Privacy with Encryption and PKI.

February 18, 2001

Constantine Konstantinidis

"Several dozen" PKI pilot projects and experiments are under way in agencies ranging from the Social Security Administration and the Defense Department to the Federal Aviation Administration, Dyer told members of the Armed Forces Communications and Electronics Association Nov. 20. 2000
http://www.fcw.com/fcw/articles/2000/1120/web-afcea-11-21-00.asp

1. Introduction -

This paper sets out to explain the nature of PKI(public key infrastructure) and digital certificates and applying them in today's real world, along the way it is important that I explain encryption, ciphers….etc as they inter-relate. You will also find that I repeat myself throughout this paper, this is done to emphasise key points in a cryptographic system. Many discussion groups have been formed around the world including the IETF(http://www.ietf.org/html.charters/pkix-charter.html), The OpenGroup(http://www.opengroup.org/public/tech/security/pki/index.htm) and NIST (http://csrc.nist.gov/encryption/aes/) to formulate discussion groups on PKI. There is a global trend towards the use of the Internet as a means for carrying information and conducting business. Users, companies, governments are faced with many questions when considering the Internet as a business communication medium, which includes;

- How do I know the "message" will be safe?
- Are my credit details transported or sent safely?
- Can the competition access my company's sensitive information?
- How do I prove the sender is who they say they are?
- Can others read my private e-mail in transit or when stored on a server?
- Is the receiver who they say they are?
- Is it possible for me to know what the person sent was in fact what I received?

How are these problems, and others addressed?

In todays world we are able to sign a letter in our own handwriting and put it into a sealed envelope. By doing this we solve the problems of **authenticity** – it is signed with a verifiable signature; **privacy** – it is in a sealed envelope; certainty the recipient will get it – addressing the envelope; and clarity – it is written out. Can this be achieved in the electronic world with the required levels of additional security dictated by the medium and the environment?
The answer is "yes". Public Key Infrastructure using encryption is the means to achieve a similar outcome in the world of e-commerce.

2. The Internet Threat

Information sent from one computer to another via the Internet can be routed via numerous other intermediary systems on it's way. Normally, these intermediary computers don't monitor the traffic that flows through them, but it is possible for someone to intercept your communications or credit card transaction whilst it is traversing the superhighway and in plaintext for all to see! Because of the way the Internet has been architectured, there will unfortunately always be a way for unscrupulous people to reek havoc on electronic messages and transactions. Fortunately though, we have been presented with more tools than ever before to foil their attempts at gaining unauthorised information. Although the Internet and IT in general is of relatively new technology, this process of foiling and counter foiling has been going on for many millennia.

3. Encryption and how does it work.

Above I explained that in the war against hackers and eavesdroppers we have been presented with an array of weapons to fight off the threat, one of those tools is encryption. Encryption is the process of transforming information that originates in clear or plain text to be encrypted or scrambled/encoded into an unreadable "cipher text". Decryption is the opposite whereby you decrypt the scrambled cipher text back into legible text. Encryption comes in many guises with modes like symmetric and asymmetric, block and stream ciphers like DES, 3DES, Blowfish, RSA, RC*, IDEA, ECC, AES, CAST, standards and protocols like SSH, SSL, S/MIME, PGP, IPSec, that all essentially serve the same ultimate goal, to assist in hiding information that is only for the intended recipient.

