The Evolution of Cryptography and Its Foundations in Discrete Mathematics

Nearly, 12.35 billion terabytes of data are securely transferred between users daily. Only through the works of cryptography are we able to achieve this level of safety from different hackers and cybercriminals. Cryptography in modern times is defined as, “the study or process of using algorithms to scramble or hide data, validate messages and digital signatures, etc., in order to secure the digital information against unauthorized access or corruption”. We use many different algorithms and equations to hide and encrypt our data, many of which come from the topics of discrete mathematics. Discrete mathematics is defined as “the study of mathematical structures that can be considered discrete rather than continuous". Topics studied in discrete mathematics include a variety of topics including number theory, logical statements, and graphs. These different topics apply to the various ways to encrypt, decrypt, or even study the logical capacity to fight against brute force algorithms. Thus, discrete mathematics has many applications to cryptography, from the early ages of the Roman Empire, all the way to the future of quantum computing.

Encrypting messages can be seen dating back to ancient Mesopotamia around 1500 BCE. It is there that the first formal use of using substitution cipher was recorded. The people wanted to keep a recipe for a pottery glaze a secret from their competitors, so they decided to substitute certain characters of their language for new symbols that would equate to the same character when decrypting. It was a simple yet effective cipher because the only way to decrypt the message at the time was to have the key to show which symbols represented which characters. Following them, around 500 BCE, the

Spartans implemented the Scytale. This device involved writing the message on a piece of leather that was wrapped around a rod of a certain diameter. When unraveled, the message appeared to be scrambled because lining up the letters with each other would be guessing. To decrypt the message, the user would need a rod of the same diameter otherwise the message would still be scrambled. This proved to be an effective use of military communications for the Spartans because it allowed them to quickly transpose messages in the field of battle. They didn't rely on calculations and resubstituting characters back in place creating a fast decryption. Then in the ancient Roman Empire, Julius Caesar used a substitution cipher that shifted all the letters in the alphabet by a certain number to the left or right. This created even more encrypted messages because he was changing every letter in the message. This allowed the Romans to pass military orders throughout their empire without messages ever being able to fall into their enemies' hands. However, the Caesar cipher was found to have a major flaw discovered during the Islamic Golden Age. An Arab scholar named Al-Kindi noticed that in any given language, certain letters and combinations of letters appeared more frequently than others. So, by looking at the frequency of symbols and other letters in a substitution cipher, it became possible to reason that the same frequencies in the substitution pattern would equate to that of the language it came from. This would become the first major scientific cryptanalysis. It laid the groundwork for foundational encryption analysis.

At the root of modern cryptography, many different mathematical concepts are used to encrypt messages and secure our data. Number theory is the basis of many modern algorithms involving the use of prime numbers and modular arithmetic. Prime numbers become valuable in many encryption patterns such as RSA. This algorithm involves the multiplication of two large prime numbers causing it to become very hard to factor the number into its prime divisors. This allows for a security level that increases with the size of the prime numbers that you use. When you apply the uses of modular arithmetic, the security of these algorithms increases even more. The main use case is in modular exponentiation. This is very efficient for computers to computer given a private key, but it becomes almost impossible to reverse without the same key. In secure programs, before modular exponentiation is applied, many numbers can be at least 1024 bits long. The next concept is combinatorics. It is used to study the complexity and security of certain systems. Different systems have different key generation patterns. By being able to count the different number of permutations or combinations, it can be ensured that there is a large enough pool of keys to be able to deter brute force attacks from the system. When the total number of different keys is too low, it becomes susceptible to brute force attacks that try every single key until the correct one works. Boolean algebra and logic statements are other key contributors to cryptography. Logic gates such as AND, OR, XOR, and NOT become frequently used because of their ease of working with and reversibility. When combining hundreds of these logic gates, it creates more confusion between the plaintext and ciphertext.

