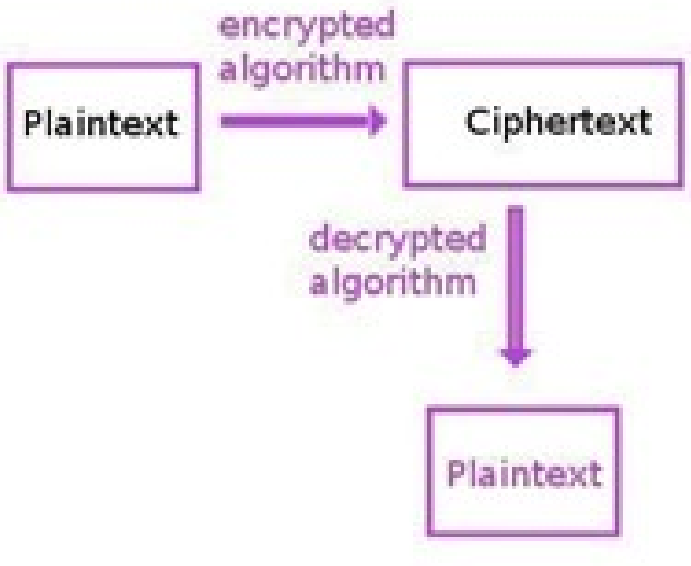
MORGAN CREEK
DIGITAL
ALTERNATIVE THINKING ABOUT INVESTMENTS

Welcome to Morgan Creek Digital's digital asset update. It is comprised of a thought piece from our team. We hope you find this content interesting. Please let us know if you have any comments or questions or if you would like to speak to a member of the Morgan Creek Digital team.

The Evolution of Cryptography: Understanding Modern Methods



Modern cryptography is the foundation of digital security and in fact, the term “crypto” referred to the study of securing digital communication long before cryptocurrencies became mainstream. (Before computers, cipher was used to scramble text often related to military communications, a measure that was taken by a particular faction to avoid interception by their opponent—dating back to the ancient Spartans in 650 B.C, but this is a topic for another day)[1]

As the world has become increasingly digitally dependent, simple cipher systems have given way to more complex cryptographic protocols to secure everything from individual privacy to national security. Simply put, the field of cryptography has the purpose of safeguarding information from unauthorized access or manipulation. This primary objective is achieved through a variety of functions. Foremost among them is the operation of ensuring sensitive data remains accessible only to authorized parties via encryption into an unreadable form, known as *ciphertext*, which can only be deciphered with the appropriate *decryption* key.[2] Another objective is to ascertain the *integrity* of data, and therefore various mechanisms are employed to detect alterations that may occur during decryption or transmission. Cryptographers also leverage authentication protocols to validate or *authenticate* the identities of communicating parties, ensuring secure exchanges, and bolstering trust.[3] It is worth noting that modern Web 3 cryptography seeks to replace the reliance on third parties for data authenticity with smart contracts and trust with immutable blockchains. (We will come back to the topic of Web 3 authenticity and integrity below, see *Blockchain: Hash Functions and Digital Signatures)*

Essential to comprehending cryptography are fundamental terms such as *plaintext* (original unencrypted data), *ciphertext* (encrypted data), *encryption* (the process of converting plaintext to ciphertext), *decryption* (the inverse of encryption— the process of converting ciphertext to plaintext), *cryptographic keys* (secret codes utilized for encryption and decryption), and *algorithms* (mathematical functions guiding operations). This newsletter is intended to present an informed view of modern cryptography and to reinforce that use cases extend beyond digital currencies.

Symmetric and Asymmetric Cryptography

Symmetric cryptography is characterized by the use of a single key for both encryption and decryption.[4] This form of cryptography is generally viewed as efficient, particularly in environments where data flows abundantly and speed is crucial. Algorithms like AES (Advanced Encryption Standard) are designed to be both computationally efficient and robust against various forms of attack. Approved back in 2001, AES is still widely adopted for encrypting files and communications to secure sensitive government and financial data, and operates on a fixed block size of 128 bits, and key sizes of 128, 192, or 256 bits. [5,6] The encryption process involves several rounds of transformation: substitution of bytes using a non-linear table (SubBytes), shifting rows of the block cyclically (ShiftRows), mixing the columns using a polynomial operation (MixColumns), and adding the round key to the block (AddRoundKey).[7] The number of rounds (10, 12, or 14) is determined by the size of the key. To improve its versatility and security across various use cases, AES can be implemented alongside different operational modes such as CBC (Cipher Block Chaining) and GCM (Galois/Counter Mode). CBC is ideal for encrypting large volumes of data and typically utilizes an initialization vector (IV) to enhance randomness and security.[8] On the other hand, GCM integrates CBC's encryption capabilities with authentication, protecting both integrity and confidentiality, a critical attribute for modern high-throughput communications.[9] These operational modes enhance AES's foundational strengths, enabling it to effectively meet diverse data protection needs.

