4. Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to their original form through decryption. In general, the longer the Key is, the more difficult it is to crack the code. This holds true because deciphering an encrypted message by brute force would require the attacker to try every possible key. To put this in context, each binary unit of information, or bit, has a value of 0 or 1. With modern technology, cyphers using keys with these lengths are becoming easier to decipher. DES, an early US government-approved cypher, has an effective key length of 56 bits, and test messages using that cypher have been broken by brute force key search. However, as technology advances, so does the quality of encryption. Since World War 2, one of the most notable advances in the study of cryptography is the introduction of asymmetric key cyphers (sometimes termed public-key cyphers). These are algorithms that use two mathematically related keys for encryption of the same message. Some of these algorithms permit the publication of one of the keys, due to it being extremely difficult to determine one key simply from knowledge of the other.

Beginning around 1990, the use of the Internet for commercial purposes and the introduction of commercial transactions over the Internet called for a widespread standard for encryption. Before the introduction of

the Advanced Encryption Standard (AES), information sent over the Internet, such as financial data, was encrypted if at all, most commonly using the Data Encryption Standard (DES). This had been approved by NBS (a US Government agency) for its security, after a public call for, and a competition among, candidates for such a cypher algorithm. DES was approved for a short period but saw extended use due to complex wrangles over the use by the public of high-quality encryption. DES was finally replaced by the AES after another public competition organized by the NBS successor agency, NIST. Around the late 1990s to early 2000s, the use of public-key algorithms became a more common approach for encryption, and soon a hybrid of the two

schemes became the most accepted way for e-commerce operations to proceed. Additionally, the creation of a new protocol known as the Secure Socket Layer, or SSL, led the way for online transactions to take place. Transactions ranging from purchasing goods to online bill pay and banking used SSL. Furthermore, as wireless Internet connections became more common among households, the need for encryption grew, as a level of security was needed in these everyday situations|