Superiority of Asymmetry

Mitch Meyer

Bellevue University

Abstract

This research paper will discuss various forms of asymmetric cryptographic algorithms. Each algorithm will be analyzed and compared to determine its most appropriate use. The functions of private and public keys will be examined as will how each algorithm creates and manages encryption keys. The mathematical formulas used to encrypt the data in each discussed algorithm will also be examined. Finally, the superiority of asymmetric cryptography as a form of securing network transmissions will be explained.

According to a 2013 Mena banking report, German company Giesecke & Devrient has been contracted by the Republic of Kosovo to manufacture electronic passports for their citizens. Kosovo contracted Giesecke & Devrient to become one of the first European Union member nations to conform to the new EU regulations requiring asymmetric encryption on electronic passports. These regulations were scheduled to take effect December of 2014 requiring all new electronic passports to use the Supplemental Access Control(SAC) protocol to encrypt personal data stored on passports. SAC is an asymmetric encryption protocol and according to the 2013 Mena report, Integrity Guard security chips deploying this protocol “…offer the highest level of protection against data manipulation that is available.” (Mena, 2013) Securing data and protecting its integrity is becoming more important as dependence upon information systems continues to grow in all sectors of life.

Encryption is the process of changing plaintext into ciphertext. This transforms data into a secure form that cannot be accessed without a key to decipher the encrypted data. There are many ways to encrypt information, but asymmetric is proving to be a very powerful and flexible method for securing data. Asymmetric encryption can be done a number of different ways, is typically deployed to address security concerns regarding network traffic, and is proving to be the superior method of establishing and maintaining secure connections over the Internet.

Encryption is the process of making data unreadable by scrambling it using a key. That data must then be unscrambled using that same key. What makes that scrambled data secure is maintaining the secrecy of the key that was used to encrypt the data, but in order to share that data, the key must be shared as well. This is the security paradox that asymmetric encryption solves. Asymmetric encryption algorithms typically make use of two keys to secure data, a public key and a private key. A person’s public is freely available to everyone to use while their private key is known only to them. Using an asymmetric encryption algorithm, a secure message can be sent to someone by taking their publicly known key and using it to encrypt messages sent to that specific person. Upon receiving an encrypted message, the private key must be used to decrypted the message encrypted with the public key.

This also works going the opposite direction, meaning that a message encrypted with a private key can be decrypted using that person’s public key. This feature gives asymmetric encryption algorithms the ability to confirm the identity of a person who is sending an encrypted message and provides nonrepudiation, meaning the actual sender of a message is unable to deny being responsible for sending the message. While these fundamental principles of asymmetric encryption grant it strength and solve many problems of securing data in transmission, each encryption algorithm generates the keys used to secure the data differently. The strength of those generated keys is what grants strength to an encryption method and each algorithm does it differently.

There are many different algorithms that are used for asymmetric encryption but two are the RSA algorithm and Elliptic Curve Cryptography algorithm. RSA is an algorithm that was created in 1977 by three developers named Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. The algorithm is named for the three men who developed it. How RSA creates the private and public keys used in its encryption is explained by Mark Ciampa:

“The RSA algorithm multiplies two large prime numbers *p* and *q* to compute their product (*n = pq*). Next, a number *e* is chosen that is less than *n* and a prime factor to (*p-*1)(*q*–1). Another number *d* is determined, so that (*ed* – 1) is divisible by (p – 1)(q – 1). The value of *e* and *d* are the public and private exponents. The public key is the pair (n,e) while the private key is (n,d). The numbers p and q are disgarded.”

RSA uses large prime numbers to create its keys so they are extremely secure, but because this algorithm uses such large and complex keys to encrypt data, RSA runs slower than other encryption algorithms and requires more computer processing resources to be viable.

Elliptic Curve Cryptography is an asymmetric encryption algorithm that derives its public and private keys from an elliptic curve function that is drawn on an x-y axis. The two parties each pick a point on the curve from which a third point can be derived. Each publicly selected point is used to generate the respective public keys and the two points together are used to generate the shared private key. ECC was first introduced in 1985 and was met with a lot of skepticism in the cryptography field according to Gupta. (Gupta, 2011) Elliptic Curve Cryptography requires much less resources to process than RSA and provides a similar level of security to its connections. According to Gupta, “it is worthy of note that a 160-bit ECC security key has about the same level of security as a 1024-bit RSA key.” (Gupta, 2011) The fact that ECC can provide the same level of security with a fraction of the number of bits involved in the key allow ECC to operate with fewer processing resources. This makes ECC a fantastic choice for securing connections from a mobile device.

