The History of Cryptography - From Hieroglyphics to Federated Aggregations

Sundar, Ramamurthy
University of the Cumberlands
ISOL 535 Section B01 - Cryptography
Dr. Chanel Suggs
July 23, 2023

The History of Cryptography - From Hieroglyphics to Federated Aggregations

Information has always been important throughout history - from the individual to the societal level. It's just that with computers and the internet, it has become far easier to receive, transmit, and store data at scale as well as democratize access to said data. Through the warehousing of data in massive data centers, the 21st century has become known as the information age, where details regarding the state of business in the form of raw transaction data is used for policy and decision making at a global scale. Even before the internet, messages and data were needed for the functioning of a state or business, but the ability to collect/transmit data at such scale as in the 21st century has never been seen before. Despite this scale and realization that warehousing data can be used to generate value and cut costs, the study of cryptography has always been an important one. From the use of hieroglyphics, to the initial cracking of the Enigma Code, the creation of the Internet, and the prominence of blockchain, cryptography and encryption algorithms have always been important and have come a long way. The need to keep some information private through various transformations is a fairly old concept, but the process(es) through which information privacy can be achieved is a difficult subject to explore. There are many ways to make a message/data difficult to interpret, but the computer has given us may new tools that can change what cryptography is capable of. It is not necessarily true that one would want to make a message only readable between two parties bilaterally for it to be secure. Making the trends of a transaction system visible while making the private data unviewable is something that would only be possible with computers. This paper briefly touches on the history of cryptography and asks 7 challenging questions about cryptography.

A Brief History of Cryptography - From Hieroglyphics to Federated Aggregations:

Despite not even being the first ancient language to be understood, the deciphering of the Egyptian language and hieroglyphics turned out to be a centuries long process (Chadwick, 1999). Since both the language and the script of the ancient language were unknown to explorers who found the ancient remains, it took the collaboration of experts from around the world in order to make sense of the letterings. The understanding of the Egyptian hieroglyphic, as Chadwick puts it, lead to the strengthening of the field of study known as philology. Fundamentally, hieroglyphics and other languages make use of substitution ciphers which make it so that people who do no understand the langue will have great trouble understanding what is going on. Being able to relate such a foreign script with known languages like English can be known as an early form of code-breaking!

While simple hieroglyphics could be seen as a proper way of encoding information, the field of cryptography has progressed a lot since the times of ancient empires. There have been stronger and more powerful protocols like symmetric and asymmetric cryptography schemes as computers and the internet came about, but blockchain technology has pushed the envelope even further. Zhu et al. (2021) describe an encryption scheme that allows one to keep private data secure, while allowing a secure peer-to-peer server to observe and record trends occurring within the private data. This form of encryption is known as federated learning/aggregation and can really gain benefits when compared to the client-server models. Security features such as

disintermediation, transparency, and democratization are features the client-server model did not provide, but the peer-to-peer model can.

The internet makes use of the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) as of now (Stallings, 1999). These standards have been tested and are known to work well, but advancements in technology like blockchain technology and quantum computing could make these tried and tested standards obsolete eventually. Just as hieroglyphics or the Cesar Cipher were no longer viable solutions for secure encryption, the DES and AES standards could also require replacing.

7 Questions About Cryptography:

An 800 page paper isn't really enough to explore the full history of cryptography. It has a history going back to the times before christ and is still in the process of changing as time moves on. Below are seven questions regarding the field of cryptography that are worth exploring:

1. Is there a right balance between security and speed?
2. Can there be such a thing as too much privacy/confidentiality in an IT system?
3. What are federated learning/aggregations and homomorphic encryption and how will these protocols change the field of cryptography?
4. What is cryptographic hashing and how does it differ from distributed cryptographic hashing?
5. What is the relationship between cryptography and technology?
6. How has the field of cryptography changed over the course of history?
7. What does the future of cryptography hold, particularly with the rise of quantum computing?

Question one attempts to point at that properties such as the block size might help make an algorithm more secure, but it makes it much slower from a user experience (UX) perspective. This means that the field of cryptography is as much about efficiency as it is security. Question 2 brings up the concept of complete confidentiality and the ring signature encryption algorithm. Alonso & Joancomarti (2017) describe everything we know about the Monero cryptocurrency and they point out the the ring signature encryption algorithm is perfectly fit for money laundering purposes. Is such levels of security a threat to national security or a god-given right? Questions 3 and 4 dig into the mechanics of federated aggregations, where these encryption protocols have the potential to disrupt the distributed computing environment. By making it so that everyone transacting in a digital economy does not even need a key in order to securely transact, it could make the application of cryptographic functions at the end-user level more widespread than we have seen in history. Finally, questions 5-7 try to bring in the concepts of history and technology within the cryptography context. The level of technology reflected the types of encryption/decryption algorithms used as the time, as simple hieroglyphics make use of almost no technology while quantum cryptography, federated aggregations, and basic symmetric/ asymmetric ciphers make use of varying levels of technology. It takes along time for cryptographic schemes to be considered secure, so it is unlikely that any federated aggregation or quantum cryptography methods will be green-lit soon, but the future seems exciting nonetheless.

Conclusion:

Privacy and encryption has become a fundamental human right now that information is the new currency. At one point in time, only messages that served some special purpose like religious, militaristic, or strategic would be encrypted due to the costs involved. Technology has now made it so that any message I want to send can be easily and rather securely encrypted. It is not a question then, of what I aught to encrypt, but rather how (securely) one encrypts plaintext. Limniotis (2021) describes the fundamental need for cryptography to preserver human rights. Economies and societies simply function better when there is more data to be used in decision making. Encryption schemes like homomorphic encryption, server models like blockchain, and technology like quantum computing all have an impact on security and cryptography. As long as the private data is not easily reverse engineered, data is democratized, and proper incentive mechanisms are in place to reward the sharing of data, it makes sense to share as much of ones data as is possible. For the vision of a smart city, for example, it is the secure crunching of private data that could lead to a better future.

References

Alonso, K. M., Joancomarti, J. H. (2017). Monero - Privacy in the blockchain. *IACR Cryptology EPrint Archive*, *2018*, 535. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/75205/6/alonsokTFM0118memoria.pdf

Chadwick, R. (1999). The story of decipherment from Egyptian hieroglyphs to Maya script . Maurice Pope. Near Eastern Archaeology, 62(4), 255–256. https://doi.org/10.2307/3210738

Limniotis, L. (2021). Cryptography as the Means to Protect Fundamental Human Rights. Cryptography, 5(4), 34–. https://doi.org/10.3390/cryptography5040034

Stallings, W. (1999). Information and Network Security Concepts. In *Cryptography and network security: Principles and practice* (pp. 112–131). essay, Prentice Hall International.

Zhu, S., Li, R., Cai, Z., Kim, D., Seo, D., & Li, W. (2022). Secure verifiable aggregation for blockchain-based federated averaging. High-Confidence Computing, 2(1), 100046–. https://doi.org/10.1016/j.hcc.2021.100046