In the modern era, there are many different algorithms used to encrypt and decrypt functions securely. One major concept used today is the idea of public-key cryptography, which involves the receiver generating two different keys. In the RSA algorithm, one key is a public key that is sent to the sender that tells them how to encrypt the data. The other key is a privately generated key that is used to decode the public key. This algorithm works because the encryption technique used in the public key must be irreversible without the private key. This allows the sender to privately send the data without ever needing to decode the file itself. In the Diffie-Hellman Key Exchange, a property of modular arithmetic is used to securely exchange private keys without ever sending the actual key over the Internet. The security of this public-key encryption is based on the difficulty of solving a discrete logarithmic problem. If given a public value of (ga mod p), it is computationally difficult to derive a without already knowing the values of g and p. This principle is what allows the Diffie-Hellman key exchange to be used for a secure data transfer. Hash functions are another major use in cryptography today. Hash functions are mathematical algorithms used to produce a hash value of whatever string of characters you input. They are used to store and verify different values. Because a hash function produces the same value every time the same sequence of characters is input, it can be used to determine if data has been tampered with or changed. If changed, it will produce a different hash value if the size of outputs is large enough to hold the number of different inputs. In sending digital signatures, a hash value is applied to the string before being sent using the recipient's private key. They then will decrypt the hash message and apply the same message to compare hash values to ensure that data is not tampered with between users.

Discrete mathematics is used in many modern-day cryptanalysis techniques. Complexity theory is the study of how computational problems relate to security. For many encryption algorithms, it relies on the assumption that solving these problems is computationally impossible in a certain amount of time. These types of problems are referred to as NP (Nondeterministic Polynomial Time) because they can be verified in polynomial time but cannot be solved in polynomial time. These problems are considered to be NP currently because there has not been an efficient way to solve them yet. Examples of algorithms using these assumptions are: RSA assumes that factoring large integers is computationally hard and Diffie-Hellman assumes that solving the discrete logarithm problem is hard. Discrete mathematics is also used in assessing the probability and randomness of success of brute force attacks. Many times there are biases in pseudo-random number generators. By locating these biases with graphs and other tools, encryption becomes more secure because of the removed biases. Graphs are also a great tool used to study and determine the quality of different cryptographic algorithms. Even today, elliptic graphs are used to secure our data. We can securely pass keys between two computers by creating massive graphs that make it difficult to find a pathway from one point to another. Overall, discrete mathematics has many uses in modern cryptography and will continue to have value for different algorithms.

Even with modern uses, cryptography continues to grow and adapt to the different attacks that are used to try and break encryptions. A branch that is beginning to grow in development is quantum cryptography. Unlike modern cryptography, which uses mathematical formulas to secure data, quantum cryptography uses the properties of quantum mechanics to provide nearly unbreakable encryption. In using quantum key distribution, two people would be able to securely pass keys to one another by passing keys encoded in quantum states. If an attacker were to try and intercept the keys, the quantum state of the keys would be disturbed. This allows the people exchanging information to be alerted of the attacker. This would provide virtually secure key exchange based on the laws of physics instead of difficult math problems. However, many challenges are still faced in this field, such as distance and cost. Currently, these machines are limited by the fact that they either need optic cables or open space to communicate with one another. These machines are also too expensive to massively produce in the current day. It is not a point where it is practical to use them over current cryptographic systems. Whenever these quantum computers stack up against classic algorithms used today, they become outdated. Using the power of quantum computing, algorithms like RSA, ECC, and DSA, which are all currently viewed as NP problems, become solvable in polynomial time. This removes the inherent assumption that the mathematical problems are hard to solve which marks these as outdated algorithms. Even though outdated algorithms would be moved on from, discrete mathematics will continue to evolve based on whatever type of cryptographic methods are being used. It plays a role in the designing of quantum algorithms such as lattice-based cryptography, error-correction techniques, and security proofs. Additionally, discrete mathematics will continue to be used in analyzing and improving algorithms. Even today it is used to study the weaknesses of algorithms and that will continue to stay that way throughout the future.

Cryptography has developed from simple substitution ciphers to the key ciphers that we use today. It will continue to evolve into the quantum age to defend against the growing number of cyber-attacks that are used. Even as it grows, discrete mathematics will always have its role in evaluating the effectiveness of ciphers and their strength against attacks. Even though the future of cryptography doesn’t involve heavy mathematical formulas, that doesn’t mean that it leaves discrete mathematics behind. It will continue to evolve and grow alongside the subject.

Sources cited:

Definitions:

https://www.dictionary.com/browse/cryptography

https://en.wikipedia.org/wiki/Discrete_mathematics

History of Cryptography:

https://antigonejournal.com/2021/06/deciphering-spartan-scytale/

https://muslimheritage.com/al-kindi-cryptography/

Application of Discrete Mathematics:

https://www.thepharmajournal.com/archives/2019/vol8issue2/PartN/13-2-160-245.pdf

Quantum Cryptography:

https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2024.1456491/full