Asaithambi.N, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 4, April- 2015, pg. 8-13 ISSN: 2321-8363

A Study on Asymmetric Key Cryptography Algorithms

ASAITHAMBI.N
School of Computer Science and Engineering, Bharathidasan University, Trichy, asaicarrier@gmail.com

Abstract

Asymmetric key algorithms use different keys for encryption and decryption. The keys are: Private Key and Public Key. The encryption key is public, decryption key is secret. Anyone can encrypt a message but only the one who knows the corresponding private key can decrypt it. The decryption key cannot be derived from the encryption key. Asymmetric key algorithms used for transmitting encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private. This paper discuss about some asymmetric key algorithms with its advantages and disadvantages.

Keywords: Cryptography, Diffie-Hellman, RSA, ElGamal, ECC, DSA.

1. Introduction

Asymmetric key algorithms are used for key distribution. Asymmetric key algorithms are also known as public key algorithms. Asymmetric key algorithms using two keys: A public key and a private key. Public key are used to encrypt the message and private keys are used to decrypt the message. Public key is known to public and private key is only known to user. So there is no need to distribute the keys before transmission [4]. In this type of algorithms it is very difficult to derive one key from the other.

This paper work mainly focuses on brief description about various asymmetric key algorithms. Such as Diffie-Hellman, Rivest Shamir Adleman, ElGamal Encryption Algorithm, Elliptic Curve Cryptography and Digital Signature Algorithm.

2. PUBLIC KEY CRYPTOGRAPHY ALGORITHMS

2.1 Diffie-Hellman (DH)

Diffie-Hellman is the first asymmetric encryption algorithm, invented in 1976 by Whitfield Diffie and Martin Hellman, using discrete logarithms in a finite field. It allows two users to exchange a secret key over an insecure medium without any prior secrets. Diffie-Hellman (DH) is a widely used key exchange algorithm [3].

The Diffie-Hellman protocol to be secure when an appropriate mathematical group is used. The generator element used in the exponentiations should have a large period. Usually, Diffie-Hellman is not implemented on hardware.

Key algorithm:

1. A and B publicly select a finite group G and an element $\alpha \in G$.
2. A generates a random integer a, computes α^a in G, and transmits α^a to B through a public communications channel and vice versa.
3. A receives α^b and computes $(\alpha^b)^a$.
4. B receives α^a and computes $(\alpha^a)^b$.

Now A and B both know the element α^{ab} which can be used as a private key for further communication. The Diffie–Hellman protocol is a widely used method for key exchange. It is based on cyclic groups. A prime of length 2048 bits should be chosen for long-term security.

2.2 Rivest Shamir Adleman (RSA)

RSA is the most commonly used asymmetric algorithm. It can be used both for encryption and for digital signatures. RSA can be used for key exchange as well as digital signatures and the encryption of small blocks of data. Today, RSA is primary used to encrypt the session key used for secret key encryption or the message's hash value.

RSA mathematical hardness comes from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers. Although employed with numbers using hundreds of digits, the math behind RSA is relatively straightforward.

Key algorithm:

1. Choose two prime numbers, p and q. From p and q you can calculate the modulus, n = p*q.

2. Select a third number, e, which is relatively prime to the product (p-1)*(q-1). The number e is the public exponent.

3. Calculate an integer d from the quotient (ed-1) / [(p-1)*(q-1)]. The integer number d is the private exponent.

RSA key lengths of 512 and 768 bits are considered to be pretty weak. For a reasonable level of security the key size should be greater than 1024 bits. 2048 bits key size should allow security for decades.

2.3 Elgamal Encryption Algorithm

ElGamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie-Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal is the predecessor of Digital signature algorithm. ElGamal encryption consists of three components: they are key generator, encryption algorithm, and the decryption algorithm [7].

Key Algorithm:

1. A finite cyclic group G of order n and generator $\alpha \in G$ are chosen. Each user picks a random integer $l \in \{0, 1, \ldots, n-1\}$ (private key), and makes public α^l (public key). We suppose that messages are elements of G and that user A wishes to send a message, m, to user B.
2. A generates a random integer $k \in \{0, 1, \ldots n-1\}$ and computes α^k.
3. A looks up B's public key α^l and computes $(\alpha^l)^k$ then $m\alpha^{lk}$.
4. A sends to B the pair of group elements $(\alpha^k, m\alpha^{lk})$.

5. B computes $(m\alpha^{lk})\ ((\alpha^{k})^{l})^{-1} = m\alpha^{lk}(\alpha^{lk})^{-1} = m$ and recovers the message.

ElGamal encryption is probabilistic, (i.e.) a single plaintext can be encrypted to many possible cipher texts, with the consequence that a general ElGamal encryption produces a 2:1 expansion in size from plaintext to cipher text. For encryption ElGamal requires two exponentiations. These exponentiations are independent of the message and can be computed ahead of time if need be. Decryption requires only one exponentiation.

2.4 Elliptic Curve Cryptography (ECC)

ECC was introduced by Victor Miller [8] and Neal Kolbitz as an alternative to established public key systems such as RSA [9]. In 1985, they proposed a public key cryptosystems analogue of ElGamal encryption schema witch used Elliptic Curve Discrete Logarithm Problem (ECDLP) [10]. Elliptic curve cryptosystems (ECCs) include key distribution, encryption algorithms. The key distribution algorithm is used to share a secret key and the encryption algorithm enables confidential communication. ECC is based on the addition of rational points on a chosen elliptic curve.

One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. Elliptic curves are applicable for the encryption, digital signatures, pseudo-random generators and other tasks. It is also used in several integer factorization algorithms that have applications in cryptography.