4. How Secure Is Encryption?

This question all depends on the type of encryption used and the way it is administered and managed. The best most secure encryption algorithm is absolutely rendered worthless if the most important link in the chain is compromised – people! We have to observe our utmost vigilance in the encryption life cycle. If we where to be to lax in our approach to security and divulge our private or secret keys and or passphrases then all the strongest encryption system won't help you, it's that blunt and simple. Your private or secret keys and passphrases are just that, private and secret. Now that we have covered the human nature aspect, lets focus on the encryption side itself. The strongest encryption systems are those that utilise ciphers with the longest bits. For instance the *DES* cipher has been around since the early 70's and uses a 64-bit (56-bit keys) block cipher, symmetric algorithm that has probably seen better days in terms of strength. A brute force attack on this type of bit length would result in it's capitulation within days. It's offspring, triple DES is another story. By combining DES with a further 2 keys would increase it's strength to 168-bit. Generally, the larger the key lengths, the stronger the cryptosystem is and typically it is not the algorithm itself that is usually the weak point but rather the lax security on the servers used to house the sensitive data, meaning if your going to use strong encryption to conduct business on the Internet by using say, SSL (which coincidentally can be used with both symmetric and asymmetric modes with strong algorithms) and be reasonably assured of safe communications, but the credit card information is then stored in the clear on the database server with a weak security build, then your private information can still be obtained after it has been transmitted from your client software to the weak server, after all security should be considered a holistic exercise , right?. Relying on just point to keep you secure is really not the correct approach when considering storing sensitive data such as customer's credit card numbers. Sensitive data once transmitted from the Internet should then be downloaded or housed on a server that has been hardened by the security analysts in your company. Examples of securing NT and Unix servers can be sourced from a myriad of sites like the reading room at www.sans.org. Part of maintaining a secure encryption infrastructure should also involve key storage as well. If you are to use an asymmetric encryption infrastructure such as PKI, then the issue of safely securing your private key should be considered. Private keys should be kept private and protected with an additional password to use the private key. Consider using a personal firewall on your home PC or work laptop when on the move to warn on suspected intrusion attempts whilst on a network or on the Internet. A safer bet is to store your private keys on a smart card or token. You can't physically get into these devices without breaking and they come with passphrase protection to use them, so a hacker would have to guess your password and the randomness of the private key settings to use it which is highly unlikely. But if your private key was to be copied or stolen then you must immediately create a new key pair.

So to summarise this section, encryption is considered to be a secure means to safely transmit sensitive data across the Internet. There have been no public reports claiming to have compromised algorithms like RSA (asymmetric keys) and Triple DES (symmetric keys) themselves. The most vulnerable parts to a cryptosystems cycle is the human aspect talked about above and the weak web server used to house sensitive data. Once you have addressed these concerns, then using encryption would be considered a safe and secure means to conduct sensitive business and correspondence on the Internet or network.

5. Encryption Ciphers

A cipher is described as a set of mathematical rules (logic) used in the process of encryption and decryption or a cryptographic or encipherment algorithm. It is the mathematical process applied when taking readable text and turning it into an unreadable mess. The mathematical process used in these ciphers is quite complex and long to discuss in this paper, but briefly the mathematical strength of these ciphers comes from "intractable problems of the difficulty of factorising large integers into their two prime factors" meaning that our worlds top mathematicians find it difficult to solve a mathematical problem of factorising large integers. It is this intractability or difficulty that has been positively used in creating strong mathematical algorithms, which in turn can be applied to cryptography. No one is claiming that it can never be solved but the likely hood of this happening in polynomial time or any time soon is low. Without these ciphers encryption just wouldn't be the secure tool it is today. A cryptosystem is the algorithm, the keys, the plaintext, the certificates. There are many ciphers in use in today's real world of electronic communications. As discussed earlier, DES (Data Encryption Standard) a 64-bit block cipher, using 56 bit keys was the default standard cipher adopted by the US government in 1977 to protect federal agencies with sensitive and unclassified information.

That was then, and this is now……..where DES would of served it's intended use at that time quite well, recently it has been demoted as the choice of serious cryptographers in favour of others popular ciphers like Triple DES and RSA.

