A Review Of Encryption Algorithms-RSA And Diffie-Hellman

Nilesh A. Lal

Abstract: Network security is protecting data and message from cybercrime. Cryptography system is designed freely to communicate over a computer network. It is a process where sender sends encrypted message to the recipient. Symmetric encryption is known as the single key encryption. RSA algorithm is a symmetric key encryption.it uses public key and private key. Diffie Hellman cryptography is where both parties exchange secrets keys to encrypt message.

Index Terms: Cryptography, Diffie Hellman, Network Security, Public key, Private key, RSA, Symmetric

1 INTRODUCTION

Network Security has may policies designed to prevent crackers from invading and damaging the computer information system. The major concern of network security is the protection of data and message while it is send to the recipient over the computer network. Network security ensures that the data and message reaches the destination correctly and on time. As many users are now connected through network, Network Security has become a major concern [1]. Now protecting data and message is becoming more concern to IT professionals. Cryptography system was designed for users to communicate freely over a computer network. It is a process where a sender sends encrypted message and to the recipient. The recipient decodes the message back to plaintext. For example the sender Alice wants to send the message to Bob. The message he will send will be a plaintext. Alice encrypts the message known as ciphertext and sends to Bob over the network. The third person Ocsar tries to electronically tap the system and download the message which will be no use to him. Bob will have the encryption keys and he will be able to reverse engineer it to plaintext [2]. Cryptography is an essential information security gadget. It gives the four most crucial organizations of information security − Privacy − Encryption framework can screen the information and correspondence from unapproved revelation and access of information. Approval − the cryptographic frameworks, for instance, MAC and propelled imprints can secure information against mimicking and imposters. Data Integrity − the cryptographic hash limits are expecting basic part in ensuring the customers about the data respectability. Non-repudiation − the modernized mark gives the non-disavowal organization to get ready for the verbal confrontation that may develop due to contradiction of passing message by the sender. All these significant organizations offered by cryptography has engaged the lead of business over the frameworks using the PC structures into an extraordinary degree profitable and intense way. Nowadays, the frameworks have gone worldwide and information has taken the mechanized sort of bits and bytes. Fundamental information now escapes, took care of and transmitted fit as a fiddle on PC structures and open correspondence channels. Since information expect such a basic part, adversaries are concentrating on the PC systems and open correspondence channels to either take the tricky information or to bother the fundamental information structure. Exhibit day cryptography gives an effective course of action of methodologies to ensure that the pernicious points of the adversary are thwarted while ensuring the true blue customers get to information." Here in this segment, we will discuss the focal points that we draw from cryptography, its confinements, and furthermore the destiny of cryptography [3]. All IT professional encrypt devices to secure the message and data. Encryption is a process of protecting against passive attacks as called eavesdropping. This protection is known as message authentication [4]. Symmetric encryption is also known as conventional encryption. It is known as single key encryption. Conventional encryption works with five elements. 1. Plaintext, 2. Encryption algorithm, 3. Secret key, 4. Cyphertext, 5. Description algorithm. Fig.1 shows how symmetric encryption works.

