International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

Secured Encryption: A Proposed Algorithm based on Combination of SHA-1 and Rijndael Encryption Algorithm

Jyoti Mahajan
Department of Computer Engineering, Govt. College of Engineering. & Technology, Jammu, India
Email address: jmahajan1972@gmail.com

***Abstract*—**The present world of internet communication is facing the problem of data theft that are predominantly made during the online communications. So there arises a need of providing a more secured mechanism of data communication. This paper proposes a secured algorithm formed by the combination of SHA1 and the Rijndael encryption algorithm.

***Keywords*—** Cryptography; Encryption; Hash; Symmetric Key; Asymmetric Key.

I. INTRODUCTION

The technique of protecting the information by encrypting it to get cipher form so that it can't be readable by unauthorized user. With the gradual evolution of technology from ancient days to modern times several innovative form of encryption methodology have been developed, extensively used and then discarded after brilliant insight into new cryptanalytic methods [1]. In this cryptography the message which is in plain text format is converted into cipher text, this process of converting plain text into cipher text is called as encryption. And the reverse process of this i.e. converting cipher text into plain text is called as decryption. Many cryptography algorithms are applied for achieving encryption and decryption. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

Cryptography systems can be classified into: "symmetric-key systems'' that use a single key that both the sender and recipient have, and key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses

A. Symmetric Key Cryptography

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. While in case of public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them. Symmetric key encryption provides secrecy when two parties, say Alice and Bob, communicate. An adversary who intercepts a message should not get any significant information about its contents [2].

Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption overcomes this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric key ciphers are implemented as either block ciphers or stream ciphers.

B. Asymmetric Key Cryptography

Two keys are used in asymmetric cipher (e.g., RSA)—a public and a private one. RSA is an algorithm for public - key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [3]. The public one is available for everyone, but the private one is known only by the owner. When the message is encrypted with the public key, only the corresponding private key can decrypt it. Moreover, the private key can't be learned from the public one. Asymmetric cipher solves the problem of secure key distribution. Alice takes Bob's public key and uses it to encrypt the session key. Only Bob can then decrypt the encrypted session key, because he is the only one who knows the corresponding private key. Asymmetric ciphers are quite slow when compared with the symmetric ones, which is why asymmetric ciphers are used only to securely distribute the key. Then, Alice and Bob can use symmetric cipher and the session key to make the communication confidential. Use of an asymmetric cipher also solves the scalability problem. Everyone will need only one public key and one private key to communicate with other people. In the real world, symmetric and asymmetric –key cryptography techniques are used in combination. They are used in digital envelopes which proven to be sound technology for transferring message from the sender to the receiver, achieving confidentiality [4].

C. Hash Algorithms

A hash function is simply an algorithm that takes a string of any length and reduces it to a unique fixed length string [4]. Hashes are used to ensure data and message integrity, password validity as well as the basis of many other cryptographic systems. Each hash is unique but always repeatable. That means that the word 'cat' will hash to something that *no* other word hashes too, but it will *always* hash to the same thing. The function is 'one way'.

Jyoti Mahajan, "Secured encryption: a proposed algorithm based on combination of SHA-1 and Rijndael encryption algorithm", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 223-226, 2015.

II. EXISTING SYSTEMS

The existing systems involve the use of various cryptography algorithms like AES, DES, MD5 etc. Blowfish, which has a long key (448 bit), outperformed other encryption algorithms. DES and 3DES are known to have worm holes in their security mechanism, Blowfish and AES do not have any so far [5]. The algorithms used for this paper work are SHA1 and Rijndael.

A. SHA1

SHA stands for Secure Hash Algorithm it use o generate the message digest this message digest is the condensed form of representation of the message .The SHA1 is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required [6]. This verifying of digital signature is done on both the receiver and the sender end by the use of SHA1 technique. Whenever there is an input of length less than or equal of 2^64 bits as input the condensed representation in the form of 160-bits as output the message digest is generated. The message digest can then be input to the Digital Signature Algorithm (DSA), which generates or verifies the signature for the message. In this instead of message the message digest is signed which improve the efficiency of the process. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature. The best part in this is that SHA1 is most secure and the reason behind this is that it is infeasible to find two different messages which produce thesame message digest.

B. Rijndael

DES stands for Data Encryption Standard this is created by U.S National Bureau of Standards which offer another way to encrypt the data, this was replaced by Rijndael encryption. This Rijndael name was derived from the name of the two person who are the author of this method they are John Daemon and Vincent Rijmen, they are two Belgian cryptology expert. This method provides the protection against the brute force attack by using the key of varying size of 128, 192, or 256 bits. This encryption is three times more efficient and faster than the DES. This is mostly used in the exchanging key securely. IN USA the top secret government document uses the AES-256.

Because of government standardization on this algorithm, it is expected to become a widely used replacement for the DES, although ASP.NET still relies heavily on DES and 3DES. However, Rijndeal is the default algorithm that fully runs in managed code [6].

