operations of which it comprises; where some involve replacing inputs by specific outputs i.e. substitutions & rest involve shuffling bits around i.e. permutations.
Also called as substitution-permutation network.

The computation of AES is performed on bytes rather than bits. It treats the 128 bits of a plaintext block as 16 bytes so as to arrange them in four rows & four columns for processing as a matrix.

Process:

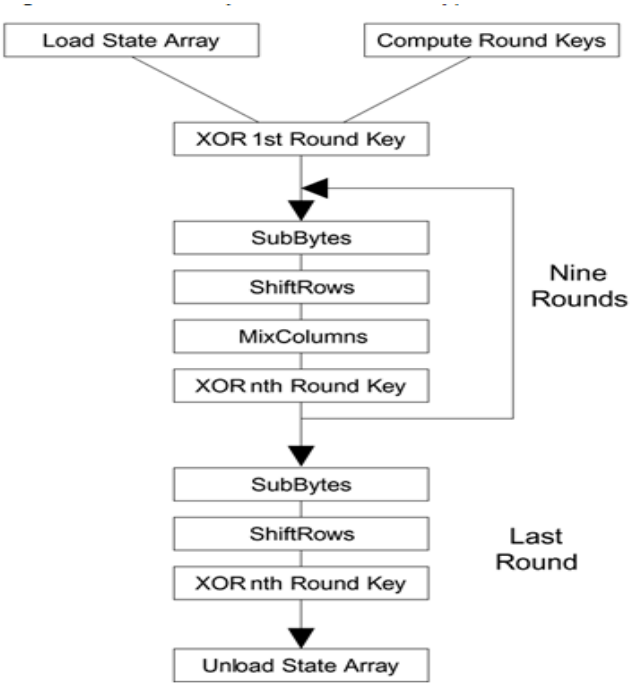

Fig. 6.2 AES Transformations

Step 1:- Byte Substitution

Substitution of the table is done at first stage, where 16 input bytes are substituted by looking up at fixed table. This result would be in four rows & four columns.

Step 2:- ShiftRows

Each of the four rows of matrix is shifted on left side. Any entries after that are reinserted on the right side of row. It is done in following manner:-
- First row remains unchanged.
- Second row is shifted one byte to the left.
- Third row is shifted two positions to the left &
- Fourth row is shifted three positions to the left

Now, we get a new matrix consisting of same 16 bytes but shifted with respect to each other.

Step 3:- Mix Columns

In this process, four bytes of column is transformed using special mathematical function. This functions takes input as four bytes of one column & outputs four completely new bytes by replacing the original column. This creates a new matrix consisting of 16 bytes. Mix Columns is not performed in last round.
The 16 bytes of the matrix are now considered as 128 bits and are XOR-ed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Step 4:- AddroundKey

The 16 bytes of the matrix is now considered as 128 bits & XOR-ed with 128-bits round key. Now this output of 128 bits is taken as 16 bytes & will continue for second round and so on. Once it reached the last round the output is the ciphertext.

VII. Proposing A Model

There are various hashing functions, symmetric & asymmetric algorithms used so far for encryption of the messages. For instance, SHA-1, SHA-2 etc. for hashing techniques & DES,3DES,IDEA, Twofish etc. as symmetric key algorithm.

Here, we propose a more sufficient & reliable hashing technique & encryption algorithm which is faster & stronger compared to the previous algorithms used.

We use whirlpool hashing function as our hashing algorithm which is of 512 block cipher & only be used for hashing. Along with it we use AES-256 as symmetric encryption algorithm. As the name implies, it is considered to be stronger than its predecessors – DES/Triple DES as it uses longer key lengths & also has faster encryption technique with low latency & higher throughput.

Also one of the reasons in using whirlpool is that, the clock cycles required for transforming each block is 10 cycles which is lesser compared to the clock cycles required in SHA 256 is 64 cycles.

RSA 4096 is used as asymmetric encryption algorithm and remain unchanged due to the
Stronger technique it follows.