Triple DES is the child or offspring of DES. Triple DES is a symmetric, block cipher which actually is the DES algorithm used three times with three different keys giving you a total of 168 bits. This is considered by many to be currently quite secure with no public reports of breaking this algorithm to date. There are two ways you can apply encryption technology, symmetric and asymmetric, which I'll explain in the next couple of topics. There are also two types of cipher modes currently used, stream and block. Quite simply **block ciphers** (like DES, Triple DES, AES (Rijndael), RSA, Blowfish) encrypt data in chunks, typically 64 bits at a time. Often the key length is the same as the block size. These sorts of ciphers are suited to the encryption of data. The problem with block ciphers is that usually the message does not end on a block boundary, requiring padding or extra bits to be added to complete the last block. **Stream ciphers** (like RSA's RC4), by comparison, encrypt one bit at a time. These are particularly applicable to real time streams like audio or video or other hardware types like hardware based VPN's. Block ciphers are much more efficient when used with software based encryption and stream ciphers are not as strong as block ciphers and are therefore less commonly used. You will also need to understand the different modes that block ciphers can be applied. The easiest way to use a block cipher is in ECB (electronic code book) mode, in which each block is encrypted separately although each block will encrypt the same each time which could lead to all sorts of attacks. A better approach is by encrypting each block differently in different messages….and that is what CBC (cipher block chaining) does. In CBC mode each plaintext block is combined, using an XOR with the last ciphertext block before encryption. This means that the encryption of each block depends on what was already encrypted making it more difficult for attackers. As XOR is reversible, chaining can be done at decryption time. Other cipher modes to mention are CFB(cipher feedback) and OFB(output feedback) which turn block ciphers into stream ciphers. Other ciphers to note are ECC(Elliptical curve cryptosystem) which been receiving lots of press lately even though ECC has been proposed since the mid 1980's. It is generally acknowledged that ECC is faster than RSA and delivers similar levels of security with smaller key lengths. Behind the scenes there is some heavy-duty mathematics happening and is quite complex to go into here but to briefly explain, the security depends on the intractability of solving the discrete logarithm problem over points on an elliptic curve.

The working mechanism of most public key cryptographic algorithms is generally openly published and widely known. The security of the cryptosystem comes from the secrecy and size of the private key and not from the secrecy of the algorithm itself. You need to ensure that key lengths are kept large to avoid brute force attacks on small key lengths.

6. The AES project in brief

AES stands for Advanced Encryption Standard and what instigated by the NIST(US National Institute Of Standards And Technology) back in 1997 as a replacement for the ageing DES standard. This was devised as a worldwide competition to find a new encryption algorithm for the 21st century. The winner of this competition was selected in November 2000 to be Rijndael from Joan Daemen and Vincent Rijmen, cryptographers from Belgium. To find out more about this new algorithm visit; http://csrc.nist.gov/encryption/aes/

7. Symmetric & Asymmetric

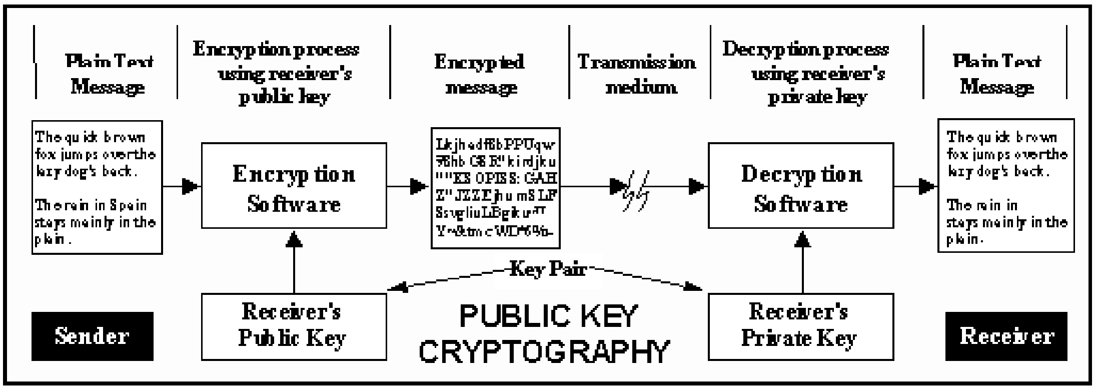
These two terms refer to methods applied in cryptography using either **symmetric keys**(meaning the encryption and decryption key are either the same or can be calculated from one another) or **Asymmetric keys**(a separate but integrated user key-pair, compromised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information cannot be used to decrypt the same data). Symmetric encryption is considered better in performance than Asymmetric encryption. One way companies have started to get around the performance question of symmetric Vs asymmetric encryption has been the hybrid approach. Put simply both symmetric and asymmetric encryption is used. The idea is that most of the encryption is done with a symmetric cipher, using a randomly selected session key. The session key is then encrypted with the recipient's public key and prepended to the ciphertext. Only someone with the correct private key can decrypt the session key, and hence the message. This approach gives the best of both worlds, the speed of symmetric with the scalability of public keys.

