Advances in Cryptology: An Introduction to Quantum Cryptography

Johanna N. Barreto

The following discussion presents the development and growth of cryptology. It explores the very first methods used to hide secret messages from unauthorized individuals; the ones utilized today; and finally, promising methods for the future. The battle between code makers and code breakers, and the advances of technological innovations, have forced the continuous development of cryptology. The world depends on security to prevent identity or property theft. The purpose of this work is to identify some cryptographic techniques that can be used to securely transmit data through computer networks.

Cryptography (in Greek *crypto* means hidden and *graphein* means to write) is the art of developing secret codes and ciphers. Cryptanalysis is the art of breaking them, often called eavesdropping. The study of both is cryptology which is mostly used in network security. It involves software to create algorithms, and hardware to send and receive information. This project concentrates on the following types: Classical, Modern, and Quantum Cryptography (Singh).

Classical cryptography started two thousand years ago with the need to secure communications. Kings, queens, and heads of the military relied on it to protect their country or themselves from the enemy. Fear was the main motive that generated the creation of secret codes and ciphers. Prior to that, messages were hidden instead of coded, which came to be known as steganography (in Greek *steganos* means covered). For instance, a message was hidden within a hard-boiled egg; ink made from aluminum and vinegar was used to write on the shell. The ink penetrated the shell and the message would become invisible. Only the intended recipient could read the message by removing the shell. However, any method that is discovered by the enemy forces a change to create a better method. Julius Caesar was the first one to implement a substitution cipher (Caesar Shift) that consisted of shifting the letters of the alphabet a number of places to the right or left. Cryptanalysts began to use frequency analysis to encipher the intercepted messages. In the English language, some letters are used more often than others.

For example, the letter *e* has the highest frequency while the *x* has the lowest. Such a sophisticated technique was challenged when a poly-alphabetic substitution cipher was implemented. It utilized more than one Caesar shift to encrypt the message (Vigenère Shift). It was an added security feature, but it was not invincible. These methods, however, stood strong for decades, helping win and lose wars between countries or opposite parties (Bosworth; Singh; Washington).

Modern cryptography has reached a very high level of security to protect government and banking transactions. It involves complicated mathematical functions that only a computer can solve within a reasonable time. The creation of integrated circuits and of computers facilitated the advancement of cryptology. On the one hand, cryptographers could input a plaintext and let a computer program output the corresponding cipher-text. On the other hand, cryptanalysts could check for thousands of possible keys that would produce a meaningful plaintext. What makes it possible for methods such as the DES and RSA algorithms to be secure is the time it takes to find the secret key. The DES (Data Encryption Standard) was first submitted by IBM with the name *Lucifer* to the NBS (National Bureau of Standards). The NBS or NIST (National Institute of Standards and Technology) made it the official data encryption standard in 1977. The major concern up to this point had been the "key distribution problem," because the sender and the receiver needed to have met at least once before to coordinate the key. Another alternative is to send a courier with the key which reduces the security of the system and increases the expense. The objective was to find a way to encrypt a message without the inconvenience of the key distribution. The solution was a Public Key Cryptosystem that consisted of two different keys: the public key and the private key. The RSA uses that technique, providing more security and freedom to send the public key through a corrupted transmission cable. The RSA was proposed by Rivest, Shamir, and Adleman in 1977. This method has proven to be effective and is now being used by banking institutions and government agencies (Singh; Washington).

Quantum Cryptography is the newest and most secure way to protect data traveling in a network. The data is translated into light pulses and its carrying-channel is an optical fiber. Fiber optics is a leading-edge technology that is already replacing the traditional metallic cables because of the safety and speed of its transmission capability. This subject is still in research and development. It is based on quantum mechanics and physics because in principle it can perform computations that classical computers cannot. One of the characteristics that makes Quantum Cryptography secure is that the data will never be compromised by an intrusion because only by observing the light will the pulses be changed. In addition, the intrusion can be detected by the sender and receiver for the same reason (Hesseldahl).