Table 1 shows the comparative encrypted text generated by SHA1 encryption and Rijndael encryption.

Table 1. Comparative encrypted text generated by SHA1 encryption and Rijndael encryption.

Plain Text	**Encrypted Text**	
	SHA1 Encryption	**Rijndael Encryption**
hello	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	kNWQ7/I=
cryptography	48c910b6614c4a0aa5851aa78571dd1e3c3a66ba	my8N+G3wV+e2WujE
computerscience	527cc8f50577e3fcef568c23ec1cbae6cc117cd3	mzI1uuSHI7nwcryaACOj
government	1785a93e5a968f37278f64cef35098943f62b438	n9xzBYuEhwM/JQ==
working on project	fdfa440e7adfb8641a1896a53316c4f664b8faac	jx54wGKLzTLS4mXJmiobKx79
encryption program	4d363064ee3a1a9ec60d0a64137c8256d04dfff9	nXbOP8/SMFcpujmizN35pHBy
Hello	aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d	kNWQ7/I=
cryptography	48c910b6614c4a0aa5851aa78571dd1e3c3a66ba	my8N+G3wV+e2WujE
computerscience	527cc8f50577e3fcef568c23ec1cbae6cc117cd3	mzI1uuSHI7nwcryaACOj
government	1785a93e5a968f37278f64cef35098943f62b438	n9xzBYuEhwM/JQ==

III. PROPOSED SYSTEM

Here in this section we would like to propose a new algorithm which could be used for encryption. This proposed algorithm is constructed with the combination of the Rijndael and the SHA-1 encryption algorithm. This algorithm uses a 256 bit encryption key. Plain text is provided as the input and in return the algorithm produces a base64-encoded result. Also it involves the use of different parameters which are listed below:

1. *Passphrase*: Passphrase can be any fixed string. Here we assume it to be an ASCII string.
2. *Saltvalue*: Saltvalue can be any fixed string. Here we assume it to be an ASCII string. Together Saltvalue and Passphrase combine to generate the password
3. *hashAlgorithm*: hashAlgorithm is the variable which holds the name of the hash algorithm to be used for generating the password.the possible values of hashAlgorithm are MD-5 and SHA-1. SHA-1 is bit slower than MD-5, but more secured than MD-5. Hence we have considered SHA-1 for our algorithm.
4. *Password iterations*: Password Iteration is the user-defined runtime variable which decides the number of iterations to be given to the password .It's value is different for different plaintext.

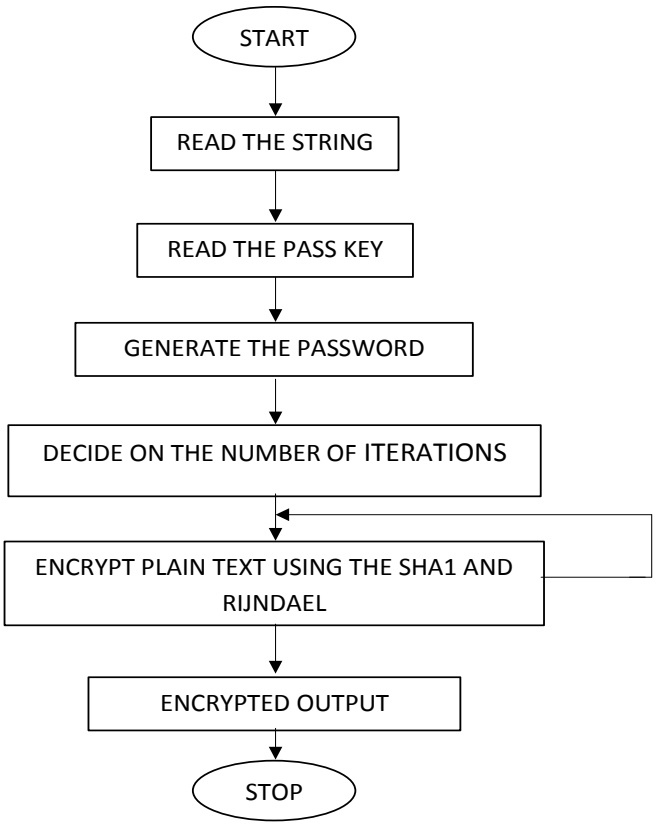
Jyoti Mahajan, "Secured encryption: a proposed algorithm based on combination of SHA-1 and Rijndael encryption algorithm", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 223-226, 2015.

5. *initVector*: This represents the initialization vector and its value is used to encrypt the first block of plaintext. For this algorithm initVector must have 16 ASCII long value.
6. *keySize*: The variable keySize indicates the size of the key to be used for encryption.
7. Larger the key size greater would be the security. Here we have used key of size 256.

Table 2. Comparative encrypted text generated by the proposed algorithm for different iterations.