Symmetric encryption is like a combination lock protecting a safe. The same combination or key is used to unlock the safe. The problems associated with symmetric encryption is that as the keys used are the same, if someone uncovers any of the keys, they can then encrypt and decrypt any message that has been encrypted or decrypted by the same key. It is also generally regarded not the ideal solution for large-scale encryption implementations because of the issue of managing all the shared keys. If you distributed hundreds of shared keys across the place and someone other than those intended to use the symmetric key got hold of it, then you would have to re-distribute new keys to assure privacy again. The use of asymmetric keys has gone a long way to fix this problem. The only key being distributed would be your public key. You use your private key to encrypt a message and then the recipient would use your public key, which was either sent to them or downloaded from a server to decrypt the message. This is generally accepted to be a more safer way for large business to conduct e-business, because the only time you would have to redistribute a key pair would be in the event that your private key was uncovered, which is unlikely as you are keeping it secure right? add certificates to assure a public keys authenticity, a strong well known cipher and a digital signature to assure message contents haven't been tampered, you then come up with a strong cryptosystem called PKI or Public Key infrastructure.

What is PKI?

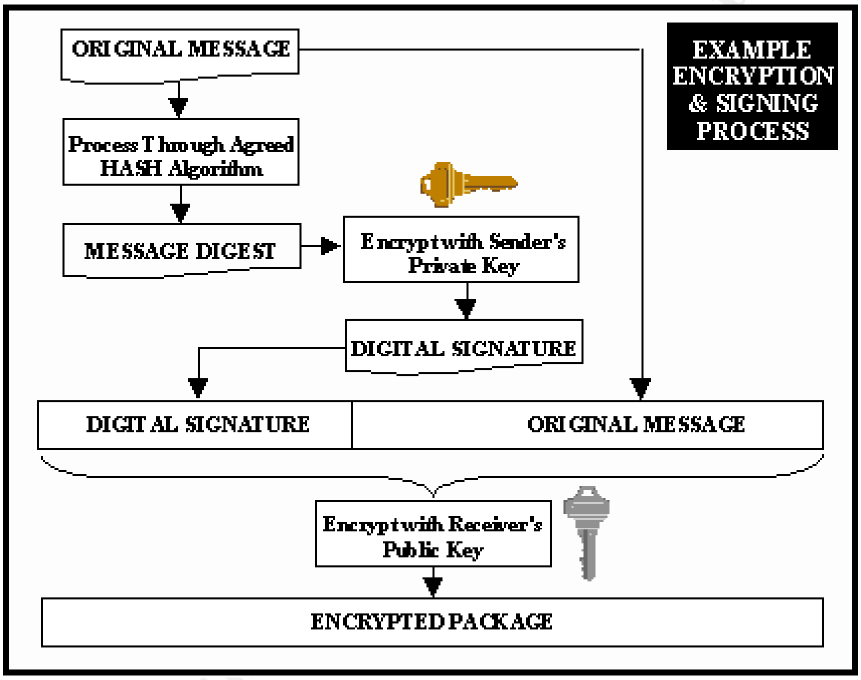
PKI stands for Public Key Infrastructure, which basically utilises key pairs to ensure, when properly implemented;

- **Confidentiality** – Confidentiality is achieved when only those intended to be able to access a message can do so. In PKI the key pair allows this feature.


