Review Article

ACCENTS Transactions on Information Security, Vol 1(1)
ISSN (Online): 2455-7196

Brief comparison of RSA and diffie-hellman (public key) algorithm

Ayan Roy*
Department of Computer Science, St. Xavier's College, (Autonomous) Kolkata, India.

Abstract

With the increasing usage of internet all over the world, it becomes extremely necessary to encrypt the data that needs to be transmitted across the network. Over the years many such algorithms has been developed to encrypt the plain text in order to provide security to the data that is in transit. There are two methods of sending such data using the Asymmetric and Symmetric key cryptography. The author of this paper has highlighted the difference between the two encryption algorithms and further concluded that Asymmetric key cipher technique is way more secure compared to that of the symmetric key cipher technique. The author has also compared two prominent public key cryptography algorithms namely RSA algorithm and Diffie-Hellman algorithm and concluded that each such algorithms has its importance on particular context and each one holds the advantage over the other in specific context.

Keywords

RSA, Diffie-hellman, Asymmetric key, Symmetric key, Encryption.

1. Introduction

With the increasing usage of internet across the entire world, it becomes extremely necessary to protect the data that is in transit across the network against potential threat to confidentiality.[1][2] The main aim of an attacker is to gather the confidential information that is in transit across a public network.[4] Therefore, it is the job of a cryptographer to protect the data against such attacks by creating a cipher text for a plain text. The cipher text makes it difficult for an attacker to break the code and acquire the confidential information that is in transit across the network. Various strategies are used in order to generate the cipher text for a pain text.[5]

However there are two main strategies that are used on order to generate the cipher text for any given plain text. The two process of key generation are named as Asymmetric key Encryption Algorithm and Symmetric Key Algorithm.

In this paper the author has highlighted the above mentioned algorithms in specific details and emphasized upon 2 asymmetric key techniques namely RSA and Diffie-Hellman. Furthermore, the author has also made a comparative study of the 2 algorithms.

2. Asymmetric key Vs. symmetric key

Symmetric-key algorithms are those algorithms for cryptography that uses the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may undergo some simple transformation while it is in transit. There are many types of symmetric key algorithm.[3]

Asymmetric key or public-key algorithms are those algorithms in we have keys known as the 'public keys' to decrypt a message whereas we have keys known as the 'private keys' to encrypt the message, for proper and secure transmission of data.[8] The encryption is done using the private key of a sender while the decryption is done using the public key by the receiver.

Symmetric key suffers from both threat to confidentiality and integrity as the same key is used for the process of encryption and decryption.[6] An attacker can not only view the contents of the data in transit but also modify them.[7] Asymmetric key on the other hand, does not pose a threat to integrity as the encryption needs to be done by the private key of the sender.[10][9]

In the following sections the author has made a comparative study of 2 prominent Asymmetric key algorithms namely RSA and Diffie-Hellman algorithms and compared the two algorithms on certain user defined parameters.

*Author for correspondence

3. Diffie-hellman algorithm vs. RSA algorithm

Asymmetric key or public key cryptographic algorithm is far more superior compared to the symmetric key cryptography when the security of the confidential data is concerned. Asymmetric key includes large number of cryptographic algorithms. Out of the all the algorithms, the author has particularly chosen two efficient algorithms, one being the RSA algorithm and the other being the Diffie Hellman algorithm.[11] In the later subsections, the author has described the 2 strategies in details and compared the two based on certain user defined parameters.

3.1Diffie-Hellman Algorithm

Diffie-Hellman is a key exchange algorithm and allows two parties to establish, over an insecure communications channel, a shared secret key that only the two parties know, even without having shared anything beforehand. The key shared between the two parties is an asymmetric key.

It creates a shared secret between two (or more) parties, for subsequent symmetric encryption. However, it is susceptible to man in the middle attack.[14] In cryptography and computer security, a man-in-the-middle attack is an attack in which the attacker secretly alters the data involved in a communication between two parties who believe they are directly communicating with each other.