2.5 Digital Signature Algorithm (DSA)

The Digital Signature Algorithm (DSA) has been suggested and standardized by the National Institute of Standards and Technology (NIST) of the U.S. the DSA defines the technique for generating and validating digital signatures. The DSA can be used by the recipient of a message to verify that the message has not been altered during transit as well as ascertain the originator identity. It is an electronic version of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. The digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time.

The DSA is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Every signatory has a public and private key. In the signature generation process the private key is used and the public key is used in the signature verification process.

Key algorithm:

1. Generate two large, distinct prime's p, q
2. Compute $n = p*q$ and $\varphi = (p-1)(q-1)$
3. Select a random number $1 < e < \varphi$ such that $\gcd(e, \varphi) = 1$
4. Compute the unique integer $1 < d < \varphi$ such that $ed \equiv 1 \bmod \varphi$
5. (d, n) is the private key
6. (e, n) is the public key

p and q must be destroyed at the end of key generation.

Signature generation:

1. Compute m* = R(m) an integer in [0, n–1]
2. Compute s = m*d mod n
3. A's signature for m is s

Signature verification:

1. Obtain A's authentic public key (*e*, *n*)
2. Compute m* = se mod n
3. Verify that m* is in MR; if not reject the signature
4. Recover m = R-1(m*)

3. Advantages and Disadvantages

The advantages and disadvantages of various asymmetric key cryptography algorithms are discussed in the following table.

Table 1. Advantages and disadvantages of various asymmetric key cryptography algorithms.

S.no	***Algorithms***	***Advantages***	***Disadvantages***
1	Diffie-Hellman (DH)	Solving the discrete logarithm is very challenging, secret key is never itself transmitted over the channel.	Expensive exponential operations, Cannot be used to encrypt messages, lack of authentication.
2	Rivest Shamir Adleman (RSA)	Increased security, provide a method for digital signatures.	Very slow in processing.
3	ElGamal	For long messages our generalized encryption is very fast, same plaintext gives a different ciphertext each time it is encrypted.	The ciphertext is twice as long as the plaintext.
4	Elliptic Curve Cryptography (ECC)	Greater exibility, smaller key sizes with the same security.	Hyper elliptic cryptosystems over even smaller key sizes, difficult to explain/justify to the client.

5	Digital Signature Algorithm (DSA)	Authentication, Integrity, the document is free from forgery or false information.	Cost, Training and troubleshooting, Necessity, Technological Compatibility, Security Concerns, Legal Issues, Non-repudiation.

4. Conclusion

The conclusion of the study is that from the security point of view the Asymmetric Cryptography technique is more secure than the symmetric cryptography. Because asymmetric cryptography is difficult to break the system, that uses two different keys. In most practical implementations asymmetric key cryptography is used to secure and distribute session keys. In this paper the basic asymmetric key algorithms, key concepts, security are presented and in feature the researchers can introduce different asymmetric algorithms.

References

[1]. Vishal Garg and Rishu, July-August 2012,Improved Diffie-Hellman Algorithm for Network Security Enhancement, *International Journal of Computer Technology & Applications*, Vol 3 (4), 1327-1331.

[2]. M. Preetha, M. Nithya, June 2013, A Study And Performance Analysis Of RSA Algorithm, *IJCSMC*, Vol. 2, Issue. 6, pg.126 – 139.

[3]. Alese, B. K.Philemon E.D., Falaki, S. O., September 2012 , Comparative Analysis of Public-Key Encryption Schemes, *International Journal of Engineering and Technology*, Volume 2, No. 9.

[4]. Dr. Prerna Mahajan, Abhishek Sachdeva, 2013 , A study of Encryption algorithms AES, DES and RSA for security, *Global Journal of Computer Science and Technology*, Volume 13 Issue 15 Version 1.0.

[5]. Certicom Corp., 2004, An elliptic curve cryptography (ECC) primer, *White paper*, Certicom.

[6]. Williams Stallings, 2006, Cryptography and Network Security, *Prentice Hall*, 4th Edition.

[7]. S. Vijaykumar and S. Saravanakumar, 2011, Future Robotics Memory Management, *Advances in Digital Image Processing and Information Technology*, pp. 315–325.

[8]. S. Vijaykumar and S. Saravanakumar, 2011, Future Robotics Database Management System along with Cloud TPS, *Intl. Journal on CloudComputing: Services and Architecture (IJCCSA)*, pp. 103–114.

[9]. Rashmi Singh, Shiv Kumar, December 2012, ElGamal Algorithm in Cryptography, *International Journal of Scientific & Engineering Research*, Volume 3, Issue 12.

[10] V. S. Miller, 1986, Use of Elliptic Curves in Cryptography, *Advances in Cryptology Crypto'85*, LNCS.218, New York, *Springer-Verlag*, pp. 417-426.

[11] N. Demytko, 1994, A New Elliptic Curve Based Analogue of RSA , *Advances in Cryptology Eurocrypt'93*, *Springer-Verlag*, New York, pp. 40-49.

[12] Dahab, R., and J.Lopez, 2000, An Over-view of Elliptic Curve Cryptography, Institute of Computing State University of Campinas Brazil, Brazil.

A Brief Author Biography

Asaithambi – I had completed BCA from Bharathidasan University and MCA degree from Anna University. Currently pursuing M.phil (Computer Science) at School of Computer Science and Engineering, Bharathidasan University, Trichy, India. I have interested in the research area`s are cloud, cryptography and data security. I started my research publication from here, this is my first publication.

