Symmetric Key Cryptography: Technological Developments in the Field

Md. Sarfaraz Iqbal
Student
Department of CSE
Amity University, Noida, India

Shivendra Singh
Student
Department of CSE
Amity University, Noida, India

Arunima Jaiswal
Asst. Professor
Department of CSE
Amity University, Noida, India

ABSTRACT
This paper presents the various developments and emerging trends in the symmetric key cryptography technique. It provides an overview of latest inventions and approaches that are implemented in the recent scenario for the betterment of private key cryptography technique with respect to its efficiency, effectiveness, etc.

General Terms
Safety, Key, Hiding, Symmetric, Stream, Block, Security, Algorithms.

Keywords
Cryptography, cipher, encryption, decryption, symmetric key.

1. INTRODUCTION
Today we send many confidential information across the internet, like, account information, credit, debit card details. The list is endless. These information are important to us, hence they demand protection or security from being compromised. Here arises the need of some technique that protects our information. Cryptography is the study of techniques that are implemented to establish a secure communication in which no information is compromised. One type of cryptography is using symmetric key technique. Symmetric key cryptography is a cryptography technique that uses same key or public key for encrypting the information as well as decrypting it back to the original form. The key, here, can also be understood as the shared secret between the two parties among which the transfer of information is taking place.

2. SYMMETRIC KEY CRYPOGRAPHY

2.1 Overview
Symmetric key cryptography or private key cryptography, in layman language can be understood as the technique which uses a single key for the encryption as well as the decryption of data. Technically, it is a technique which converts plaintext into cipher text and vice verse using the same key. The symmetric key cryptography system involves the following [1]:

- **Plaintext:** original information that is fed as input to the algorithm.
- **Encryption algorithm:** algorithm which performs various permutations and substitutions on the plaintext
- **Secret key:** also an input to the encryption algorithm, changing the key results in the generation of different output.
- **Cipher text:** statement in which the actual information is hidden.
- **Decryption algorithm:** reverse of the encryption algorithm; produces the original information.

There are two requisites for the symmetric key cryptography:

- We need not keep the algorithm secret; but instead the key should be kept secret.
- Sender and receiver must have obtained copies of the secret key in a secured way and must keep the key safe.

2.2 Types
- Stream cipher: encrypt the bytes of the information one at an occasion.
- Block cipher: take number of bits and carry out encryption on them as a solitary unit.

2.3 Implementation
Some popular symmetric key cryptographic algorithms are 3DES, CAST5, AES, RC4, Serpent, Twofish, Blowfish, and IDEA.

3. LITERATURE SURVEY
There has been a lot of research in the field of symmetric key cryptography. Some are related to the advancement in the field whereas some are a part of increasing its effectiveness on the present scenario.

Fiskiran et al (2005) [2] discusses the workload characterization of five widely-used symmetric key ciphers that rely heavily on table lookups in their round structure. Paper also describes the new **ptlu** instruction to accelerate and parallelize the table lookup.

Elbirt et al (2005) [3] discusses the mapping of block cipher algorithms to the COBRA architecture and implementing them. This paper also verified that COBRA architecture attains resourceful realization of a wide range of block ciphers while considerably out-performing the software implementation.

Erguler et al (2008) [4] presented two protocols based on the symmetric key cryptography which solved the problem of offline dictionary attack from which LDH protocol suffers.

O'Melia et al (2008) [5] proposed the instruction set extensions for improving the software implementations of symmetric key algorithms. The instructions had a significant positive effect on the execution time, logic utilization, clock frequency.

Kholidy et al (2008) [6] discussed about the "HIMAN" middleware which demonstrated that every time the file size is large then by7 selecting the right size of block and suitable thread number can result in accelerating the schema performance.

Chen et al (2010) [7] presented a comparison between symmetric key cryptography and other approaches. It showed that symmetric key, hash function and MAC algorithms are comparatively far more efficient than the asymmetric key equivalents.

Fan Wu et al (2010) [8] presented a technology in proficiently performing symmetric key cryptography using GPU instead of CPU for faster implementation and a significant performance improvement.

Chatterjee et al (2011) [9] presented a new symmetric key algorithm using extended MSA method: DJSA symmetric key algorithm. Its advantage is that it is almost impossible to break without its key matrix being compromised.

Gaspar et al (2011) [10] proposed a principle which allows general purpose processors to operate with secret keys in a highly secure way. It is abase on the formation of split processor, cipher and key zones. This was implemented on FPGAs and testing was done using NIOS II, MicroBlaze, Cortex M1 processors.

Debajan Das et al (2011) [11] presented an integrated Symmetric key algorithm using Generalized modified Vernam cipher method which the called DJMNS symmetric key algorithm. Complexity of the method ensured that decryption of data becomes impossible by any brute force.