Plain Text	Encrypted Text		
	Iteration=2	Iteration=4	Iteration=8
Hello	cAOPjUqZWhazI3BKbDK0OA==	UBGW0psbDm0cPAIcZj+Cnw==	X+D6j5ETrAjATlwgUhlC9Q==
cryptography	exSakVH9Nm/ZWBM4Yz27Nw==	WwaDzoB/YhR2R2FuaTCNkA==	VPfvk4p3wHGqNT9SXRZN+g==
Computer science	ewmOkVDmNG/LSxIkCVraMg==	WxuXzoFkYBRkVGByA1fslQ==	VOr7k4tswnG4Jj5ON3Es/w==
government	fwmVhFf8PHjWXH1HYT+5NQ==	XxuM24Z+aAN5Qw8RazKPkg==	UOrghox2ymalMVEtXxRP+A==
working on project	bwmRikz8Nj3XRlsxFVbVVs04yLhITJ23ga9Zc797Ex4=	TxuI1Z1+YkZ4WSlnH1vj8VGBL54seCIZI5vgP0Za8Vk=	QOrkiJd2wCOkK3dbK30jm57heYpJDcDKzn4oJGrrHWc=
encryption program	fQiAk1ziJXTXRlsxFVbYQYlwrUzlhv8Efrglv4vNWh8=	XRqZzI1gcQ94WSlnH1vu5ngCmeM5GKPA6/5U5AAGlvw=	Uuv1kYdo02qkK3dbK30ujOPmmrhD2wSCU3jcUVFBcI8=
secure messaging agent	awOAlFf3cXDdWwggAFDRVBIh34dk2aXe7yfKOj4L7XU=	SxGZy4Z1JQtyRHp2Cl3n82CMKsX0ZX51pV19uIh69+0=	ROD1lox9h26uNiRKPnsnmSl8jIexIbMK+iqEDgEW65s=
personal computer	aAORkkr8MHGYSxQsF0zLVn7zjPnNyQBpP6UPA2YJXvY=	SBGIzZt+ZAo3VGZ6HUH98UV0ZVGO3myB4NhgIk4P5Hk=	R+DkkJF2xm/rJjhGKWc9m9KeaTj3QfCkZRYYXn+eMXc=
artificial intelligence	eRSXiEP7MnTZRFsoCU3aXxZR5X5BI3hw8ZxAS6IZHWk=	WQaO15J5Zg92Wyl+A0Ds+Fm/lqxJTN25eAgk7U8bxyI=	VvfiiphxxGqqKXdCN2Yskhz3BCJLQsa5zsDuGsnpufE=

A. Working



The steps involved in the working of the algorithm are:

1. Initialize the plaintext with the text to be encrypted.
2. Convert Passphrase, Saltvalue and the plaintext into byte arrays.
3. Next we create the password from the specified Passphrase and the Saltvalue. The password will be created using the specified hash algorithm given in the variable hashAlgorithm. Also the password generation can be done in several iterations.
4. Then this generated password is used to generate pseudo-random bytes for the encryption key. The size of key must be in bytes.
5. Create an uninitialized Rijndael encryption object.
6. Generate the encryptor from the existing keybytes and the initvector.Define the memory stream which will be used to hold the encrypted data. Also define the cryptographic stream and start encrypting.
7. Once the data is encrypted, convert the encrypted data from the memory stream into the byte array.
8. In the last step we convert data from the byte array into a base64-encoded string, which will be our final output.

IV. Conclusion

From the detailed study of SHA-1, Rijndael , and the proposed algorithm, we arrive at the conclusion that the proposed algorithm is more secure than the former ones. In case of Rijndael and SHA-1 encrypted text is same for the same plaintext everytime. This makes it easier for the attacker to derive some pattern of encryption, and hence break the security. However this is not the case with the proposed algorithm which is extremely difficult for the attacker to crack.

References

[1] S. Natarajan, M. Ganesan, and K. Ganesan "A novel approach for data security enhancement using multi level encryption scheme," *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 2, issue 1, pp. 469-473, 2011,

Jyoti Mahajan, "Secured encryption: a proposed algorithm based on combination of SHA-1 and Rijndael encryption algorithm", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 223-226, 2015.

ISSN: 2454-1532

[2] H. Gupta, "Multiphase Encryption Technique," An Article, Amity University U.P., 2011.
[3] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.
[4] A. kahate, *Cryptography and network security*, 3rd ed. New Delhi McGraw Hill Education (India) Private Limited.
[5] S. P. Singh, and R. Maini "Comparison of data encryption algorithms," *International Journal of Computer Science and Communication*, vol. 2, no. 1, pp. 125 – 127, 2011.
[6] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Prentice Hall, 1999.
[7] ''IT Engg Portal'', SHA-1 Algorithm: Information Security – BE [COMP, IT].
[8] M. M. Burnett and J. C. Foster, *Hacking the code: Auditor's Guide to writing Secure code for the web*, Rockland, MA Syngress Publishing Inc.

Jyoti Mahajan, "Secured encryption: a proposed algorithm based on combination of SHA-1 and Rijndael encryption algorithm", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 223-226, 2015.