The Takeaway: Symmetric cryptography, exemplified by AES, efficiently secures data using a single key for both encryption and decryption, much like a lock and key mechanism in a digital format, and remains robust against attacks through multiple transformation rounds tailored by key size.

However, the Achilles' heel of symmetric cryptography is secure key distribution, particularly in situations where secure channels are scarce. Unlike symmetric cryptography, *asymmetric* cryptography utilizes a pair of keys, public and private, a method that is foundational for the digital signatures and SSL/TLS protocols[10] securing the internet. RSA (Rivest, Shamir, & Adleman) and ECC (Elliptic Curve Cryptography) are two primary examples of asymmetric algorithms.[11] Based on the difficulty of factoring large integers, RSA is widely used for secure data transmission.

However, its computational intensity makes it less practical in environments where speed and resource constraints are important.[12] ECC, on the other hand, offers similar levels of security with smaller key sizes, making it more efficient than its predecessor RSA.[13] This efficiency makes ECC particularly popular in mobile applications and devices with limited processing power.[14]

Asymmetric cryptography is also crucial in the implementation of digital signatures, which provide authenticity and integrity to digital documents. Protocols like ECDH (Elliptic Curve Diffie-Hellman) enhance security by enabling two parties to generate and exchange a shared secret key independently over a public network, like the Internet, without them being intercepted.[15] Elliptic curves, or complex mathematical equations, are graphed by a smooth, curved line, shaped somewhat like a symmetrical, flattened "S", properties that allow for the creation of smaller, faster, and more reverse-engineer resistant keys, compared to preceding methods.[16]

The Takeaway: Asymmetric cryptography, also known as public key cryptography, is often considered more versatile than symmetric cryptography because it uses two separate keys, one public and one private. This setup enables parties who have never met to securely communicate, as they only need to share the public key openly while keeping the private key secret.

Cryptographic Protocols

The Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that secure communications over computer networks. Note that there are numerous other protocols used on the backend of the Internet, each serving distinct functions to facilitate communication, data transfer, and network management, but we will focus on SSL and TLS communication layers.[17] SSL/TLS protocols are known as the bedrock of secure internet communication because they establish encrypted connections between our web browsers and the websites we visit. They employ advanced encryption algorithms to protect our sensitive data, such as login credentials and financial information, from interception by cyber criminals.[18] Despite their critical role in ensuring online security, SSL/TLS protocols often operate seamlessly in the background, seldom drawing attention from everyday users. Yet, without these protocols quietly safeguarding our online interactions, activities like online shopping, banking, and accessing confidential information would be vulnerable to exploitation. The evolution and adoption of blockchain cryptographic protocols are expected to function similarly, on the backend of peer-to-peer transactions and digital ownership validations rather than appearing on the consumer-facing front-end. Nevertheless, we believe these foundational layers will be critical for Web 3 network communications.

Blockchain: Hash Functions and Digital Signatures

Blockchain primarily uses cryptographic hash functions, asymmetric key algorithms, and digital signatures to secure its transactions. Each block in a blockchain contains a cryptographic hash of the previous block, creating a chain of blocks.[19] Hash functions convert data of arbitrary size to a fixed-size string, securing data.[20] This use of hash functions like SHA-256, part of the SHA-2 family, ensures the *integrity* of the blockchain by making it tamper-evident, as altering any single block would require recalculating the hashes of all subsequent blocks, which is computationally infeasible in large chains.[21] Further, each transaction is signed using the private key of the sender, and this signature can be verified by anyone using the sender's public key. This not only confirms the origin of the transaction but also ensures it has not been altered after being issued, confirming *authentication*. Further, consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS) are employed to agree on the validity of the blocks added to the blockchain, making malicious attacks difficult and expensive.