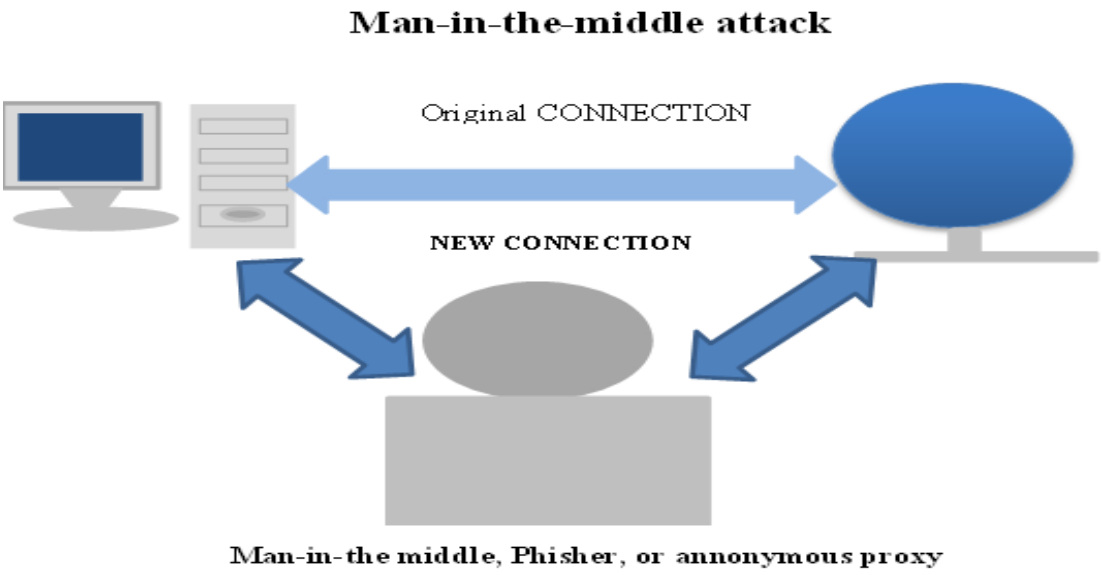

Figure 1 Representation of Man in the Middle Attack

It can be expressed as:

(gens1) s2 = (gens2) s1 = shared secret (mod prime) (1)

Where gen is an integer whose powers generate all integer in (1, prime)(mod prime),s1 and s2 are the individuals' "secrets", only used to generate the symmetric key.

Example of Diffie-Hellman Algorithm:

Suppose A and B wants to exchange messages using these parameters.

First, A chooses a random private integer value a, and B chooses a random private integer b. Neither a nor b is revealed to the public. A sends g^a(mod p) to B, and B sends g^b(mod p) to A, and these values are revealed publicly. Privately, A then computes $(g^b)^a$(mod p), and B computers $(g^a)b$(mod p). Since $(g^b)^a \equiv g^{ba} \equiv g^{ab} \equiv (g^a)^b$(mod p), A and B have a shared secret key, $(g^a)^b$, which they can use to send messages.

3.2RSA Algorithm

It is used to perform "true" public-key cryptography. In this algorithm the sender encrypts the data to be transferred using his public key and the receiver decrypts the encrypted data using his private key[13] RSA's results are subsequently used to generate a symmetric key.

$(m^e)^d$ = m (mod n) (lets you recover the encrypted message)

Where:

n = prime1 × prime2 (n is publicly used for encryption)
φ = (prime1 - 1) × (prime2 - 1) (Euler's totient function)
e is such that 1 < e < φ, and (e, φ) are coprime(e is publicly used for encryption)
d×e = 1(mod φ) (the modular inverse d is privately used for decryption)

Example of RSA Algorithm:

Choose p = 3 and q = 11
Compute n = p * q = 3 * 11 = 33
Compute φ (n) = (p - 1) * (q - 1) = 2 * 10 = 20
Choose e such that 1 < e < φ (n) and e and n are co-prime.

Let e = 7
Compute a value for d such that (d * e) % φ (n) = 1.
One solution is d = 3 [(3 * 7) % 20 = 1]
Public Key is (e, n) => (7, 33)
Private Key is (d, n) => (3, 33)
The encryption of m = 2 is c = 27 % 33 = 29
The decryption of c = 29 is m = 293 % 33 = 2

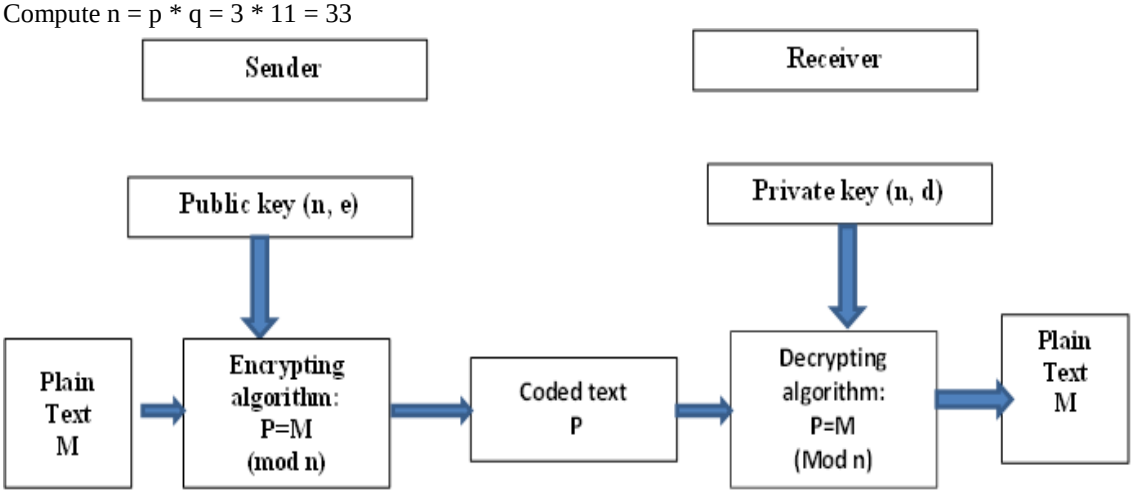

Figure 2 Pictorial Representation of RSA Algorithm

4. Comparative study of RSA and Diffie Hellman

In this section the author has compared the two algorithms on certain user defined parameters:

