**Cryptography in Digital Forensics**

Corbin Osman

American Public University System

ISSC266 – Cryptography Concepts

Joel Stewart

11/26/2023

**Introduction**

The field of technology continues to grow daily in many ways, and more of the world is beginning to implement technology in every walk of life. As the use of technology increases, more confidential and sensitive personal information is stored, transmitted, and shared across networks and the internet. With such crucial information traversing the digital world, it is important to find ways to protect data from individuals and parties who seek to capture and misuse it. Criminal activity occurs in both the physical and digital worlds, and the practice of forensics helps to collect and analyze evidence from crimes that have been committed.

One field within the practice of digital forensics that deals with the security of digital data and information is cryptography. This paper will explore the practice of cryptography and how it is used in digital forensics to both protect sensitive information and decipher potential evidence that has been encrypted. The purpose of the paper is to help readers understand the field of cryptography, learn how it works and is performed, and recognize its purpose in forensic investigations. Understanding cryptography and how data and information can be encrypted will allow forensic investigators to recognize encrypted data, know what methods of encryption may have been used to encrypt it, recover original data as evidence, and be able to make conclusions on what the digital evidence shows.

**Definition of Digital Forensics**

To understand how cryptography relates to the practice of digital forensics, it is first vital to understand what digital forensics is. Digital forensics, as shared by the National Institute of Justice, is “the collection and analysis of digital evidence” (National Institute of Justice). This practice, also referred to as computer forensics, typically involves searching for evidence at a crime scene or on a device, properly collecting the evidence, and transporting it to a forensic laboratory or similarly secured location. Once there, forensic investigators and analysts can examine the evidence, perform tests as needed, determine conclusions regarding the evidence and its contents, and report on the findings of the investigation.

Digital forensics plays a vital role in the field of criminal justice. When investigations are performed, forensic investigators and analysts can search for evidence that will aid in determining who may have been involved with a crime that has been committed. Many of the digital interactions of individuals are recorded in some way, whether on a local machine, network, server, or the internet, and forensic investigators can use practices and tools to locate the evidence that is left behind by their actions. Once collected, investigators can begin examining and analyzing the evidence for information that will help solve crimes. This evidence can be prepared and presented in a court case to help prosecute potential suspects. Following a simple investigation process with steps such as collection, examination, analysis, and reporting will aid forensic investigators in performing their searches and examinations properly and efficiently.

**Introduction to Cryptography**

With a basic understanding of digital forensics and their role in the field of criminology, let us now explore the practice of cryptography. Returning to the topic of digital forensics, we understand that forensic investigators will search for digital evidence such as digital documents, photos, text and email communications, and raw binary data. In its original format, also known as plaintext, this data may be easy for investigators to locate. If the data is instead hidden or encrypted in some form, the process of locating and interpreting the data may be much more difficult.

This is the practice of cryptography. Cryptography simply defined is the practice of securing data and information by transforming it into a format that can only be understood by its intended recipients (Fruhlinger, 2022). This is performed by taking data or information that is in plaintext, or its original form, and making changes to it so that the plaintext data cannot be easily understood. This format is commonly known as ciphertext. The changes made to the data occur with the use of an algorithm, which is essentially one or more mathematical equations that change the values of the data being encrypted. Once data has been encrypted through the use of cryptography, it can be shared with others intended to receive the data. Those individuals or parties can then work to decrypt the ciphertext back to its original plaintext form to understand its message and contents.

In times past cryptography was performed manually using a cipher or algorithm, known as a key. This key is crucial as it is the cryptographic component that allows both the sender and receiver of cryptographic data to understand the encrypted data. The party sending the data will follow the key to encrypt the data, and the receiving party will use the key to decrypt the data. Without the key, it is nearly impossible for a human being to manually decipher encrypted data. In modern times with the advancements of technology, computers can encrypt and decrypt data much faster than a human being. With enough time and computing power, computers can decipher encrypted data even without the necessary key for its decryption.

**Cryptography in Digital Forensics**

The utilization of computers is a strong tool for forensic investigators who are attempting to decipher encrypted data. If forensic investigators and analysts find encrypted data that could contain criminal evidence and attempt to decipher it manually, it could take them months and even years to have even only a small chance of deciphering the data. By using computers to decipher the data, they can save time and resources for other tasks in an investigation.

