Cryptography

The Past, Present, and Future of Encryption

Jake O'Connor

UAT MS507

Final

Introduction

Humankind has always had the need to protect data of all sorts from adversaries. From the location of the most abundant gathering spots in pre-history, to the troop movements of antiquity, to the bank details of modern day, humans have and always will have a need to secure their data. Cryptography is the process by which messages and data are secured against the prying eyes of adversaries, and as long as written language has existed there has likely been some form of cryptography applied to sensitive data. Throughout this document we'll discuss the basic principles of cryptography as well as specific examples throughout the ages, from antiquity through today.

Definition of Terms

While this document is intended for those unfamiliar with cryptography and cryptology, and will be worded as such, there are some integral terms which are necessary for the clear communication of ideas. These terms are defined below and should be the only cryptography terms within the text that are assumed to be known.

Plaintext & Ciphertext

Plaintext and ciphertext are the two opposite sides of the coin that is cryptography. Plaintext is any data, message, or content which has not been obscured cryptographically and is usable in its current form. Ciphertext is any data, message, or content which has been obscured cryptographically, and is generally unusable. Cryptographic processes are meant to convert plaintext into ciphertext and then later convert that ciphertext back into identical plaintext.

Encryption & Decryption

Encryption and decryption are the cryptographic processes by which plaintext and ciphertext are converted. When plaintext is converted to ciphertext it is being encrypted. When ciphertext is being converted back to plaintext it is being decrypted. There are countless algorithms and processes for encryption and decryption, each with their own flaws, but all can convert plaintext to ciphertext and then back to identical plaintext.

Key(s)

Cryptographic keys, much like physical keys, are what protects encrypted ciphertext from being decrypted back into plaintext. Generally, the more complex the cryptographic key the more likely that encrypted data will be secure from outsiders. Key complexity is tied to the complexity and security of the encryption technique, with simpler techniques using only single small numbers and more complex techniques involving multiple, complex keys or mathematical equations.

Past

Since the dawn of written language, humans have found the need to obscure their information. From tradesmen's desire to protect their processes from competitors to keeping urgent military orders out of the hands of adversaries, people have been encrypting their data for thousands of years. Below are three historical instances of cryptography from three distinct periods in human history, how they were used, and how, like all forms of encryption someday will be, they were broken.

Scytale – 7th Century BC

One form of historic encryption believed to have been used in ancient Rome is known as a Scytale cipher, which was a form of transposition cipher that used a pair of identical batons or cylinders (called Scytalae) in order to quickly encrypt and decrypt messages. According to ancient Roman philosopher and historian Plutarch, in his biography of Spartan admiral Lysander written around the 2nd century AD, when military commanders were dispatched to war they were provided with one of these two identical Scytalae with which to encrypt and decrypt messages (Perrin & Plutarch). Direct and specific records of the Scytale cipher are sparse, but indirect records mention Scytale being used as early as the 7th century BC.

The premise of the Scytale cipher is incredibly simple. Given a rod of a defined diameter, a piece of hide or parchment is wrapped tightly around the rod leaving no space. Onto the wrapped rod, plaintext messages are written. Then the hide or parchment is unwound from the Scytale, now containing the transposed ciphertext, and sent along with a messenger. At the other end, the recipient wraps the ciphertext around their identical Scytale and can then read the plaintext. The key to encrypting and decrypting the Scytale cipher is the diameter of the Scytale itself.

As you can probably imagine, this was not an incredibly secure form of encrypting messages. In order to break a Scytale cipher in transit it would only take a simple process of wrapping the ciphertext around various differently sized objects until a message could be understood. There are various theories about the Scytale cipher and if it was ever truly used as a form of encryption, due to its extreme weakness. One theory posits that the Scytale cipher was actually used as a form of authentication instead of encryption, where a message would only be believed to be from the stated sender if the plaintext perfectly lined up when wrapped around the Scytale.

Caeser Cipher – 1st Century BC

This form of historic encryption is likely the most well-known of all. In the first century BC this cipher was used by Julious Caesar to communicate with his troops in the many battlefields of ancient Rome. The Caesar cipher is a simple substitution cipher which could quickly encrypt and protect messages to and from Caesar's generals.

The premise of the Caesar cipher is the same as with any substitution cipher, each character of one alphabet is replaced with a corresponding character from another alphabet. In the case of the Caesar cipher, which is within a subset of substitution ciphers called shift ciphers, the secondary alphabet used is always the same alphabet as the first but shifted three characters to the right. In modern English, a Caesar cipher would replace ‘A’ with ‘D’, ‘B’ with ‘E’, and so on. To decrypt ciphertext encrypted with a Caeser cipher, one must perform the same operation in reverse, replacing each encrypted character with its corresponding character three to the left.