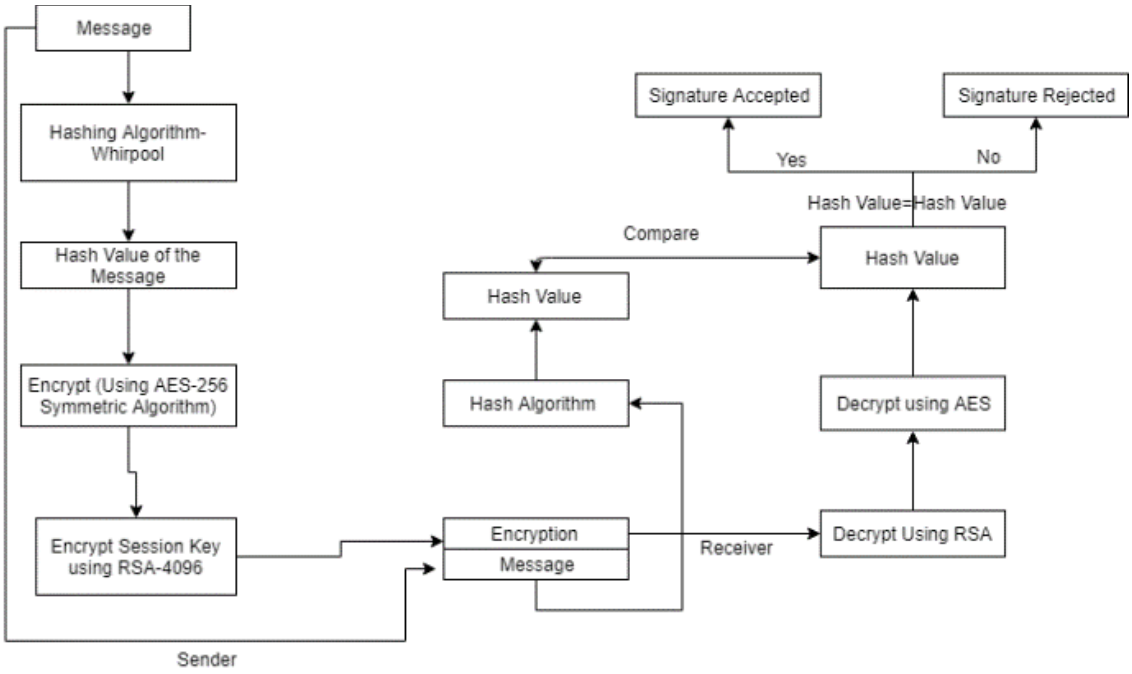

Fig. 7.1

Process:

On the Sender Side:-

1. The sender first signs the message i.e. digital signature by using Whirlpool hashing function.
2. Next step in the process it does is to encrypt the message with a session key i.e. by using AES-256 cryptographic algorithm.
3. Finally, in the last process it encrypts the session key using recipient's public key i.e. RSA 4096
4. Now the original message is pretended with Session key & sent across to receiver.

On the Receiver Side:-

1. The receiver will decrypt the message using RSA 4096 i.e. own private key.
2. Next, this one time session key is decrypted using AES-256 & hash value is obtained.
3. Finally, this hash value is compared with the hash value which gets generated by computing hash value of original message arrived at receiver If both matches, then the message is accepted or rejected.

VIII. Conclusion

The whirlpool is a promising function as it can do only hashing but, it does it well. It is faster on platforms with plentiful resources while also can be scale well to hardware level. It has been detected as collision free & can be recommended to be used in future. AES-256 as name suggest advance encryption technique works great with whirlpool as it is designed by one the same author of whirlpool.

Using both can provide a stronger & faster hashing & encryption technique along with RSA 4096 for a mini PGP application for greater efficiency & better outcome.

References

[1]. Rijmen, V. with Willia Stallings. Private communication September 9th, 2005.
[2]. Barreto, P. and V. Rijmen. 2003. The Whirlpool Hashing Function. Submitted to NESSIE, May.
[3]. P. Kitsos, O. Koufopavlou: "Efficient Architecture and Hardware Implementation of the Whirlpool Hash Function". IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, Feb. 2004
[4]. Zimmermann, "An Introduction to Cryptography", PGP v 6.0 documentation, 1998.
[5]. Alex Biryukov and Dmitry Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, ".

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Mr. Nikhil Joshi "Delineation of Trivial Pap Security." IOSR Journal of Computer Engineering (IOSR-JCE) 20.3 (2018): 17-23.