Let us explore a few areas within cryptography that are important for forensic investigators and analysts to understand.

**Recognizing Encrypted Data**

For investigators to begin the decryption process, they must first find and capture encrypted data. Investigators should learn what encrypted data looks like so that they recognize it when searching a crime scene or captured devices. Encrypted data can be as short as a few characters or lines in length, but it may also be much longer. An example of the ciphertext version of a simple sentence is shown in the following image, along with the key that was used.

A close-up of text

Description automatically generated

The ciphertext as shown appears to be unreadable in its current form, but it can be easily recognized as encrypted data. Ciphertext can contain a combination of letters, numbers, and even special characters if desired, and investigators should learn to recognize ciphertext as they search for evidence. When encrypted data is found, investigators can capture it and later work on decrypting the data to reveal its plaintext contents.

Encrypted data can be found practically everywhere in the digital world. A few common locations are in email communications, text documents, file directories, and audio and video files. Ciphertext is not limited to these locations, but they are areas investigators should explore when searching for encrypted data. The type of device on which encrypted data can be found extends to most digital devices, such as desktop computers, laptops, mobile devices, and more. If a device found at a crime scene is reasonably suspected to contain evidence, it can be seized to search it for encrypted data and ciphertext.

Along with recognizing encrypted data, it is also important for investigators to be able to recognize cryptographic keys. These keys may appear to look like encrypted data themselves and are often sequences of random bytes of data (Maartmann-Moe, 2009). Because it is good practice to not store a cryptographic key with the encrypted data, the keys will most likely be stored in a location other than that in which the ciphertext is found. Modern computers do have the strength to decipher encrypted data without the proper key, but if investigators can locate the key that was used, they may be able to save time in the decryption process.

**Common Types of Encryption Algorithms and Methods**

There are various types of encryption algorithms and methods that investigators should learn about and understand. Three types that will be explored here are symmetric, asymmetric, and hash algorithms.

Symmetric algorithms, or symmetric key cryptography, is the practice of using a single cryptographic key for both the encryption and decryption of data (Sangeeta & Er, 2017). The process generally goes as follows: The sending party will encrypt a plaintext message or data with a symmetric key, the ciphertext will be shared with the receiving party, and the receiving party will use the same symmetric key to decrypt the ciphertext. How the key is shared between the sending and receiving parties is up to those involved, but it will usually be shared through an avenue different from the one used to share the ciphertext. A few of the most common types of symmetric cryptographic algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES), and BLOWFISH.

Asymmetric key cryptography is different from its single-key symmetric counterpart in that it uses a pair of keys – a public key and a private key. The public key is available to anyone who wants to encrypt data, while the private key is only known by the recipient of the encrypted data (Rani & Kaur, 2017). This allows for encryption in an environment where anyone who needs to send encrypted data can convert it to ciphertext, but only those intended to receive and understand the ciphertext can do so because they hold the private key. Some common asymmetric algorithms are Rivest-Shamir-Adlemen (RSA), DIFFIE-HELLMAN, and Elliptic Curve Cryptography (ECC).

Hashing algorithms are different from traditional encryption algorithms. Instead of generating ciphertext through encryption that can later be decrypted, hashing algorithms generate and output a string of characters known as a hash value (Constantin, 2021). This hash value is used to confirm the integrity and validity of various sources. This is accomplished when a specific input results in the same hash value each time it is performed. By using the same input, the resulting hash will be the same each time it is entered. Individuals or parties looking to confirm that data or information has not been manipulated or changed can refer to a hash value which helps confirm that its integrity is intact.

Companies around the world are working on strengthening existing cryptographic methods and algorithms while also designing new ones for the future of information security. A few notable companies that are involved in the growth of cryptography are Qrypt, Post-Quantum, Quantum Xchange, and Crypto Quantique (Dargan, 2021). These and other companies are working on strengthening encryption algorithms that are already in use while focusing on the development of newer practices such as quantum cryptography, which will briefly be explored later in this paper.