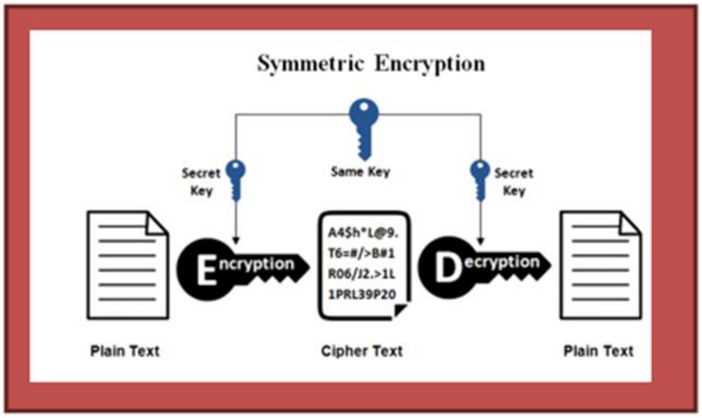


Fig.1. *Model Symmetric Encryption [5]*

However symmetric encryption is not a feasible solution to data authentication. For example, if a hacker attacks the system and reorders the blocks of cipher text then it can be successfully decrypted. Thus, block reordering is a major concern when using this type of encryption. Symmetric encryption is the most established and best-known procedure. A mystery key, which can be a number, a word, or only a string of irregular letters, is connected to the content of a message to change the substance especially [6]. Thus, this paper will review the best public-key cryptography algorithm currently

- *Nilesh Arvind Lal is currently pursuing Postgraduate degree program in Information Technology in University of Fiji, Fiji, PH:+6798034492. E-mail: nileshlal@rocketmail.com*

used for network security. It will highlight the algorithms, specify its strengths, application areas in network, current and future challenging and will recommend the novel solutions

2 RSA ALGORITHM

Public key cryptography is also known as a symmetric cryptography. This cryptography method is different from symmetric cryptography where it uses only one key for encryption and decryption. In public key cryptography it uses two keys. One for encryption and one for decryption. These two keys are known as public key and private key. The sender of the message will keep the private key secret and will send the public key to all the recipients of the message. The diagram below will show how the public encryption works [7].

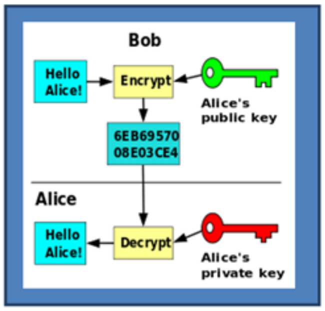
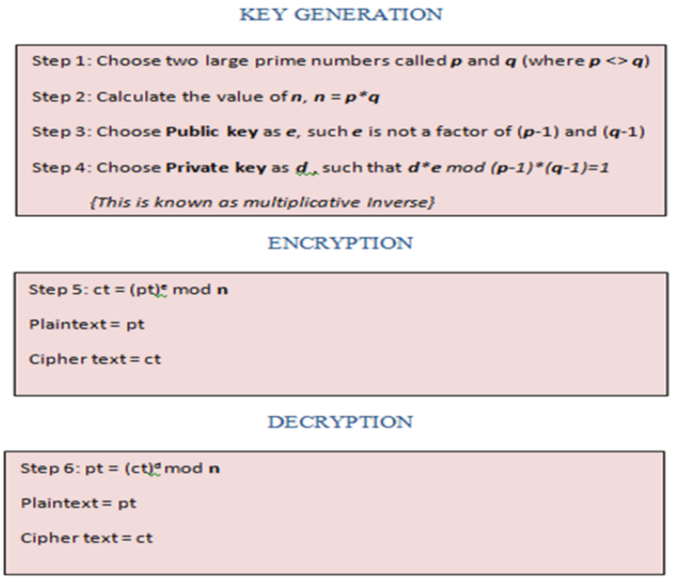


Fig. 2. *How public key cryptography works [7]*

Bob uses Alice's Public key to encrypt the message and sends it to Alice. Lice on the other hand will use her private key to decrypt the message to plaintext. There are two public key cryptography algorithms most commonly used. The first one is RSA and the second one is Diffie Hellman cryptography. These two cryptography will be further explained and analyzed. Furthermore, RSA algorithm is called a public key algorithm. RSA uses one key for encryption and the second key for decryption. The key used for encryption is called public key and the key used for decryption is called private key. RSA is invited y three most popular people. **R**ivest, **S**hamir and **A**dleman. Hence the algorithm is called RSA. The encryption and decryption uses modular exponentiation. Public key is more advance and being used for many years. RSA uses mathematical computation. The Public key encryption has six components. 1. Plaintext, 2. Encryption Algorithm, 3. Public and Private Key, 5. Cipher text, 6. Decryption Algorithm[4], [8]. Plaintext is an original message which the send sends. Encryption algorithms performs various mathematics operation and convert the plaintext to unreadable form called cipher text. During this process, public and private keys plays a major role. The decryption algorithm gets the cipher text as the input and using the reverse engineering using the private key it determines the plaintext. The original message. RSA encryption uses a block cipher in which the plaintext and cipher text are integers between *0* and and *n-1* for some *n.* [4].