Plain Text Message
Encryption process using receiver's public key
Encrypted message
Transmission medium
Decryption process using receiver's private key
Plain Text Message
The quick brown fox jumps over the lazy dog's back. The rain in Spain stays mainly in the plain.
Encryption Software
Decryption Software
The quick brown fox jumps over the lazy dog's back. The rain in stays mainly in the plain.
Key Pair
Sender
Receiver's Public Key
PUBLIC KEY CRYPTOGRAPHY
Receiver's Private Key
Receiver

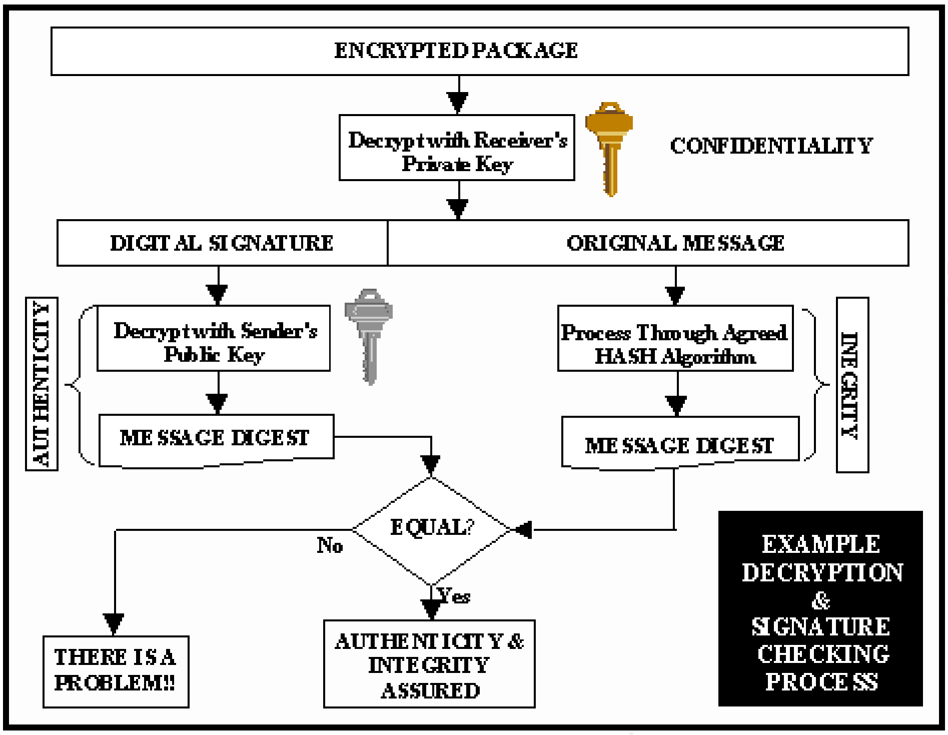
http://www.e-secure.com.au/

- **Integrity** – The integrity of the message is assured when it can be demonstrated that message delivered was the same one sent, via the use of a **digital signature.** The message digest is calculated by processing the message with a pre-agreed algorithm and encrypted using your private key, this is then decrypted using your public key by the recepient(PKI in reverse), whom then matches the message digest with the pre-agreed algorithm, any mismatch occurs in the calculation and tampering could of happened in what people call "man in the middle attacks". A person tries to masquerade as you by using the global public to send a message posing as someone else, or communications are "hijacked" between two parties, the imposter tries to alter the message and pass it onto the recepient. But a digital signature would help as any disruption would cause a mismatch in the message digest.


