# A Problem with Public Key Encryption and PKI

# .Introduction

Public Key encryption provides an important functionality to Internet communications to allow the transfer of confidential information *when the two parties involved do not have the opportunity to exchange a key or keys ahead of time by some method that is inherently secure*, e.g. traditional postal mail. It is the best approach that has been evolved to date for this specific need.

In other situations, *where the safe transfer of a key or keys can be made ahead of time,* Public Key encryption (Asymmetric Encryption) is inferior to Symmetric Encryption.

# . Symmetric and Asymmetric Encryption in Brief

## ..Symmetric Encryption

Symmetric encryption involves the use of a key that we will call the Symmetric Key.

This Symmetric Key will be used to encrypt a message. This <u>very</u> <u>same</u> Symmetric Key must be used to decrypt the message. There is only <u>one</u> key in Symmetric Encryption - the Symmetric Key.

### ...Example

Alice wants to send an encrypted message to Tom, say over the Internet. Therefore, Alice has to find a way to safely get the Symmetric Key to Tom.

Inasmuch as Alice encrypts her message before sending it over the Internet, it is clear that she does not consider the Internet to be a secure way to send messages. She fears, rightly so, that somehow her message could get into the hands of some person other than the intended recipient. Since Alice's premise is that the Internet is not secure (without encryption) she may use traditional postal mail to send the Symmetric Key to Tom. She could also hand the Symmetric Key to Tom, saying, "Any time in the future that I want to send you a secure message, I will use this Symmetric Key. With this Symmetric Key you can decrypt the message I send to you."

Interestingly, this one Symmetric Key can be used for either of these two parties to send encrypted messages to each other. As noted later in this paper, Asymmetric Encryption is not this way.

## .. Asymmetric Encryption - Public Key Encryption

Asymmetric Encryption uses two keys, a Private Key and a Public Key.

- The Public Key is used to encrypt a message.
- The Private Key is used to decrypt a message.

This is where the term “asymmetric” comes from. Different keys are used on each end of an encrypted communication between two parties.

Someone who wants to receive an encrypted message will use PC-based software to generate these two keys, as a pair of keys. Then the Public Key will be sent to the party who has the message to send. When the encrypted message is received, the Private Key will be used to decrypt it.

There is an important feature here. Assume that the Public Key is sent over the Internet. In many cases we don’t care if the Public Key is intercepted. The Public Key is only used here to encrypt a message. In many cases it does not matter if a hostile party has the Public Key. All they would gain from that is the ability to send their own encrypted message. As noted later in this paper, this could be a problem of a different nature.

### ...Example

Alice wants to send an encrypted message to Tom, say over the Internet. In order to do this, Alice has to request that Tom create a Public Key - Private Key pair, and send the Public Key to her. Tom does not need to find a way to safely get a key to Alice because Tom will send the Public Key and if the Public Key is intercepted, that does not allow an intercepting party to decrypt the message that he sends to Alice.

Note that the Public Key that Tom sends to Alice is for transmittal of **messages from Alice to Tom**. For the reverse, **messages from Tom to Alice**, Alice must create her own Public Key-Private Key pair and send that Public Key to Tom.

## ..Public Key (Asymmetric Encryption) - an Inherent Problem

One of the prime advantages of Public Key Encryption leads to one of its most significant problems - conducting e-commerce.

## ..Example

Alice wants to make an online purchase from abcstore.com. She will have to type her credit card number into her browser. She is worried that either abcstore.com may not be careful with her credit card number, or even be dishonest. In addition, she has heard about the so-called man-in-the-middle problem where someone gets in between her and abcstore.com and she ends up giving her credit card info to someone else who is eavesdropping.

The Public Key Infrastructure is designed to solve this problem with the use of a Certificate.

A Certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key.

A Certificate Authority (CA) is an entity that validates identities and issue certificates

The certificate issued by the CA binds a particular public key to the name of the abcstore.com. Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with abcstore.com’s private key.

In addition to a public key, a certificate always includes the name of abcstore.com, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA's digital signature allows the certificate to function as a "letter of introduction" for users who know and trust the CA but don't know abcstore.com.

When Alice types in the URL, abcstore.com, she will notice that:
the http:// in her address box of her browser has changed to:
https://

The extra “s” means that this is a secure transaction using Secure Sockets Layer (SSL).

Behind the scenes, Alice’s browser is getting a certificate from the abcstore.com server. Recall that the certificate was issued by a CA.

In that certificate is a Digital Signature from the CA. Now Alice’s browser decrypts the Digital Signature with the Public Key she received from the abcstore.com server. The browser then compares that decrypted digital signature with the digital signature and Public Key that Alice already has on her computer for that specific CA. If they match, then she can feel that the certificate she has received is good and that she can trust the abcstore.com server.

## ..What Is Wrong With This?

The problem is basically that the arena-of-trust is getting larger and larger, and a strong profit motive (for the CA business) could result in a great deal of interest in being a CA, including companies who won't do a good job at an extremely critical function.

It is not simply that Alice is interacting with abcstore.com. She is now interacting with a CA. If she does business with several or many online stores, she may be interacting with information and services of several CAs.

Providing certificates can be an attractive business. It does not take a significant staff to man a few Certificate-issuing servers. The cost to make a certificate, incrementally, is almost zero. It is estimated that the world-wide market for certificates is 45 million servers. If you issue certificates for $100 per year and have only 100,000 clients, that's $10 million per year in revenue for a small staff and a few servers. It can be very attractive business. Are people getting into it for the money without attention to performing a worthy job?

CAs are associated with the word "trust". Who gave the CA its claimed "authority" and "trust"? The companies issuing the CAs gave it to themselves.

# .Summary and Conclusions

Symmetric encryption is inherently more secure than Asymmetric encryption. Symmetric encryption has not yet been made to work for the e-commerce mass market; therefore, asymmetric encryption and the PKI together are the umbrella of e-commerce today. This structure, however, suffers from the basic architecture of a "Public Key" (i.e. a non-secure key) and a CA business model that may be too lucrative.