2.1 RSA Algorithm Breakdown



KEY GENERATION

Step 1: Choose two large prime numbers called ***p*** and ***q*** (where ***p*** <> ***q***)

Step 2: Calculate the value of ***n***, ***n = p*q***

Step 3: Choose **Public key** as ***e***, such ***e*** is not a factor of (***p***-1) and (***q***-1)

Step 4: Choose **Private key** as ***d***, such that ***d*e** mod (p-1)*(q-1)=1*

{This is known as multiplicative Inverse}

ENCRYPTION

Step 5: ct = $(pt)^e$ mod **n**

Plaintext = pt

Cipher text = ct

DECRYPTION

Step 6: pt = $(ct)^d$ mod **n**

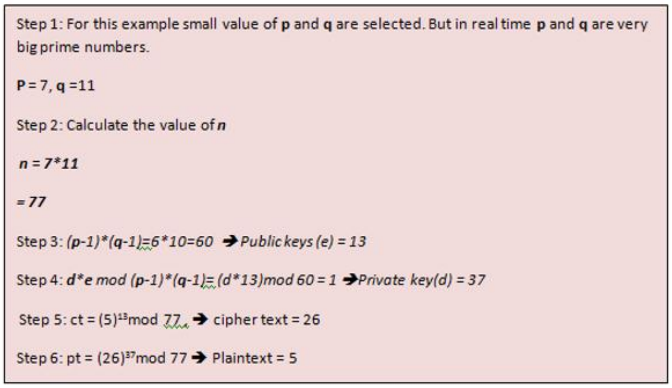
Plaintext = pt

Cipher text = ct

Fig. 3. *Shows breakdown of RSA Algorithm [4]*

In step 1 of Key generation, the two large prime numbers are selected called **p** and **q**, where **p** <> **q**. in step 2 the value of **n** where **n** is product of **p** and **q**. In step 3, the **public key** is selected as **e**, where **e** is not a factor of (**p**-1)*(**q**-1). In step 4, the private key selected such that **d***e mod (**p**-1)*(**q**-1) = 1. Here **d** can easily be calculated using multiplicative inverse. In step 5, Encryption is done using the formula ct = $(pt)^e$ mod **n.** The plaintext is converted to cipher text and in step 6 of Decryption the formula used is pt = $(ct)^d$ mod **n.** The cipher text is converted back to plaintext.

2.2 Worked example for RSA Algorithm



Step 1: For this example small value of **p** and **q** are selected. But in real time **p** and **q** are very big prime numbers.

P = 7, **q** =11

Step 2: Calculate the value of ***n***

n = 7*11

= 77

Step 3: *(**p**-1)*(**q**-1)=6*10=60* ➔ *Public keys (e) = 13*

Step 4: ***d*e** mod (**p**-1)*(**q**-1)= (d*13)mod 60 = 1* ➔*Private key(d) = 37*