EXAMPLE ENCRYPTION & SIGNING PROCESS
ORIGINAL MESSAGE
Process Through Agreed HASH Algorithm
MESSAGE DIGEST
Encrypt with Sender's Private Key
DIGITAL SIGNATURE
DIGITAL SIGNATURE
ORIGINAL MESSAGE
Encrypt with Receiver's Public Key
ENCRYPTED PACKAGE

http://www.e-secure.com.au/

- **Authenticity** – When a key pair is issued, a Digital Certificate is also issued. A Digital certificate is a formatted file that binds a public key to an individual, application or service. When the owner of the certificate distributes it, the public key is included. The receiver of the pubic key uses the information in the certificate, along with a level of trust in the certificate issuer, to accept the public key is valid and comes from the person whom it is said to belong to. As above, the sender uses their private key and the message digest to create a digital signature. The sender's public key, which the recipient has and has trusted by virtue of the certificate, is able to dicipher the digital signature. If this process is successful, and the message digest equates to that calculated by the recipient, the Authenticity has been satisfied.


ENCRYPTED PACKAGE
Decrypt with Receiver's Private Key
CONFIDENTIALITY
DIGITAL SIGNATURE
ORIGINAL MESSAGE
AUTHENTICITY
Decrypt with Sender's Public Key
Process Through Agreed HASH Algorithm
INTEGRITY
MESSAGE DIGEST
MESSAGE DIGEST
EQUAL?
No
Yes
THERE IS A PROBLEM!!
AUTHENTICITY & INTEGRITY ASSURED
EXAMPLE DECRYPTION & SIGNATURE CHECKING PROCESS

http://www.e-secure.com.au/

- **Non-Repudiation** – Preventing the denial of previous commitments or actions. In other words proving that the message did in fact come from the correct sender, by the use of a certificate and digital signature.

In fact it is very important to note that when implementing any security system or securing any application and system that these four points be observed at all times as these are the four pillars of Information Security. The keys in question are called asymmetric keys and as opposed to symmetric keys, are generated as a pair, a public key, which can be shared or distributed to whomever needs to communicate with you and a private key, which is your private property. You don't share or distribute your private key to anyone. In PKI as I explained, uses to different keys, but are which mathematically related. You firstly generate your private key and then from that you compute your public key and from the public key we can create a shared message key. The idea of using key exchanges was derived from a couple of guys named Whitfield Diffie and Martin Hellman with input also from Merckle back in 1976. For PKI to work you would also require the use of an encryption algorithm, such as the ones described in types of ciphers. It is probably in your best interest to use only those ciphers that have gone through public scrutiny over the years and not some propriety algorithm built into some application that hasn't been scrutinised or debated through the international cryptographic community. Strong ciphers are strong because of their randomness and scrutinisation by experts not by their elusiveness to be scrutinised. Examples of algorithms that can be used in PKI are RSA, El Gamal, ECC . The strength of PKI does not only come from the ciphers used, but is a combination of many aspects. The privacy of your private key is of paramount importance, if your private key gets compromised, well it's game over and you are best to re-generate your key pairs, a hassle offcourse, but one which will allow your privacy to be ensured. There a couple of ways to keep your private key private. Firstly protect your private key with a passphrase, that way if anyone was to get to your private key, they would also have to obtain the password. If practical or economics allow for it, don't store your private key on a server that can be gotten to easily, or if you must, such as in the case of SSL, ensure the server or system has been hardened!! Use a smartcard or smart key tokens to store your private key, this way ensuring it is not left lying around on a system somewhere.

