3.5.1 Asymmetric keys and encryption methods

In Chapter 1.6, you were introduced to the concepts of Data security and integrity. In this topic, we are going to build on the concepts learned previously giving more attention to how data is transferred over the Internet securely.

When an organization or any source on the internet opens some of its network facilities up, there is a problem of confidentiality of data. An organization may well wish that potential customers have access to their product database. However, they will not want them to have access to personal files.

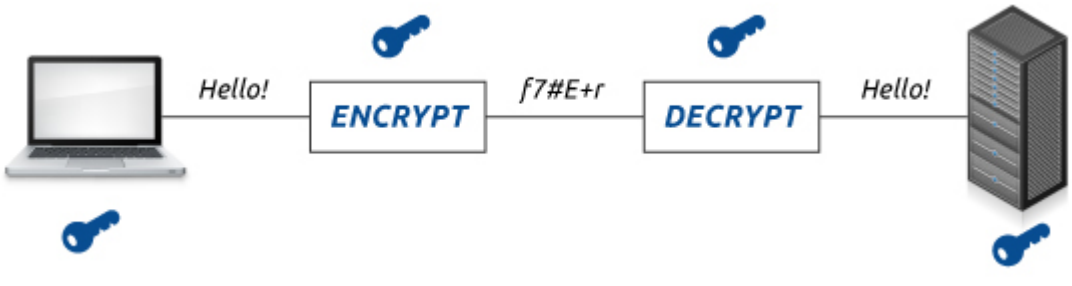
One solution to this problem could be to **encrypt** the data.

Encryption is applying a mathematical function using a key value, to a message so that it is scrambled in some way. There are many techniques for this. The problem is to make it virtually impossible for an unknown user to unscramble the message. Clearly, whatever function is applied to the original message must be reversible. The problem is to make it very difficult for an unwanted user to find the inverse of the original function. It also means that there is a problem of many wanted people needing to decrypt the message. All these people need the key to unlocking the message. This makes it highly likely that an unwanted person will get a hold of this key.

One method of overcoming this is to use the **Symmetric key encryption.**

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt messages **using the same key.**

It uses a single key for both encryption and decryption. The one single key is needed for both computers to communicate.

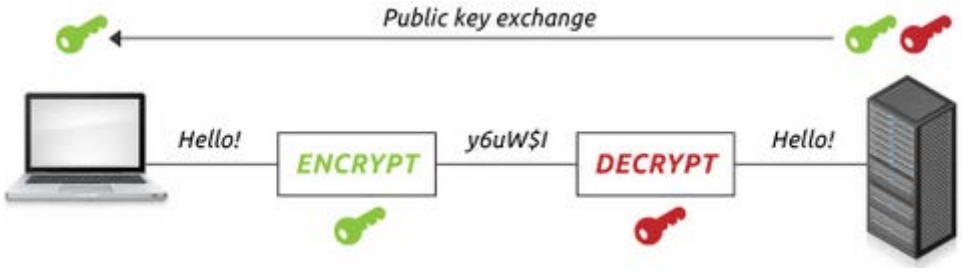


The main issue with Symmetric encryption is that the same key is used for encryption and decryption. Which means that if the key falls into the wrong hands, then your data is no longer confidential to a group of people.

This issue is resolved using another technique called **Asymmetric key encryption.**

Also termed as (public-key cryptography) uses a secret key for encryption and decryption.

3.5.1 Asymmetric keys and encryption methods



This involves the sender having a **public key** to encrypt the message and only the receiver having the **private key** to decrypt the message. Anyone can use the public key to encrypt a message. However, private keys are kept secret. This way only the intended receiver can decrypt the message.

Which Is Stronger?

Since asymmetric keys are bigger than symmetric keys, data that is encrypted asymmetrically is tougher to crack than data that is symmetrically encrypted. However, this does not mean that asymmetric keys are better. Rather than being compared by their size, these keys should compared by the following properties: computational burden and ease of distribution.

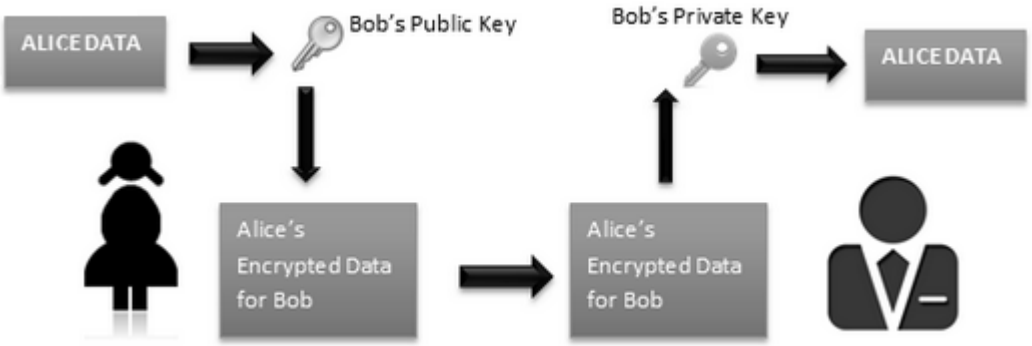
Symmetric keys are smaller than asymmetric, so they require less computational burden. However, symmetric keys also have a major disadvantage—especially if you use them for securing data transfers. Because the same key is used for symmetric encryption and decryption, both you and the recipient need the key. If you can walk over and tell your recipient the key, this isn't a huge deal. However, if you have to send the key to a user halfway around the world (a more likely scenario) you need to worry about data security.