Roy et al (2011) [12] proposed an improvisation in symmetric key cryptography using the DNA based strong cipher. Under this method the cipher text was again passed through DNA mechanism to obtain the final cipher text.

Niraj Kumar (2011) [13] presented a new technique for generation of symmetric key of an image based data. Cryptographic concepts like key generation, encryption, decryption of images through MATLAB and analysis were presented in it.

Roy Nandi et al (2011) [14] presented the PCA based symmetric key block cipher algorithm. Complexity of PCA algorithm is O(n x m) where n is the half of the group order of CA and m is total number of blocks.

3.1 Summary of literature review

Table 1. Author wise addressed issues in their papers

Author name	**Issue addressed**
A.Murat Fiskiran et al [2]	Parallel table look up
Adam J. Elbirt et al [3]	Instruction –level distributed processor
Imran Erguler et al [4]	Password based key establishment protocol
Sean O'Melia et al [5]	Instruction set extensions
Hisham A. Kholidy et al [6]	Enhanced "ULTRA GRIDSEC"
Lanxiang Chen et al [7]	Comparison between public key and symmetric key cryptography
Fan Wu et al [8]	Accelerating symmetric key cryptography using GPU
Dripto Chatterjee et al [9]	DJSA symmetric key cryptography
Lubos Gaspar et al [10]	Secure extensions of FPGA soft core processor
Debanjan Das et al [11]	DJMNA symmetric key algorithm
Bibhash Roy et al [12]	DNA based strong cipher
Niraj Kumar et al [13]	Symmetric key cryptography for an Image
Satybrata Roy et al [14]	Application of Cellular Automata

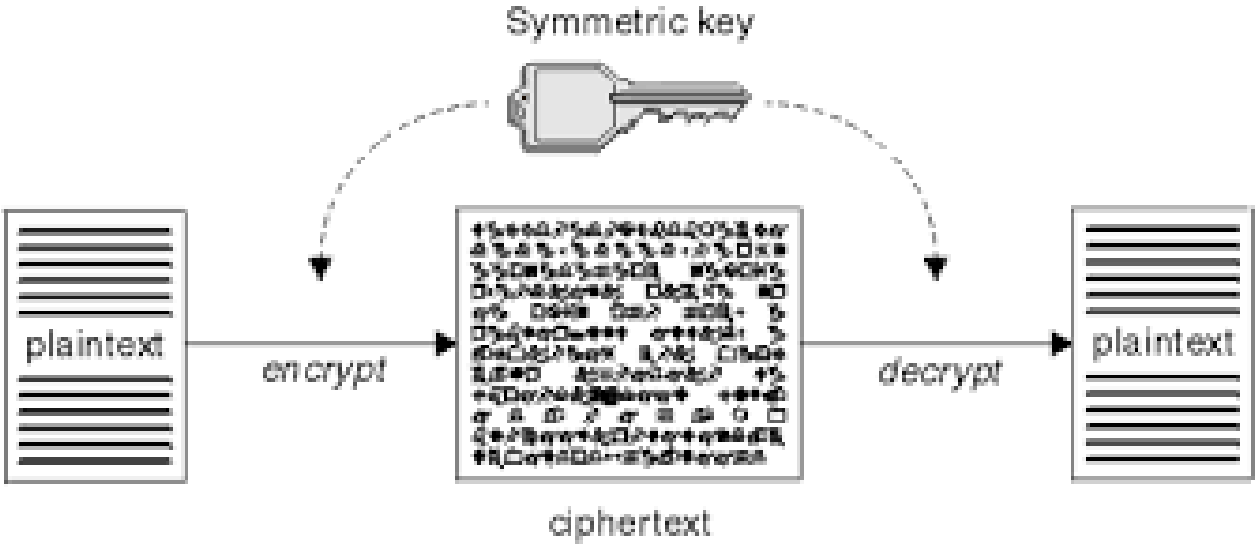

Fig 1: Symmetric key cryptography mechanism

4. ADVANTAGES & DISADVANTAGES

Like all the rest the symmetric key cryptography technique also has its share of advantages and disadvantages.

4.1 Advantages

Following are the advantages of symmetric key cryptography

4.1.1 Extremely Secure: One of the most widely-used symmetric key encryption systems is Advanced Encryption Standard. It would take about a billion years for a 10 petaflop computer to guess the key through a brute-force attack. 256-bit AES is essentially unbreakable.

4.1.2 Relatively Fast: One of the short comings of public key encryption is that they require relatively complex mathematics to work, making them very computationally intensive. On the other hand, symmetric key data is relatively easy to do. Many SSDs, which are typically extremely fast, use symmetric key encryption internally to store data and they are still faster than unencrypted conventional HDDs.

4.1.3 In Symmetric key Cryptography systems, encrypted data can be transferred even if there is a chance that the data will be intercepted. As there is no key transmitted along with the data, the possibility of data being decrypted is null.

