3.5.2 Digital signatures and digital certificates

What is a digital signature?

It is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Digital signatures rely on certain types of encryption to ensure authentication. You already know what encryption is from the last section. Authentication as mentioned above is the process of verifying that information is coming from a trusted source. Encryption and Authentication work hand in hand for digital signatures.

There are several ways to authenticate a person or information on a computer:

- **Password –** The use of a username and password provide the most common form of authentication. You enter your name and password when prompted by the computer. It checks the pair against a secure file to confirm. If either the name or password do not match, then you are not allowed further access.

- **Public key encryption –** It uses a combination of a private key and a public key. The private key is known only to your computer while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key provided by the originating computer and its own private key.

  The key is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value.

Here's a simple example:

-Input number: 10667
-Hashing Algorithm = (Input #) x 143

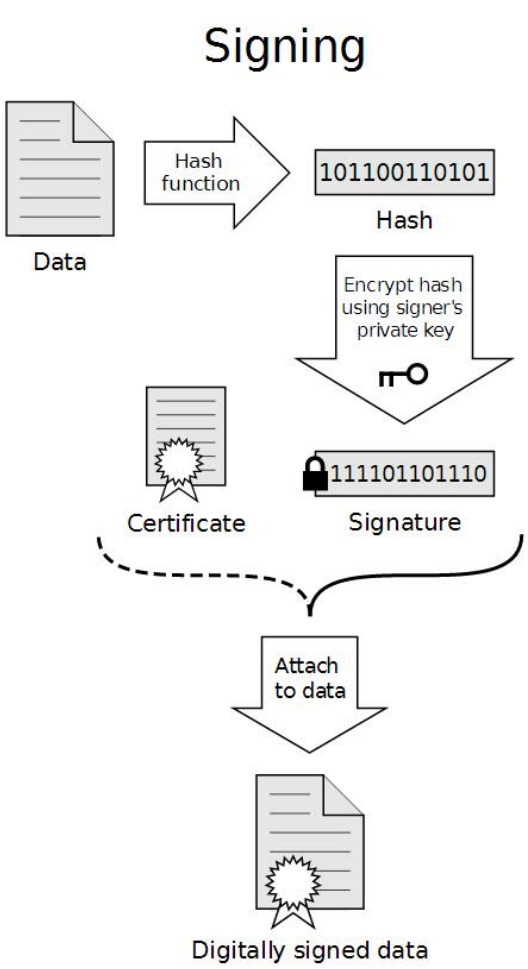
Hash value = 10667 x 143 = 1525381

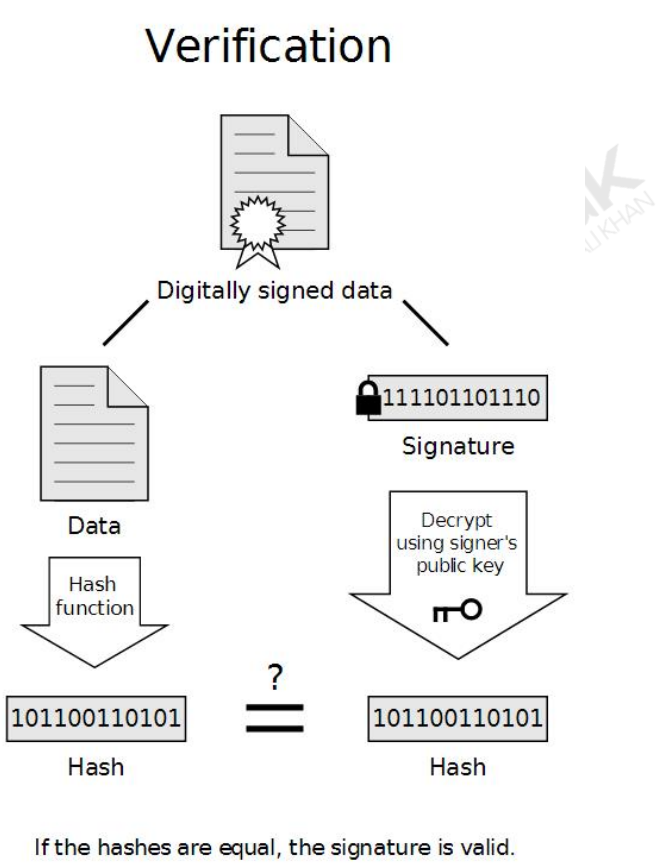
You can see how hard it would be to determine that the value of 1525381 came from the multiplication of 10667 and 143. But if you knew that the multiplier was 143, then it would be very easy to calculate the value of 10667.

To implement public key encryption on a large scale would require a different approach. This is where digital certificates come in. A digital certificate is essentially a bit of information that says the Web server is trusted by an independent source known as a **Certificate Authority (CA).** The CA acts as the middleman that both computers trust. It confirms that each computer is in fact who they say they are and then provides the public keys of each computer to each other.

3.5.2 Digital signatures and digital certificates

To re-iterate points, A **digital signature is used to verify a message.** You could say that is an encrypted hash of the message. The recipient can check if the message was tampered with by hashing the received message and comparing this value with the decrypted signature. To decrypt the signature, the corresponding public key is needed.





3.5.2 Digital signatures and digital certificates

What is a digital certificate?

An **attachment** to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

An individual wishing to send an encrypted message applies for a digital certificate **from a Certificate Authority (CA).** The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through the internet.

The recipient of an encrypted message uses the public key to decode the digital certificate attached to the message and then verify the key as a legitimate key from the CA. The recipient also receives the public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

Today, there are a number of authorities which provide digital certificates; one of them is "**Verisign"**

The procedure to obtain your own digital certificate is a standard procedure and not a very hard one.

It starts with you opening your web browser and navigating to their website. There will be a form which you have to fill in with your personal details and the type of certificate you wish to apply for. Enter your details and pick the level of security you wish to attain on your certificate this procedure usually asks for a fixed fee to be paid before you are entitled to actually use the certificate.

After all the details have been approved and the fee has been paid, A pop-up window will show with information about your certificate. Click on the Install button to install the certificate in your web browser.

Now all the encryption and decryption of messages will be done automatically thanks to your new digital certificate.

To re-iterate points, **A digital certificate** is used to bind public keys to people or other entities. If there were no certificates, the signature could easily be faked because the recipient would be unable to check if the public key belongs to the sender.

The certificate itself is signed by a trusted Certificated Authority like VeriSign.