**Process of Recovering Original Data and Evidence**

With a basic understanding of encryption and hashing algorithms, let us look at some methods forensic investigators and analysts use to recover evidence from encrypted data and ciphertext. First is an analysis method known as frequency analysis, which involves the knowledge that certain characters of an alphabet are more commonly found in literature and sentences than other letters (Poritz, 2023). For example, the letters A, E, O, and T are some of the most common letters in the English language and are more likely to appear than letters such as J, X, and Z. This knowledge can assist forensic investigators who are attempting to decrypt ciphertext that has been encoded using a substitution cipher. They can search ciphertext for the letter that appears the greatest number of times and reasonably suspect that the letter was used as a substitution for one of the common letters previously mentioned. Frequency analysis will usually be more effective when used with ciphertext of greater lengths, as there will be a greater collection of data.

Additional manual methods of decrypting data include searching for original plaintext data and searching for cryptographic keys. By scanning a device investigators may be able to locate ciphertext, original plaintext, or cryptographic keys that can be used to decipher encrypted data. Depending on the strength of the computer performing the scan or the size of the location being scanned, this process can take a lot of time. An alternative method is for investigators to manually search a device and its contents to search for the same data and information. Investigators can use their knowledge of devices and operating systems to make reasonable assumptions about where encrypted data or plaintext may have been stored, and they may be able to locate such data quickly and efficiently.

Moving on to computational methods, we have the brute force method. This practice involves attempting any possible cryptographic combinations in quick succession one after another in the hopes that the correct combination will be stumbled upon (Swinhoe, 2020). Brute force attacks are commonly used to crack passwords, but they are also used to crack encryption keys and similar encryption methods. Computers can crack less secure and shorter encryption keys and algorithms in a relatively short amount of time, but the larger the encrypted data or key the longer it would usually take to decipher encrypted data. If the data being encrypted is valuable enough, malicious individuals or parties may spend any length of time to try and brute force past encryption.

These are just a few of the many different methods investigators can use to decipher encrypted data. As computers continue to grow in computational power and newer decryption methods are created, the process of decrypting ciphertext may become easier for investigators and analysts. The goal is to have practices and methods in place that can outclass the encryption methods and algorithms that criminals use to encrypt data and evidence.

**Making Conclusions and Reporting Based Upon Evidence**

Because the field of criminology is highly sensitive and a lot of confidential information may be handled, it is critical that investigators and analysts properly report findings and conclusions that are determined. Evidence that is gathered should be thoroughly examined in order to make the most accurate deductions about it. If something about a piece of evidence is not fully understood, efforts should be made to better understand how the evidence came about and who was involved with it. Investigators and analysts have this important task during an investigation, and the results of their efforts could prove helpful in a court case.

The plaintext evidence should be accurately documented so that its integrity and authenticity are assured. Investigators should document the encrypted data throughout the various stages of the investigation, such as where it was found, how it was captured, what the original ciphertext data was, what methods were used to decrypt the data, and what the plaintext results were. Having a complete record of the evidence will help its admissibility in court, and investigators will have all of their interactions with the evidence documented for their protection as well.

**Regulatory Issues and Global Implications for Cryptography**

As with many fields in the world of information technology, cryptography is not without its issues and obstacles. Because cryptography is used around the world, it can be difficult to establish universal laws and regulations that are agreed upon by every country. Additionally, import and export controls make it difficult to use certain types of cryptography in different locations. Certain countries treat cryptographic practices, software, and hardware as weapons and secure their use by placing import and export controls over them (InformIT, 2004). The exact controls that are placed differ from country to country, so it is important for forensic investigators to learn about the controls and regulations that may be in place in their country of residence so that they can comply with the standards that have been set.

Another issue within the field is the patents that are placed on some of the mathematical equations used in encryption algorithms. Most cryptographic algorithms utilize one or more mathematical equations to encrypt the plaintext data, and while some of these algorithms are public knowledge and publicly available, others are patent protected by their creators (InformIT). With the content and equations being protected, companies seeking to use them must obtain permission or a license from the creators of the equations. Forensic investigators should ensure that they use algorithms that are not patented or obtain permission to use patented algorithms to avoid legal issues.

**Future Trends in Cryptography**

With technology rapidly advancing each day, the field of cryptography continues to grow as newer practices and algorithms are found and created. One area in which the field is changing is the introduction of quantum computing and quantum cryptographic algorithms. Quantum computing involves the use of quantum mechanics to solve problems much quicker than traditional computers and technology (Gamble, 2019). With the strength of quantum computers, encrypted data can be cracked much quicker, making traditional encryption algorithms and methods less secure.

