1. DNS Lookup
2. Browser sends an HTTP request
3. Server responds and sends back the requested HTML file
4. Browser begins to render HTML
5. Browser sends additional requests for objects embedded in the html file (CSS files, images, javascript, etc.)

**1=Triple DES**

[Triple DES](https://www.tutorialspoint.com/cryptography/triple_des.htm) was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more accurate. Despite slowly being phased out, Triple DES has, for the most part, been replaced by the Advanced Encryption Standard (AES).

**2=AES**

The [Advanced Encryption Standard (AES)](https://www.tutorialspoint.com/advanced-encryption-standard-aes) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes.

AES is largely considered impervious to all attacks, except for brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

**3=RSA Security**

[RSA](https://www.comparitech.com/blog/information-security/rsa-encryption/) is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You’ve got your public key to encrypt the message and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers a lot of time and processing power to break.

**Hashing is the process of converting any input of any length into a fixed sized string of text using a mathematical function.**

* **Hashing**: Is a one-way summary of data, cannot be reversed, used to validate the integrity of data.
* **Encoding**: Reversible transformation of data format, used to preserve usability of data.
* **Encryption**: Secure encoding of data used to protect confidentiality of data.

|  |  |
| --- | --- |
| Adler32 | 1c49043e |
| CRC32 | 1c291ca3 |
| Haval | 2242f559aa860d68c6de6d025e65d32e |
| MD2 | 315f7c67223f01fb7cab4b95100e872e |

* GET requests can be cached
* GET requests remain in the browser history
* GET requests can be bookmarked
* GET requests should never be used when dealing with sensitive data
* GET requests have length restrictions
* GET requests are only used to request data (not modify)
* POST requests are never cached
* POST requests do not remain in the browser history
* POST requests cannot be bookmarked
* POST requests have no restrictions on data length