The Caeser cipher, like most substitution ciphers, is incredibly simple to decrypt without knowing the shift key if given enough time. To decrypt an intercepted ciphertext from the Roman army, one would just need to at most test each possible shift value against the text, until a clear message was revealed. Luckily for the Roman army, most of their enemies could not read Latin. The Caeser cipher is neither the first nor last use of a shift cipher or substitution cipher throughout history, and the basic process of shifting plaintext by some key value forms the foundation of many more secure cryptographic methods.

Vigenère Cipher – 1500's

As the globe became more interconnected and travel between countries became more commonplace, new and more secure encryption methods were required. The Vigenère Cipher was one such method. This cryptographic method is named after Blaise de Vigenère, but was invented by Giovan Battista Bellaso, and is heavily inspired by the polyalphabetic substitution cipher of Leon Battista Alberti (Simmons). The Vigenère cipher is based upon the idea of using multiple substitution ciphers in concert, with each character in the plaintext using their own corresponding substitution key in order to encrypt it.

In order to make use of the Vigenère cipher, you must establish a key. This key corresponds to a row or column within a Vigenère table, which contains a row and column for each letter in the alphabet. The content of each row of the Vigenère table is the alphabet, but shifted based on the index of the letter (e.g. row 1 is A-Z, row 2 is B-Z, A, row 3 is C-Z, A, B). Once you have established a key string to use, and have access to a Vigenère table, the process of encryption is simple. To encrypt a message, one simply takes the first character of the message and finds the table's cell which corresponds to that column and the first letter of the encryption key's row. This process is repeated until each character of plaintext has been encrypted into ciphertext. In order to decrypt the ciphertext, the process is simply reversed, using the encrypted character and the corresponding character from the encryption key to locate the table's cell.

This type of cipher was used heavily all the way until the early 1900's, even though it had been effectively broken many decades earlier. One of the last notable uses of the Vigenère cipher, even after it had been successfully broken by Babbage in 1854, was during the American Civil War by Confederate soldiers and secret service. The primary weakness of the Vigenère cipher comes from its key length. If a short key is repeated multiple times in order to fit the cipher table, then patterns will emerge that can be identified.

Present

There are dozens of secure cryptographic methods in use today, all of which require the power of modern computers in order to operate. Most people interact tangentially with cryptography dozens of times a day, be it from browsing the web, accessing a bank account, or using a virtual private network. Below are two of the most commonly used and most secure cryptographic algorithms today.

Rivest-Shamir-Adleman (RSA)

In the late 1900's, as advancements in technology were further accelerating and the digital age was beginning to take off, three students at MIT developed the Rivest-Shamir-Adleman cryptographic method. This new method of encryption and decryption used a novel type of cryptographic keys, now commonly referred to as public-key cryptography, in which a user would have two distinct keys, a private key known only to them, and a public key freely shared with others (Sears, 2020). By combining the use of these two keys, in addition to the complexity of reverse-engineering the keys, communication between two specific parties can be securely encrypted.

RSA encryption is extremely widely used today, as it is still one of the most effective forms of encryption, but it does have some significant drawbacks. Compared to other, more modern algorithms, RSA encryption is much slower, and not suitable for real-time data encryption. The more important flaw with RSA, as we look toward the future, is the relative simplicity of the algorithm itself. RSA's security is based on the difficulty of factoring prime numbers, a significant problem for both humans and machines alike, but as technology advances and we enter the age of quantum computing and supercomputers it is very likely that factoring large prime numbers becomes child's play compared to what it is now.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard is a data encryption standard based on the Rijndael block cipher initially created by Vincent Rijmen and Joan Daemen. This form of cryptographic method uses the standard symmetric, shared key approach to encryption. The AES algorithm was designed for the modern computer age, and the application of the complex algorithm is all but impossible to do by hand. Plaintext messages are first divided into uniform blocks, which then go through a repeated mathematical process of addition, matrix multiplication, and row shifting (Rimkienė, 2020). The resulting ciphertext of AES encryption is both extremely obscured, and quickly calculated, making it a great encryption standard for real-time data transfer.

Though it is extremely secure and has not been effectively broken yet, AES encryption is not without flaws. Being a symmetric key cryptographic method, the security of the single encryption key must be managed externally to the algorithm itself, which means that keys themselves are often transferred securely using some other form of encryption, such as RSA, to guarantee the key's security in transit. While a brute-force attack on the AES encryption standard would be fruitless using modern hardware, the potential of quantum computing and vast distributed supercomputers does pose a potential future risk.

Future

The future of cryptography offers a wide spectrum of paths down which encryption may go. With new and more powerful computers of differing types being created each year, and more and more businesses operating on the cloud each day, ensuring that data can be cryptographically secured and protected against third party intrusions will be as important as ever. There are hundreds of organizations working on thousands of future solutions to rising cryptography problems, but here are two topics which look to be incredibly important within the next decade of cryptography.