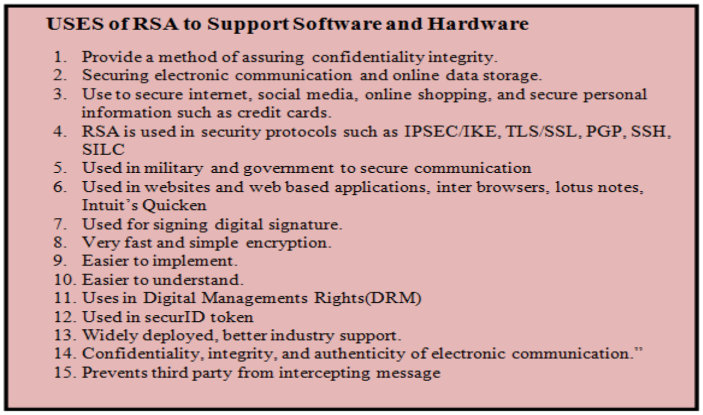
Step 5: ct = $(5)^{13}$mod 77 ➔ cipher text = 26

Step 6: pt = $(26)^{37}$mod 77 ➔ Plaintext = 5

Fig. 4 *shows worked example of RSA algorithm [4]*

2.3 Uses of RSA Algorithm

RSA is a widely used cryptography in network environment and it supports the software and hardware as mentioned in the list below:



USES of RSA to Support Software and Hardware

1. Provide a method of assuring confidentiality integrity.
2. Securing electronic communication and online data storage.
3. Use to secure internet, social media, online shopping, and secure personal information such as credit cards.
4. RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, SSH, SILC
5. Used in military and government to secure communication
6. Used in websites and web based applications, inter browsers, lotus notes, Intuit's Quicken
7. Used for signing digital signature.
8. Very fast and simple encryption.
9. Easier to implement.
10. Easier to understand.
11. Uses in Digital Managements Rights(DRM)
12. Used in securID token
13. Widely deployed, better industry support.
14. Confidentiality, integrity, and authenticity of electronic communication."
15. Prevents third party from intercepting message

Fig. 6. *How RSA is supported by hardware and software components. [11], [12] [10], [13], [14].*

2.3 Strength of RSA Algorithm

The strengths of RSA cryptography are 1. It increase and convenience. 2. Private Key will not be published. 3. It can provide a method for digital signatures. 4. It is not necessary for a single user environment but it is a good application for a open multi user environment. 5. It is a widely used public key cryptography. 6. Provides the data confidentiality. 7. Is a block cipher [9],[10].

3 DIFFIE HELLMAN ALGORITHM

Diffe Hellman cryptography is based on key exchange. The both parties need to exchange secrets key to encrypt message. It is based on difficulty of computing discrete logarithms. Diffie-Hellman is based on symmetric key exchange for both encryption and decryption. Suppose the two parties Alice and Bob would to communicate and they have decided to Diffe Hellman cryptography. Alice select prime modulus (**p**) and 23. Also generator (**g**) and as 7. The two parties publishes **p** and **g** public meaning **p** and **q** are known to both parties. Alice randomly selects number (**x**) as 3 and Bob randomly selects number (**y**) as 6. Alice will calculate the secret number (**r1**) as **r1** = **g**^{x} mod **p** and sends to Bob. **7**^{3} mod **23= 21.** So Alice will have r1 = 21 and send to Bob. Bob on the hand calculate r2 = **g**^{y} mod **p, 7**^{6} mod **23** which is **4. So r2 = 4**. Now Bob will send r2 = 4 to Alice. Now they will both calculate the share or symmetric key (**k**). Alice will calculate k = **r2**^{x} mod **p**, **4**^{3} mod **23** and k = 18. Bob will calculate k = **r1**^{y} mod **p**, **21**^{6} mod **23** and k = 18. The key k = 18 is same and both will use this key to send and receive data [4],[15].

