4. These keys transform the messages and data into "digital gibberish" through encryption and then restore them to their original form through decryption. Generally speaking, the longer the key is, the more difficult it is to crack the code. This is true because deciphering an encrypted message by brute force would require the attacker to try every possible key. Test messagesutilizing the early US Government-approved cipher DES, which has an effective key length of 56 bits, have been deciphered using brute force key search. But as technology improves, so does encryption quality. The development of asymmetric key ciphers, sometimes known as public key ciphers, is one of the most significant developments in the study of cryptography after World War 2. These techniques encrypt the same message using two keys with close mathematical ties.Because it is very difficult to figure out one key just by knowing the other, several of these algorithn1s allow disclosure of one of the keys.

A widely accepted standard for encryption became necessary starting in the 1990s as businesses started using the Internet and conducting transactions there. Prior to the release of the Advanced Encryption Standard (AES), only ve1y seldom was information sent via the Internet encrypted, most frequently using the Data Encryption Standard (DES).After a public call for candidates for such a cipher algorithm and a competition among those contenders, NBS (a US Government agency) accepted this for its security. Due to complicated disputes concerning the widespread use of high-quality encryption by the general public, DES was approved for a brief time but was in use for a longer time. DES was finally superseded by the AES following a second open competition held by NIST, the organization that would succeed the NBS. Public-key encryption techniques started to be used more frequently in the late 1990s and early 2000s, and soon a combination of the two became the standard method for conducting e-commerce transactions. Online transactions were also made possible by the development of a new protocol known as the Secure Socket Layer, or SSL. SSL was used for a variety of transactions, including buying items, paying bills online,and banking. Additionally, when wireless Internet connections spread throughout homes, the demand for enc1yption increased because these commonplace circumstances required a certain amount of protection.