 "In order to secure communications between two entities, asymmetric encryption is often employed. In an asymmetric encryption system, a public key and a complementary private key are employed for each user. The public key is published and the private key is kept private. A sender uses the recipient's public key to encrypt a message and the recipient uses its own private key to decrypt the message.” (Information Technology Newsweekly, 2015) The public key is published and made available through the use of digital certificates which are issued and managed by Certificate Authorities. A digital certificate contains information about the identity of the person being certified including the owner’s name or alias, the owner’s public key, the name of issuing authority, the digital signature of the issuer, the serial number of the digital certificate, and the expiration date of the public key. (Ciampa, 2014) Certification Authorities also provide several different categories of digital certificates to meet different needs. There are five classes of certificates but the most common are the class 1 or personal certificate and the class 2 or server certificate. Personal certificates are usually used to secure email messages and only require a name and email address be divulged in order to receive certification. Server certificates are issued from a server to connecting clients. These certificates allow clients to identify the owner of the webserver they are connecting to and to have confidence that the information they are transmitting is accessible only by the person or organization listed on the certificate. This type of certification is what makes e-commerce possible.

Asymmetric cryptography with digital certificates works by opening a connection in a web browser using, most commonly, the secure Hypertext Transport Protocol. This protocol makes use of one of two different cryptographic transport algorithms, the Secure Socket Layer algorithm and the Transport Layer Security algorithm. These algorithms use a handshake process in a client server exchange to establish a secure connection. The first step is an opening message that the browser sends to the server containing a list of cryptographic algorithms the browser supports. The server responds with a message indicating the algorithm that will be used and then it sends its digital certificate to the browser. The browser then uses the public key contained in the certificate and encrypts a randomly generated number using the selected algorithm and the server’s public key and sends back the encrypted message. This randomly generated number is called the pre-master secret key. The server receives the encrypted pre-master secret key and decrypts it using its private key and both the client and server generate the same secret master key. The secret master key is then used to create session keys. Session keys are symmetric encryption keys that have no connection to the server’s public key. “Asymmetric encryption schemes are usually used only for secretly transmitting a session key of a symmetric encryption scheme for message encryption. In fact, the hybrid usage of asymmetric and symmetric encryption schemes is very common in practice.” (Fujisaki, 2013) The use of digital certificates allows the use of powerful symmetric encryption algorithms by overcoming the paradox of exchanging a shared key securely.

Asymmetric encryption is used worldwide every day to establish secure connections for countless various purposes. This method of encryption has shown its superiority through the impact it has had on the online marketplace. Asymmetric encryption is found working for e-commerce sites, financial institutions, and government sites all across the world. Asymmetric cryptography is a superior method for opening a secure connection because it provides the ability to authenticate the identity of the parties participating in the connection and it provides non-repudiation through that identification. These are features that symmetric encryption cannot provide.

Public keys and private keys are mathematically related and public keys can be used to decrypt files encrypted with the corresponding private key and messages encrypted with the public key can be decrypted with the corresponding private key. This gives users of asymmetric encryption the ability to create digital signatures. Digital signatures are hashed documents that have been encrypted with a private key. This hashed document could only be decrypted with the public key of the person who sent the file. If a message is sent with an attached digital signature, this would serve as proof to the identity of person who sent the file. It also would prevent the sender from later denying sending the message containing the digital signature since no one else could create the signature without having access to the private key of the sender. Because symmetric keys must use a shared key to encrypt and decrypt messages, it does not provide the ability to create digital signatures without the help of an asymmetric encryption algorithm.

Asymmetric encryption is the method of choice when it comes to opening a secure connection to transmit sensitive data. In Europe, 192 million electronic passports are in circulation with an estimated 30 million more issued each year and each electronic passport uses asymmetric encryption. (Mena, 2013) The European Union understands the importance of protecting its citizens’ information and requires that sensitive travel documents “…which enhances protection against unauthorized access and possible abuse of personal data.” (Mena, 2013) Their reliance on the Supplemental Access Control asymmetric encryption algorithm provides them with many benefits over other products including “… provide better computing performance, which results in faster processing for citizens when they cross borders.” (Mena, 2013)

Asymmetric encryption has proven itself to be a powerful and flexible solution to the problem of securing connections across the Internet. There are many different algorithms available to open a secure connection and the use of digital certificates help expedite that process. Asymmetric encryption is superior to symmetric encryption because it allows the use of digital signatures which gives it the ability to authenticate the identity of the parties involved in the connection and prevents those parties from denying their involvement. Asymmetric encryption has established its superiority and its primacy as the method of choice for secure network connections.

Sources

Ciampa, M. (2015). *Security guide to network security fundamentals* (5th ed.). Boston, MA: Cengage Learning.

EMC corporation; patent issued for asymmetric encryption scheme with expiring revocable certificates having a predefined validity period (USPTO 9118487). (2015). *Information Technology Newsweekly,* , 1542. Retrieved from <http://ezproxy.bellevue.edu:80/login?url=http://search.proquest.com/docview/1708933887?accountid=28125>

Fujisaki, E., & Okamoto, T. (2013). Secure integration of asymmetric and symmetric encryption schemes. Journal of Cryptology, 26(1), 80-101. doi:10.1007/s00145-011-9114-1

Germany : Infineon supplies the security chips for the world's first electronic passports of the newest generation using asymmetric encryption. (2013). *MENA Report,* Retrieved from <http://ezproxy.bellevue.edu:80/login?url=http://search.proquest.com/docview/1417084761?accountid=28125>

Gupta, K., & Silakari, S. (2011). ECC over RSA for asymmetric encryption: A review. International Journal of Computer Science Issues (IJCSI), 8(3), 370-375.