3.1 DH Model with worked Example

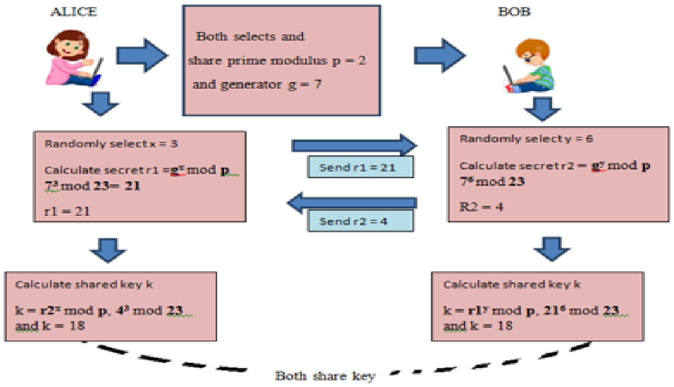
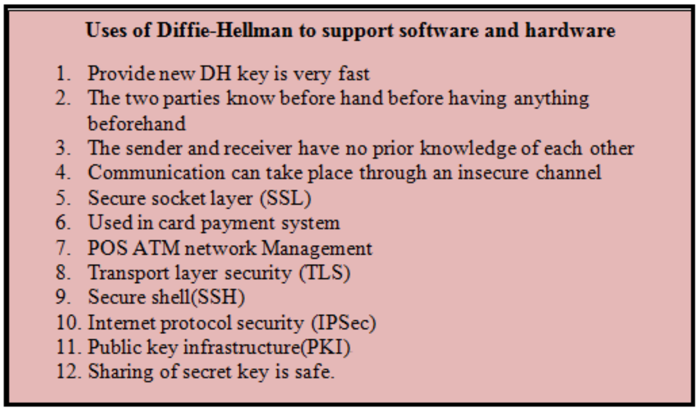

ALICE
Both selects and share prime modulus p = 2 and generator g = 7
BOB
Randomly select x = 3
Calculate secret r1 = gˣ mod p
7³ mod 23= 21
r1 = 21
Send r1 = 21
Send r2 = 4
Randomly select y = 6
Calculate secret r2 = gʸ mod p
7⁶ mod 23
R2 = 4
Calculate shared key k
k = r2ˣ mod p, 4³ mod 23 and k = 18
Calculate shared key k
k = r1ʸ mod p, 21⁶ mod 23 and k = 18
Both share key

Fig. 7. *Model of Diffie-Hellman algorithm*

3.1 HD Strength, Support hardware and Software

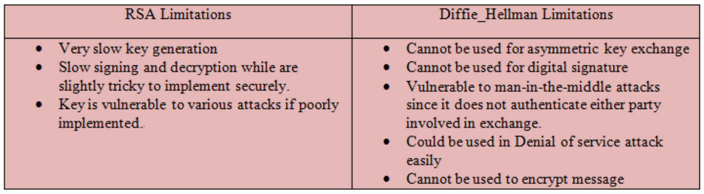


Uses of Diffie-Hellman to support software and hardware

1. Provide new DH key is very fast
2. The two parties know before hand before having anything beforehand
3. The sender and receiver have no prior knowledge of each other
4. Communication can take place through an insecure channel
5. Secure socket layer (SSL)
6. Used in card payment system
7. POS ATM network Management
8. Transport layer security (TLS)
9. Secure shell(SSH)
10. Internet protocol security (IPSec)
11. Public key infrastructure(PKI)
12. Sharing of secret key is safe.

Fig. 8 *How Diffie-Hellman (DH) algorithm is supported by hardware and software components [14], [15]*

4 RSA AND DIFFIE HELLMAN LIMITATIONS



RSA Limitations	Diffie_Hellman Limitations
• Very slow key generation • Slow signing and decryption while are slightly tricky to implement securely. • Key is vulnerable to various attacks if poorly implemented.	• Cannot be used for asymmetric key exchange • Cannot be used for digital signature • Vulnerable to man-in-the-middle attacks since it does not authenticate either party involved in exchange. • Could be used in Denial of service attack easily • Cannot be used to encrypt message