Asymmetric encryption doesn't have this problem. As long as you keep your private key secret, no one can decrypt your messages. You can distribute the corresponding public key without worrying who gets it. Anyone who has the public key can encrypt data, but only the person with the private key can decrypt it.

3.5.1 Asymmetric keys and encryption methods

In order to understand how public key cryptography works, suppose Alice and Bob wish to send secure mail to each other:

- First, both Bob and Alice need to create their public/private key pairs. This is usually done with the help of a Certification Authority (CA).
- Alice and Bob then exchange their keys. This is done by exchanging certificates.
- Bob can then use his private key to digitally sign messages, and Alice can check his signature using his public key.
- Bob can use Alice's public key to encrypt messages, so that only she can decrypt messages for him to read.
- Similarly, Alice can use Bob's Public key to encrypt messages, so that only he can decrypt her messages.



So after reading the page above, you should be familiar with a few terms:

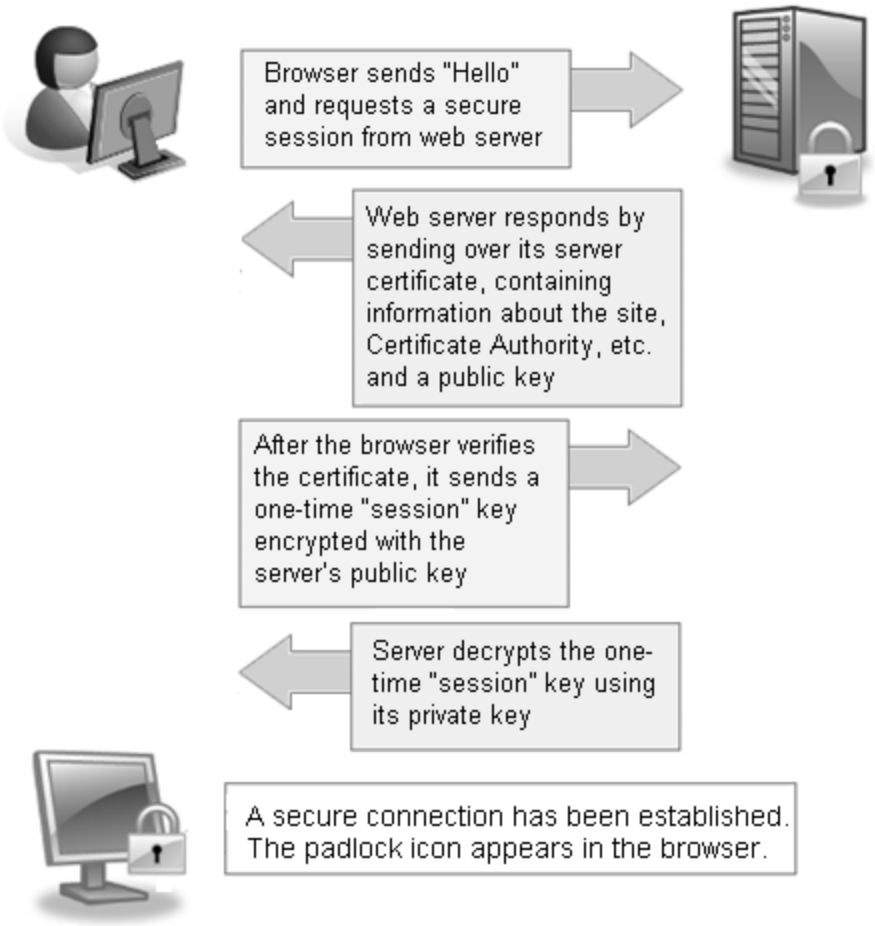
- A **public key** is used to encrypt files, so that the data is un-readable to humans.
- A **private key** is used to decrypt files, so that the encrypted file can be reverted back to the normal human readable data.
- A **plain text** is data which can be read and amended by humans
- A **cipher text** is encrypted data which cannot be read by humans
- **Encryption** is the process of translating human readable plain text into unreadable cipher text for the purpose of data security.
- **Asymmetric key cryptography** is the process of using public key and private key to send data over the internet securely as described above.

3.5.1 Asymmetric keys and encryption methods

Encryption does not only apply to data. It could also be used to secure a connection between a user and an internet server to ensure the user that the data being sent over the internet is secure and not being tampered with by hackers or anyone else of that sort.

A primary advantage of Asymmetric key cryptography is the application of digital signatures, which help combat repudiation i.e. the denial of involvement in a transaction. Since the owner keeps their private key a secret, anything signed using that key can only have been signed by the owner.

The predominant Asymmetric key algorithm is RSA, which was developed in 1977 by, and named after, Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is included as part of Web browsers and also forms the basis for many products.



How https works inside the browser using public private keys and certificates