Caesar Cipher

Each letter of the message is shifted a number of places to the right or to the left in the alphabet.

Alice (sender) and Bob (receiver) must agree in a secret key to be able to encrypt and decrypt the messages they wish to send to each other. The key is the number of places in the alphabet to be shifted (Bosworth).

The encryption takes that key and shifts each letter in the plaintext that number of places to the right.

The decryption takes the key and shifts each letter of the cipher-text to the opposite side, to the left.

Frequency Analysis: Cryptanalysts began to use frequency analysis to encipher the intercepted messages. For instance, the letter *e* has the highest frequency while the *x* has the lowest. Even with the Caesar Shift, there will be one letter that appears more often than others and that will most probably be the substitute for the letter *e*.

Vigenère Cipher

The Vigenère cipher is a poly-alphabetic substitution cipher that involves the use of two or more cipher alphabets. A secret word is used to identify which cipher alphabet to use with each and every one of the letters. The secret word is repeated as many times as necessary to encrypt all the letters of the plaintext. The process starts by identifying the first letter of the keyword which tells us that the cipher alphabet starts with that letter. Then, the first letter of the plaintext is going to be encrypted according to that alphabet. The second letter is going to be encrypted according to the second letter of the keyword. It is simply a different Caesar Shift for each letter of the plaintext.

It is meant to increase the security of the communication between Alice, the sender, and Bob, the receiver. Eve, the intruder or eavesdropper, cannot use the Frequency Analysis technique to reveal the message (Singh).

For cryptanalysts, it became more difficult to break this cipher. However, if the message were long enough, frequency analysis could be possible by finding the length of the key. Frequency analysis could be used separately on the letters encrypted by the same letter of the keyword.

DES Algorithm

The DES Algorithm follows a set of standard steps to encrypt a message. The decryption process, as always, is the inverse of encryption. It is a block cipher, which means that it takes a block of sixty-four bits, and encrypts each block separately. The message must be converted into its binary ASCII equivalent. A binary number is a string of ones and zeros, each representing a bit. A single character is stored in bytes and a byte represents a group of eight bits. Therefore, the DES takes eight characters at a time for encryption, and then takes the following eight characters separately (Washington). The algorithm involves permutations and XOR bit-wise operations.

The DES is faster than the RSA Algorithm, which makes it more suitable for the fast world we live in. The RSA, then, is used to encrypt the DES key which solves the "key distribution problem."

RSA Algorithm

The RSA Algorithm has proven to be the most secure and convenient method for the encryption of messages. Although it is easier than the previous method, DES, a computer can take longer processing the information. That is the reason why the RSA is most often used to send the secret key needed for methods such as the DES, instead of being used for the encryption of a message.
It is called a "Public key cryptosystem" or an "Asymmetric system" where there are two separate keys, one for encryption and the other for decryption. All the previous methods are called symmetric due to the fact that Alice and Bob have the same key.

Bob has the two keys: the private key (must be kept secret) and the public key (can be published in a phone directory or on the Internet). Anyone who wants to send a message to Bob can look up his public key and encrypt the message using a standard formula. Neither Eve nor Alice can deduce the private key from the public key. Therefore, Alice can encrypt a message to Bob with his public key and he is the only one with the private key that can decrypt it (Washington).
RSA Algorithm:
Step 1: Bob chooses secret primes p and q and computes $n = p \cdot q$.
Step 2: Bob chooses the encryption key, e, with $\gcd (e, (p-1) (q-1)) = 1$.
Step 3: Bob computes the decryption key, d with $d \cdot e^{-1} \pmod{(p-1)(q-1)}$.
Step 4: Bob makes n and e public, and keeps p, q, d secret.
Step 5: Alice encrypts m as $c = m^e \pmod{n}$ and sends c to Bob.
Step 6: Bob decrypts by computing $m = c^d \pmod{n}$.