As we learned, for PKI to work we must combine a number of components including;

- A PKI vendor that will help install and consult on your encryption requirements. There are many companies now that sell PKI as part of their product range, and even just as many that help in the design and implementation of PKI, examples are found in the SANS site www.sans.org.
- A certificate authority like www.verisign.com,
- A strong security policies in place to detail such things as identifying and issuing people or systems with certificates and what is needed to qualify for a certificate with also guidelines on implementing, using and managing a PKI infrastructure within your organisation. These policies must also include a disaster recovery section in the event of a major incident caused by compromising any part of the PKI use (or misuse).
- Certificate distribution methods/system – a means to let all users know about other users, obtain certificates and notices. The PKI vendor or consultant can advise on this.
- An encryption algorithm that has been tested and scrutinised by the international cryptographic community. Example www.rsa.com.

It can be seen from the above that PKI is a framework that provides users (applications or services) with levels assurance about each other. It also provides the means through which information integrity may be checked. The privacy of communications is provided by the encryption and the use of the key pairs. Coupled with this is the use of digital certificates from a trusted certificate issuer to ensure validity of the public key and the use of a digital signature to sign a document to add a level of assurance that the message has not been tampered with. All in all PKI is not a single piece of software designed to protect your privacy, but a conglomerate of pieces combined to ensure that what we have taken for granted in the paper world to ensure our privacy can now be applied in the digital age.

9. PKI Implementations

PKI can and has been implemented in a variety of ways. SSL or Secure Socket Layer from the Netscape Corporation is one of the most popular methods used to encrypt communications between your browser and a web server for secure transactions. SSL uses both symmetric and asymmetric encryption to utilise their capabilities. You probably weren't aware of using SSL as the key exchanges happen in the background between your browser (client) and a server(transaction server). One noted problem with using SSL is the subject of valid certificates from the server. Most web servers don't have valid certificates so proving whom you are conducting business with becomes a problem, but if you reasonably assured of the sites validity then SSL is a secure means for conducting transactions over the Internet. The next time you trade shares, buy a product or view your financial information on your bank site have a look at the top URL address, if it is pre-pended with HTTPS:// instead of HTTP://, then you most probably have an SSL session activated. This encrypts the session using ciphers like triple DES(ensure you are using a strong cipher for SSL) to encrypt the traffic and can be used with both symmetric and asymmetric keys to ensure both confidentiality and performance as explained in the section Symmetric and Asymmetric before. As I said most of SSL happens without your knowledge of it happening when you visit a site, but another form of PKI that you would have to be more involved is PGP or Pretty Good Privacy developed by Philip Zimmermann in 1991. It goes along the same lines as PKI although there are some variances. The public key is usually signed by other PGP users on a PGP public server. This is known as the web of trust model, and it leaves it up to people to decide weather the public key they received is from a reputable source by viewing the signatures from other people that have signed the validity of the public key. Offcourse this method is open for debate because you don't have to verify or prove who owns the public key before signing it. I personally find PGP to be best at when you want to securely communicate e-mail over the Internet with friends or associates. You know who they are and they know you, so accepting public keys from each other is not such a worry.

PKI can be implemented in areas where electronic privacy is sought with the use of encryption, in such places as transferring sensitive files over your network, credit card transacting over a public network, encrypting E-mail and sending the message across the Internet, securing transactions or communications over WAP enabled devices, VPN's, secure authentication to servers….and the list goes on. Many factors come in to play when considering a PKI roll out. You have to consider such things as the cost to purchase a PKI solution or alternatively you can source an external company to undertake some or all the components of PKI within your organisation. You have to consider the administration costs associated with PKI and certificate management, you have to document the intended use, number of users, nature of the users, possible future use, nature of the transactions your trying to protect, and any legal issues before embarking down the PKI path.