4.1.4 The symmetric key cryptography system uses password authentication to check the receiver's identity.

4.1.5 The system having the secret key can only decrypt the message.

4.2 Disadvantages

Following are the disadvantages of symmetric key cryptography:

Sharing the key: one of the main difficulties with symmetric key encryption is that we have to find a way to get the key to the party with whom we are sharing data. With this in mind, symmetric key encryption is particularly useful when encrypting your own information as opposed to when sharing encrypted information.

4.2.1 More damage if compromised: If someone gets on a symmetric key, they can decrypt everything encrypted with that. When we're using symmetric encryption for two-way communications, this means that both sides of the data get compromised.

4.2.2 It cannot endow with digital signatures that cannot be repudiated

5. CONCLUSION

This paper attempts to review major researches and developments occurred in Symmetric key cryptography in the past decade and also recognizes various advantages and disadvantages of Symmetric key cryptography over other cryptographic techniques. Symmetric key cryptography or private key cryptography, in layman language, can be understood as the technique which uses a single key for the encryption as well as the decryption of data. This paper provides an overview of latest inventions and approaches that are implemented in the recent scenario for the betterment of private key cryptography technique with respect to its efficiency, effectiveness, etc.

6. ACKNOWLEDGMENTS

We would like to thank Arunima Jaiswal from Amity School of Engineering and Technology for the useful discussions we had with her at the beginning of the paper and for the constant guidance she has provided us with throughout the completion.

7. REFERENCES

[1] Computer Networks and Computer Securtiy by Kartik Krishnan, Lecture 22-24, 2004

[2] Fast Parallel Table Lookups to Accelerate Symmetric-Key Cryptography by A.Murat Fiskiran and Ruby B.Lee, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) 0-7695-2315-3/05 $ 20.00 IEEE.

[3] An Instruction-Level Distributed Processor for Symmetric-Key Cryptography by Adam J. Elbirt, Member, IEEE, and Christof Paar, Member, IEEE, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 16, NO. 5, MAY 2005

[4] A Password-based Key Establishment Protocol with Symmetric Key Cryptography by Imran Erguler and Emin Anarim, IEEE International Conference on

Wireless & Mobile Computing, Networking & Communication, 978-0-7695-3393-3/08 $25.00 © 2008 IEEE DOI 10.1109/WiMob.2008.112

[5] Instruction Set Extensions for Enhancing the Performance of Symmetric-Key Cryptography by Sean O'Melia ∗ , Member, IEEE, and AJ Elbirt † , Member, IEEE, 2008 Annual Computer Security Applications Conference, 1063-9527/08 $25.00 © 2008 IEEE DOI 10.1109/ACSAC.2008.10

[6] Enhanced "ULTRA GRIDSEC": Enhancing High Performance Symmetric Key Cryptography Schema Using Pure Peer To Peer Computational Grid Middleware (HIMAN) by HIsham A.Kholidy, Abdulrahman A.Azab, Safia H.Deif, 978-1-4244-2020-9/08/$25.00 02008 IEEE

[7] The Comparisons between Public key and Symmetric key Cryptography in Protecting Storage Systems by Lanxiang Chen, Shuming Zhou, 20IO International Conference on Computer Application and System Modeling (ICCASM 2010), 978-1-4244-723 7-6/10/$26.00 .2010 IEEE

[8] An Efficient Acceleration of Symmetric Key Cryptography Using General Purpose Graphics Processing Unit by Fan Wu, Chung-han Chen, and Hira Narang, 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies, 978-0-7695-4095-5/10 $26.00 © 2010 IEEE DOI 10.1109/SECURWARE.2010.24

[9] A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm by D. Chatterjee, J.Nath, S. Dasgupta, A.Nath, 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE DOI 10.1109/CSNT.2011.25

[10] Secure extensions of FPGA soft core processors for symmetric key cryptography by Lubos GASPAR, Viktor FISCHER, Lilian BOSSUET, Robert FOUQUET, reference.

[11] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm by Debanjan Das1, Megholova Mukherjee2, Neha Choudhary3, Asoke Nath4, 978-1-4673-0126-8/11/$26.00 c 2011 IEEE

[12] An improved Symmetric key cryptography with DNA based strong cipher by Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta, 978-1-4244-9190-2/11/$26.00 ©2011 IEEE

[13] An Efficient and Effective Lossless symmetric Key cryptography algorithm for an Image by NIraj Kumar, reference

[14] Application of Cellular Automata in Symmetric Key Cryptography by Satyabrata Roy, Subrata Nandi, Jayanti Dansana, Prasant Kumar Pattnaik, International Conference on Communication and Signal Processing, April 3-5, 2014, India, 978-1-4799-3358-7114/$31.00 ©2014 IEEE