The only way for Cryptanalysts to find the plaintext is to factor *n* into its primes, *p* and *q*. By knowing the values of *p* and *q*, we can find the decryption key, *d*. However, the RSA is a one-way function: "It is easy to compute but difficult to invert."

The factorization of *n* is very difficult, almost impossible. This is what makes the RSA secure.

Quantum Cryptography

A quantum is an indivisible entity of energy. In Latin, *quantus* means "how much." For instance, a photon is a "light quantum" (Hesseldahl).

This is a new area of research that has the potential of guaranteeing absolute security in the future. It is based on quantum mechanics to secure communications because any attempt of Eve to read the quantum information will destroy it.

When a photon travels through space, it vibrates, and the angle of vibration is called the polarization of the photon. A Polaroid filter can pass the photons with

the same direction as the filter and reject the ones perpendicular to it. Half of the diagonally polarized photons will pass through the filter, but these are reoriented to the direction of the filter.

Quantum Key Distribution (QKD): If Alice wants to send an encrypted message to Bob, then she can use the polarizations of photons. If Eve, the eavesdropper, wants to intercept this message, then she needs to identify the polarizations of each photon. She must choose the correct orientation of the Polaroid filter; otherwise she will probably get the wrong results. However, Bob is in the same position as Eve. He will guess the right polarizations only half of the time. In order for Bob to use the same Polaroid orientations as Alice, she has to get the list of polarizations securely to him, which leads to the "key distribution problem" (Gottesman).

Advantages of a Quantum System: Over an insecure channel (i.e. telephone line) Bob can tell Alice which scheme he used for each photon. Alice would tell Bob whether his choice was correct without actually revealing the direction of the original value (0 or 1). Alice and Bob can detect Eve's presence because Eve introduces errors to the transmission when measuring it with the wrong schemes. Therefore, Alice and Bob can discard those photons that have been corrupted.

Quantum computers are not yet a reality. However, they have the potential of solving certain types of problems much faster and more efficiently than a classical computer. In a classical computer, the data is measured in bits (0 and 1). In a quantum computer, it is measured in qubits ($|0\rangle$ and $|1\rangle$). Quantum computers could perform factorizations in real time, which will make RSA and other cryptographic methods useless (Hesseldahl).

Conclusion

The evolution of cryptology explores past, present, and future methods of encrypting and decrypting messages that prevent unauthorized individuals from taking advantage of such information. The battle between code makers and code breakers, along with advancing technological innovations, have forced the continuous development of cryptology. Quantum Cryptography is the most promising method to securely transmit data through computer networks. Quantum Computers will break any existing method like RSA and DES.

References

Bosworth, Bruce. *Codes, Ciphers, and Computers: An Introduction to Information Security*. Rochelle Park, NJ: Hayden, 1982.

Frequently Asked Questions. Mar 2007 <http://www.tech-faq.com/cryptology.shtml>.
Gottesman, Daniel, and Hoi-Kwong Lo. *Form Quantum Cheating to Quantum Security*. Mar 2007 <http://www.physicstoday.org/pt/vol-53/iss-11/p22.html>.
Hesseldahl, Arik. *Special Report: A Quantum Leap in Data Encryption*. Nov. 6, 2006 < http://www.magiqtech.com>.
Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor, 2000.
Washington, Lawrence C., and Wade Trappe. *Introduction to Cryptography with Coding Theory*. Upper Saddle River, NJ: Prentice Hall, 2002.

Nominating faculty: Professor Aparicio Carranza, Computer Engineering Technology 4982, Department of Computer Engineering Technology, School of Technology and Design, New York City College of Technology, CUNY.

Cite as: Barreto, J.N. (2008). Advances in cryptology: An introduction to quantum cryptography. *City Tech Writer, 3,* 16-21. Online at https://openlab.citytech.cuny.edu/city-tech-writer-sampler/