Another way in which quantum is being used is in quantum cryptography. This is the practice of using photons and polarizers to send encrypted data that is interpreted by the receiver using beam splitters. When the receiving party receives the data, they relay back to the sender how they used the beam splitters to read the photons, and the sender can compare the results with the original data sent (Quantumxchange). This form of cryptography is secure because the photons involved will change should a third party interrupt or intercept the data communication. These changes in the photon’s state will be recognized by the sender, and they will know that the encrypted data is not safe.

**Conclusion**

As technology continues to grow and newer algorithms are created, forensic investigators must become familiar with new practices and advancements in the field of cryptography. To keep up to date with changes and perform to the best of their ability in the field, they must understand cryptography, know how to find encrypted data, and be able to decipher it. The practice of cryptography has many implications in the digital and criminal justice worlds, and with technology rapidly advancing criminals will most likely use it more in their activity. Forensic investigators and analysts must stay ahead of criminals in their knowledge and understanding of cryptography to be able to combat its criminal use. We may one day reach levels of security that are truly unbreakable, but until then it is up to those versed in cryptography and other security practices to protect against the attacks and threats of adversity.

Resources

Constantin, L. (2021, January 13). Hashing Explained: Why It’s Your Best Bet to Protect Stored Passwords. *CSOOnline*. https://www.csoonline.com/article/570229/hashing-explained-why-its-your-best-bet-to-protect-stored-passwords.html

Dargan, J. (2021, January 11). 25 Quantum Cryptography and Encryption Companies [2022]. *The Quantum Insider*. https://thequantuminsider.com/2021/01/11/25-companies-building-the-quantum-cryptography-communications-markets/

*Digital Evidence and Forensics | National Institute of Justice*. (n.d.). National Institute of Justice. https://nij.ojp.gov/digital-evidence-and-forensics

Fruhlinger, J. (2022, May 22). What is Cryptography? How Algorithms Keep Information Secret and Safe. *CSOOnline*. https://www.csoonline.com/article/569921/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html

Gamble, S. (2019, January 28). Quantum computing: what it is, why we want it, and how we’re trying to get it. Frontiers of Engineering - NCBI Bookshelf. https://www.ncbi.nlm.nih.gov/books/NBK538701/

*Legal Issues with Cryptography | Cryptography with Java | InformIT*. (2004, May 28). https://www.informit.com/articles/article.aspx?p=170967&seqNum=14

Maartmann-Moe, C., Thorkildsen, S. E., & íRnes, A. (2009). The persistence of memory: Forensic identification and extraction of cryptographic keys. *Digital Investigation*, *6*, S132–S140. https://doi.org/10.1016/j.diin.2009.06.002

Poritz, J. A. (2023, October 1). Yet Another Introductory Number Theory Textbook – Cryptology Emphasis. *LibreTexts*. https://math.libretexts.org/Bookshelves/Combinatorics\_and\_Discrete\_Mathematics/Yet\_Another\_Introductory\_Number\_Theory\_Textbook\_-\_Cryptology\_Emphasis\_(Poritz)/04%3A\_Cryptology/4.03%3A\_Frequency\_Analysis

Quantumxchange. (n.d.). Quantum Cryptography, Explained. Quantumxchange. https://quantumxc.com/blog/quantum-cryptography-explained/

Rani, S., & Kaur, H. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms. International Journal of Advanced Research in Computer Science, 8(4) http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Ftechnical-review-on-symmetric-asymmetric%2Fdocview%2F1912629254%2Fse-2%3Faccountid%3D8289

Sangeeta, S., & Er, A. K. (2017). A Review on Symmetric Key Cryptography Algorithms. International Journal of Advanced Research in Computer Science, 8(4) http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Freview-on-symmetric-key-cryptography-algorithms%2Fdocview%2F1912629193%2Fse-2%3Faccountid%3D8289

Swinhoe, D. (2020, June 23). Brute-Force Attacks Explained, and Why They are On the Rise. *CSOOnline*. https://www.csoonline.com/article/569513/brute-force-attacks-explained-and-why-they-are-on-the-rise.html