Table 1 Comparative study of RSA and Diffie-Hellman

Parameters	Rsa	Diffie-Hellman
Ephemeral Keys	Generating ephemeral keys for RSA is extremely difficult.	Generating ephemeral keys for Diffie-Hellman is extremely easy.
Security	Relies on the difficulty of integer factorization.	Relies on the difficulty of discrete logarithm.
Encryption	Encryption is cheaper.	Encryption is expensive..
Public Key Encoding	Public key is smaller to encode.	Public key is bigger to encode.
Strength	RSA 1024 bits is less robust than Diffie-Hellman	Diffie-Hellman 1024 bits is much more robust
Authentication	Authenticates only the sender.	Authenticates both the sender and the receiver.
Attacks	Susceptible to low exponent, common modulus and cycle attack	Susceptible to man in the middle attack.

5. Conclusion and future work

Thus, is can be concluded that the preference of Diffie-Hellman over RSA and vice versa is based on the inter-operability constraints. Each one gets preference over the other based on the context where they are being applied.[12] RSA and Diffie-Hellman are both based on supposedly intractable problems, the difficulty of factoring large numbers and exponentiation and modular arithmetic respectively, and with key lengths of 1,024 bits, give comparable levels of security.

Acknowledgment

The author is grateful to Department of Computer

Science for giving opportunity to do research work in Network Security. The author is also grateful to his family and dedicates his work especially to his late grandfather Sri. Amiya Ratan Das.

Acknowledgment
None.

Conflicts of interest
The author has no conflicts of interest to declare.

References
[1] Nath A, Basu D, Bhowmik S, Bose A, Chatterjee S. Multi way feedback encryption standard ver-1 (MWFES-1). International Journal of Advanced Computer Research(IJACR). 2013; 3(13):169-75
[2] Nath A, Basu D, Bhowmik S, Bose A, Chatterjee S. Modified multi way feedback encryption standard :Ver-I (MMWFES-I). International Journal of Advanced Computer Research(IJACR). 2013; 3(13):344-51.
[3] Nath A, Basu D, Bose A, Chatterjee S, Bhowmik S. Multi Way Feedback Encryption Standard Ver-2(MWFES-2). International Journal of Advanced Computer Research (IJACR). 2013; 3(13):29-35.
[4] Chatterjee S. Modified multi way feedback encryption standard Ver-2 (MWFES-2). Journal of Global Research in Computer Science. 2014;4(12):8-13.
[5] Nath A, Basu D, Bhowmik S, Bose A, Chatterjee S. Multi way feedback encryption standard Ver-3 (MWFES-3). In Information and Communication Technologies (WICT), 2013 Third World Congress on 2013 (pp. 317-24). IEEE.
[6] Nath A, Pal P. Modern encryption standard version IV:(MES-IV). International Journal of Advanced Computer Research. 2013; 3(3):216-23.
[7] Nath A, Samanta B. Modern Encryption Standard Ver-V(MES-V). International Journal of Advanced Computer Research.2013; 3(11):250-7.
[8] Nath A, Ghosh S, Mallick MA. Symmetric key cryptography using random key generator. In Security and Management 2010 (pp. 234-42).
[9] Chatterjee D, Nath J, Mondal S, Dasgupta S, Nath A. Advanced symmetric key cryptography using extended MSA method: DJSSA symmetric key algorithm. Journal of Computing. 2011; 3(2):66-71.
[10] Chatterjee D, Nath J, Dasgupta S, Nath A. A new symmetric key cryptography algorithm using extended MSA method: DJSA symmetric key algorithm. In Communication Systems and Network Technologies (CSNT), International conference on 2011 (pp. 89-94). IEEE.
[11] Khanna N, Nath J, James J, Chakraborty S, Chakrabarti A, Nath A. New symmetric key cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm. In communication systems and network technologies (CSNT), international conference on 2011 (pp. 125-30). IEEE.
[12] Chatterjee D, Nath J, Das S, Agarwal S, Nath A. Symmetric key Cryptography using modified DJSSA symmetric key algorithm. In proceedings of international conference worldcomp. 2011 (pp. 18-21).
[13] Vinogradov IM. Elements of number theory. Courier Dover Publications; 2016.
[14] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory. 1976; 22(6):644-54.

Ayan Roy is a post graduate student in Computer Science at St. Xavier's College, Kolkata.He has completed his Bachelors degree from St.Xavier's College Kolkata with major in Computer Science. His current research includes works in the fields of Mobile Learning, Data Mining and Cryptography. He has 5 publications so far and 2 conference papers.
Email: ayan.199316@gmail.com