Fig.9. *Limitations of RSA and Diffie_Hellman Algorithm [14], [15]*

4 SOLUTIONS

RSA is regarded as one of the best encryption, the future challenges with RSA could occur in cryptography implementation. It has very slow key generation and can be vulnerable to various attack if not implemented well. One of the novel solution could be combine RSA with ECC this will enhance the security for all users. The second new approach could be to scramble and unscramble the message content as indicated by the ASCII(American Standard Code for Information Interchange) and RSA calculation by changing over the message content into parallel portrayal and partitioning this portrayal to bytes(8s of 1s) and applying a bijective capacity between the gathering of those bytes and the gathering of characters of ASCII and after that utilizing this component to be perfect with utilizing RSA calculation, at long last, Java application can be worked to apply this approach specifically. Since RSA choose two big prime number the key generation is slow. To increase the speed of the key generation, the manufactures need to design devices with faster processor so that the key generation is fast and is reliable. This will also solve the problem of slow signing and decryption. Another option would improve the speed of key generation would be doing some modification to two big prime numbers. By selecting random big number could increase the speed of key generation.

5 CONCLUSION

In conclusion, RSA and DH work differently but both are used for communicating between different parties. RSA uses two key as private and public key. It has different algorithm compared to DH. But RSA is more secure compared to DH. With DH it is subjected to man-in-the-middle attack since it cannot authenticate two parties. Both algorithms have advantages and disadvantages. In future both algorithm could be modified for better performance. RSA can be combined with ECC to improve the security and performance. Diffie Hellman can be integrated with digital and public key certificates to prevent from attacks.

REFERENCES

[1]. I. Wikimedia Foundation, "Network Security," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Network_security. [Accessed 14 03 2017].

[2]. K. H. Rosen, Cryptography Theory and Practice, 3rd ed., University of Waterloo.

[3]. "Cryptography Benefits & Drawbacks," [Online]. Available: https://www.tutorialspoint.com/cryptography/benefits_and_drawbacks.htm. [Accessed 23 03 2017].

[4]. W. Stallings, Network Security Essentials, 4th ed., New York: Pearson Education, Inc, 2011.

[5]. "Symmetric vs. Asymmetric Encryption – What are differences?," [Online]. Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. [Accessed 23 03 2017].

[6]. "Description of Symmetric and Asymmetric Encryption," 2007. [Online]. Available: https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption. [Accessed 23 03 2017].

[7]. M. Higashi, "SYMMETRIC VS ASYMMETRIC ENCRYPTION," 2013. [Online]. Available: https://www.ciphercloud.com/blog/cloud-information-protection-symmetric-vs-asymmetric-encryption/. [Accessed 24 03 2017].

[8]. R. G. Anjali Patil, "A Comparative Survey Of Symmetric Encryption," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 2, no. 8, p. 62, 2013.

[9]. A. H. A. Hadi, "A Survey On Some Encryption Algorithms And," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 2, no. 12, p. 286, 2013.

[10]. S. Blanda, "RSA Encryption – Keeping the Internet Secure," 2014. [Online]. Available: http://blogs.ams.org/mathgradblog/2014/03/30/rsa/. [Accessed 24 03 2017].

[11]. F. H. a. F. R. Michael Cobb, "RSA algorithm (Rivest-Shamir-Adleman)," 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/RSA. [Accessed 24 03 2017].

[12]. H. M. J. Ali Makhmali, "Comparative Study On Encryption Algorithms," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 2, no. 6, p. 44, 2013.

[13]. D. Chauhan, "RSA and Diffie-Hellman Algrithm," 2016. [Online]. Available: https://www.slideshare.net/daxeshchauhan/rsa-and-diffie-hellman-algorithms-64170629. [Accessed 24 03 2017].

[14]. E. E. Classes, "Diffie Hellman Key Exchange in Hindi for Symmetric Key Encryption System – With Example," 2016. [Online]. Available: https://www.youtube.com/watch?v=_M2Ea_3DRGA. [Accessed 24 03 2017].

[15]. K.Suganya, "Performance study on Diffie Hellman," INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE, vol. 2, no. 3, pp. 68-75, 2014.