I have come across several new and interesting encryption methods while on researching for this report. My favorite method that I have found is quantum cryptography. Before I discuss the encryption methods, I discuss a few helpful things about encryption and decryption.

According to Stallings, encryption is “the conversion of plaintext or data into unintelligible form by means of a reversible translation, based on a translation table or algorithm.” Decryption is defined by Stallings as “the translation of encrypted text or data (called ciphertext) into original text or data (called plaintext).” Encryption can be done a number of ways. Two popular methods are asymmetric and symmetric. Asymmetric, or public-key cryptography uses two different keys, one public and one private. This method is where plaintext is encrypted using the public key and the ciphertext is decrypted by the private key. Both keys are mathematical; the private key is kept secret, and the public is made known. Symmetric cryptography uses the same key to encrypt and decrypt, thus the key must remain a secret.

Quantum Cryptography
Quantum cryptography allows for two people to transfer information through an absolutely secure quantum channel. The key is produced by a process called quantum key distribution. Quantum key distribution happens by one of the users sending a sequence of photons with random polarizations. That sequence is then used to create a series of numbers.

Quantum cryptography has the ability to detect eavesdroppers as well. This is accomplished by following Heisenberg's uncertainty principle which states that “certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other one” (Vittorio). Therefore if an eavesdropper disturbs the channel (i.e. tries to measure the key), the disturbance will be detected and the sender will send a new key.

Message Digest Cryptography
Message Digest algorithm 5 (MD5) is mostly used in security applications and also in file integrity. MD5 encrypts a message of any variable length by processing it into a fixed-length output of 128 bits. These 128 bits are broken into four 32 bit “words,” designated A, B, C, and D, which are all initialized into specific fixed constants.

The input message itself is broken into “512-bit blocks”, and the MD5 algorithm then runs on each block. The 512 bit blocks are also padded in order to make the length is divisible by 512 (Wikipedia). The padding is accomplished by attaching a bit, 1, to the end of the message, then attaching zeros until the length is 64 bits fewer than a multiple of 512. The remaining 64 bits are filled by an integer representing the size of the original message. MD5 does have its design flaws, thus making the use of the algorithm debatable.

Elliptic Curve Cryptography
Elliptic curve cryptography (ECC) is an appealing algorithm because it provides the
same level of security as standard methods, such as RSA, but with a shorter key. As technology is producing tougher, more powerful processors, the shorter key makes elliptic curve cryptography more practical. The base of ECC is derived from the Diffie Hellman method, which uses an asymmetric operation based on a discrete logarithmic problem.

Of course, I had to understand some of the older encryption algorithms before I could really understand and realize the importance of the newer algorithms and methods.

**Data Encryption Standard**

The Data Encryption Standard (DES) is a very old and familiar encryption standard. Developed in the 1970s, it became the first standard used by the United States federal government. DES uses a symmetric key encryption, where the message is encrypted and decrypted with the same key. DES encrypts by breaking up the original message into 64 bit blocks, then encrypting each block with a 56 bit key. This algorithm was broken by brute force, thus giving birth to 2DES and 3DES. 2DES and 3DES are both based on DES, but have more encryption keys. For example, 3DES first encrypts with each 64 bit block with one key, then encrypts again with another key, and finally again with another key.

**RSA Cryptography**

Named after its developers, Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is a widely used and secure asymmetric encryption algorithm. RSA has a public key and a private key. The public key is created by the user choosing two large prime numbers p & q, then multiplying p * q to get N. Another number, e, is chosen that must be relatively prime to (p-1)(q-1). Then the message, M, is encrypted by the following calculation: C = M^e(mod N), where C is the encrypted message. To decrypt the message, the user must find a number d that ed = 1(mod (p-1)(q-1)), then calculate C^d(mod N).

**Advanced Encryption Standard Cryptography**

The Advanced Encryption Standard, also known as Rijndael, is another familiar encryption standard. It encrypts and decrypts the message in 128 bit blocks using symmetric keys of either 128, 192, or 256 bits. Encryption is accomplished by encrypting and re-encrypting each 128 bit block a variable number times (depending on the length of the key) known as rounds. There are several different methods of using AES keys, such as the Electronic Code Book method, which encrypts each 128 block independently.
Works Cited