References –

National Institute of Standards and Technology, U.S. Department of Commerce(NIST) Advanced Encryption Standard (AES) Development Effort. (AES).
http://csrc.nist.gov/encryption/aes/

"Understanding encryption and SSL"
http://developer.netscape.com/docs/manuals/enterprise/mngserv/security.htm

Internet X.509 Public Key Infrastructure
Aresenault. A, Turner. S, PKIX Working Group "Document: draft-ietf-pkix-roadmap-06.txt " November 2000
http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-06.txt

"DISCUSSION ON PUBLIC KEY INFRASTRUCTURE – White paper"
http://www.e-secure.com.au/

RSA – Frequently asked questions about today’s Cryptography.
URL: http://www.rsasecurity.com/rsalabs/faq/index.html

Schneier. Bruce , John Kelsey, “Twofish: A 128-Bit Block Cipher". URL:
http://www.counterpane.com/twofish-paper.html

Paddon, Michael, “ Plain Cryptography Primer part 2”, IT Security magazine(Australian), June/July 2000.

National Cryptologic Museum
http://www.nsa.gov/museum/

Last Updated: October 17th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	**SEC401 - 201710,**	**Oct 23, 2017 - Nov 29, 2017**	**vLive**
SANS Seattle 2017	**Seattle, WA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS San Diego 2017	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**vLive**
SANS Gulf Region 2017	**Dubai, United Arab Emirates**	**Nov 04, 2017 - Nov 16, 2017**	**Live Event**
SANS Miami 2017	**Miami, FL**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
Community SANS Vancouver SEC401^	**Vancouver, BC**	**Nov 06, 2017 - Nov 11, 2017**	**Community SANS**
Community SANS Colorado Springs SEC401~	**Colorado Springs, CO**	**Nov 06, 2017 - Nov 11, 2017**	**Community SANS**
SANS Sydney 2017	**Sydney, Australia**	**Nov 13, 2017 - Nov 25, 2017**	**Live Event**
SANS Paris November 2017	**Paris, France**	**Nov 13, 2017 - Nov 18, 2017**	**Live Event**
SANS London November 2017	**London, United Kingdom**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
Community SANS Portland SEC401	**Portland, OR**	**Nov 27, 2017 - Dec 02, 2017**	**Community SANS**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
Community SANS St. Louis SEC401	**St Louis, MO**	**Nov 27, 2017 - Dec 02, 2017**	**Community SANS**
SANS Khobar 2017	**Khobar, Saudi Arabia**	**Dec 02, 2017 - Dec 07, 2017**	**Live Event**
SANS Munich December 2017	**Munich, Germany**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**
Community SANS Ottawa SEC401	**Ottawa, ON**	**Dec 04, 2017 - Dec 09, 2017**	**Community SANS**
SANS Austin Winter 2017	**Austin, TX**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**
SANS vLive - SEC401: Security Essentials Bootcamp Style	**SEC401 - 201712,**	**Dec 11, 2017 - Jan 24, 2018**	**vLive**
SANS Bangalore 2017	**Bangalore, India**	**Dec 11, 2017 - Dec 16, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	**Washington, DC**	**Dec 14, 2017 - Dec 19, 2017**	**vLive**
SANS Security East 2018	**New Orleans, LA**	**Jan 08, 2018 - Jan 13, 2018**	**Live Event**
Community SANS Hawaii SEC401	**Honolulu, HI**	**Jan 08, 2018 - Jan 13, 2018**	**Community SANS**
Community SANS Nashville SEC401^	**Nashville, TN**	**Jan 08, 2018 - Jan 13, 2018**	**Community SANS**
Mentor Session - SEC401	**Memphis, TN**	**Jan 09, 2018 - Mar 13, 2018**	**Mentor**
SANS Amsterdam January 2018	**Amsterdam, Netherlands**	**Jan 15, 2018 - Jan 20, 2018**	**Live Event**
Northern VA Winter - Reston 2018	**Reston, VA**	**Jan 15, 2018 - Jan 20, 2018**	**Live Event**
Mentor Session - SEC401	**Minneapolis, MN**	**Jan 16, 2018 - Feb 27, 2018**	**Mentor**
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	**Las Vegas, NV**	**Jan 28, 2018 - Feb 02, 2018**	**vLive**
SANS Las Vegas 2018	**Las Vegas, NV**	**Jan 28, 2018 - Feb 02, 2018**	**Live Event**