Quantum Computing

One of the major topics when considering where the future of cryptography will go is the topic of quantum computing. In extremely simple terms, quantum computers are those built on a foundation of qubits instead of bits. While traditional computers use bits, which have a binary on/off state, quantum computers make use of qubits, which have both a physical on/off state and make use of quantum mechanics to allow for a superposition of on and off at the same time.

Quantum computing is still in its infancy, but quantum algorithms have the very real potential to crack current encryption techniques in an incredibly short time. As far back as the 1990’s, quantum algorithms have been mathematically proven to be able to factor large integers in significantly less time. This is a death knell for encryption techniques such as RSA which relies on the inherent difficulty of factoring large prime numbers, as once quantum computers can run these algorithms that will no longer be a barrier to brute-force attacks (Lauter, 2018).

Homomorphic Encryption

Another topic in the future of cryptography is called homomorphic encryption, which in essence is an encryption technique that preserves the meaningful structure of the data while obscuring the actual content. In traditional encryption, performing mathematical or logical operations on encrypted data will result in unrecoverable damage to the data. In homomorphic encryption, since the structure of the data is preserved, mathematical and logical operations can be performed on the encrypted data and the effect of those operations will be meaningfully preserved, all without ever having to decrypt the data (*IBM Explores the Future of Cryptography*).

This is a big move, as it allows for customers and clients to entrust their data to third parties such as the cloud without ever having to reveal what the actual data is. For example, a hospital could upload fully encrypted healthcare data to the cloud to be analyzed and operated upon without the plaintext of that data ever being present on the cloud. Then once the operations are complete, the hospital could download the data from the cloud and decrypt it locally to reveal the resulting plaintext including the modifications. Homomorphic encryption techniques look to potentially have the high security of symmetric key algorithms such as AES but without the inherent risk of having to share the key between parties.

Conclusion

We've seen that cryptography has been used for thousands of years to protect the data of individuals and that leaps in cryptographic security often correspond to wars between countries and civilizations. In the modern era, there is an exponentially increasing amount of data being stored and transferred, and an exponentially increasing number of adversaries who want to intercept and steal that data. Every form of encryption is eventually broken, and that will eventually hold true for our modern cryptographic methods as well. As computers advance and the amount of data being transmitted and stored grows increasingly larger, encryption techniques and those who wish to crack them will grow to match the new demand.

References

CNG. (2019, September 18). *History of Cryptography: The Vigenère Cipher*. Cangea. https://cangea.com/history-of-cryptography-the-vigenere-cipher/.

Crawford, D. (2019, February 4). *AES Encryption: Everything you need to know about AES*. ProPrivacy.com. https://proprivacy.com/guides/aes-encryption.

Djekic, M. (2014, June 12). *A Scytale – Cryptography of the Ancient Sparta*. Australian Science. http://ozscience.com/technology/a-scytale-cryptography-of-the-ancient-sparta/.

IBM Explores the Future of Cryptography. IBM News Room. (n.d.). https://newsroom.ibm.com/IBM-Explores-the-Future-of-Cryptography.

Lauter, K. (2018, September 14). *The Future of Cryptography*. Queen Elizabeth Prize for Engineering. https://qeprize.org/news/the-future-of-cryptography/#:~:text=%20The%20Future%20of%20Cryptography%20%201%20An,the%20lattice-based%20cryptosystems%20mentioned%20earlier%20is...%20More%20.

Leonard Adleman Made RSA Encryption History With His Invention. Made RSA Encryption History With His Invention. (n.d.). https://www.invent.org/inductees/leonard-adleman.

Plutarch. (n.d.). *Plutarch, Lysander*. Plutarch, Lysander, chapter 19, section 5. http://www.perseus.tufts.edu/hopper/text?doc=Plut.%2BLys.%2B19.5&fromdoc=Perseus%3Atext%3A2008.01.0048.

Reynard, R. (1996, August 1). *Caesar Cipher History*. Secret Code Breaker. http://www.secretcodebreaker.com/history2.html.

Rhodes, B. (2020, April 23). *Roman Cybersecurity: The Scytale*. Medium. https://medium.com/tech-is-a-tool/the-birth-of-security-the-scytale-94d472aa480d.

Rimkienė, R. (2020, December 11). *What is AES Encryption and How Does It Work?* CyberNews. https://cybernews.com/resources/what-is-aes-encryption/.

Sears, J. (2020, January 9). *A fascinating story of RSA encryption*. NordLocker. https://nordlocker.com/blog/rsa-encryption/.

Simmons, G. J. (n.d.). *Vigenère cipher*. Encyclopædia Britannica. https://www.britannica.com/topic/Vigenere-cipher.

The Story of Cryptography: History. The Story of Cryptography : Historical Cryptography. (n.d.). https://ghostvolt.com/articles/cryptography_history.html.

Vigenère Cipher. Vigenre Cipher. (n.d.). https://www.cryptomuseum.com/crypto/vigenere/.