The Future of Cryptography

An exciting development in the field of cryptography is the progression of Fully Homomorphic Encryption (FHE) in recent years. This advanced cryptographic system enables computations to be performed on encrypted data, returning an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.[22] This powerful property allows for secure data processing without exposing the underlying data, presenting profound implications for privacy and security in cloud computing and beyond.[23] For example, this breakthrough would allow for arbitrary computations to be securely performed on encrypted data, as these two operations form a basis for any computation.

In cloud computing, users could encrypt their sensitive data and send it to a cloud service and the cloud service provider could perform computations on this data without ever seeing or decrypting the raw data. This could ensure user privacy while also utilizing the computational power of cloud services. This could be particularly useful for medical researchers analyzing encrypted data from multiple sources to study trends or develop treatments without accessing individual patient records. Another potential FHE use case is secure data sharing and processing among banks and financial institutions, enhancing privacy while complying with regulations. Despite its promise, the widespread adoption of FHE must continue to overcome the substantial computational overhead associated with FHE schemes and find optimizations that could enhance FHE performance. As computational power increases (hardware performance), along with more efficient algorithms being developed (software), we think the potential for practical FHE applications should grow. The cryptographic community remains actively engaged in refining these systems, with a focus on reducing the computational and energy costs associated with FHE operations.

Conclusion

Modern cryptography, through areas like symmetric and asymmetric encryption, cryptographic protocols, and cutting-edge fields like fully homomorphic encryption, forms the backbone of digital security in today's interconnected world. We believe that each development, from the essential frameworks protecting personal and organizational data to innovative solutions like FHE, demonstrates cryptography's critical role in shaping the future of secure digital communications and processing. As we advance, we think the innovative work of technical operators and founders in the cryptographic startup community will become pivotal in defending and enhancing our digital infrastructure and may introduce substantial investment opportunities.

Click Here to listen to the latest episode of Digital Currents

Podcast feed: subscribe to *Digital Currents* in your favorite podcast app, and follow us on Apple Podcasts, or Spotify

[1] https://research-information.bris.ac.uk/en/studentTheses/myths-and-histories-of-the-spartan-scytale

[2] https://www.linode.com/docs/guides/what-is-cryptography/

[3] Aumasson, Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017.

[4] https://www.sciencedirect.com/topics/computer-science/symmetric-encryption

[5] https://nvlpubs.nist.gov/nistpubs/jres/126/jres.126.024.pdf

[6] Daemen, Joan, and Vincent Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. 1st ed., Springer, 2002.

[7] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3089845/

[8] https://www.sciencedirect.com/topics/computer-science/cipher-block-chaining.

[9] https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf

[10] SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols designed to provide secure communication over a computer network. They use a combination of encryption, authentication, and integrity checks to ensure that data transmitted between two systems, like a web browser and a server, remains private and unaltered. TLS, the successor to SSL, is widely used today to secure internet connections and safeguard sensitive data exchanges, such as credit card transactions and personal information.

[11] https://www.netburner.com/learn/comparing-rsa-and-ecc-encryption/

[12] https://www.infosecinstitute.com/resources/cryptography/introduction-to-the-rivest-shamir-adleman-rsa-encryption-algorithm/

[13] https://www.netburner.com/learn/comparing-rsa-and-ecc-encryption/

[14] Hankerson, Darrel, Scott Vanstone, and Alfred Menezes. *Guide to Elliptic Curve Cryptography.* Springer, 2004

[15] https://www.redhat.com/en/blog/understanding-and-verifying-security-diffie-hellman-parameters

[16] Ibid.

[17] These protocols include Transmission Control Protocol (TCP) for reliable data transmission, Internet Protocol (IP) for addressing and routing, Hypertext Transfer Protocol (HTTP) and its secure counterpart HTTPS for web communication, File Transfer Protocol (FTP) for file transfer, Simple Mail Transfer Protocol (SMTP) for email transmission, Domain Name System (DNS) for translating domain names to IP addresses, and Secure Shell (SSH) for secure remote access, among others.

[18] https://www.ssl.com/article/what-is-ssl-tls-an-in-depth-guide/
[19] https://www.ibm.com/topics/blockchain
[20] https://www.ccslearningacademy.com/what-is-hashing-in-cybersecurity/
[21] Ibid.
[22] https://www.ibm.com/topics/homomorphic-encryption#:~:text=Fully%20homomorphic%20encryption%20(FHE)%20is,various%20security%20and%20privacy%20risks.
[23] Ibid.

Important Disclosures
The above information reflects the opinions of Morgan Creek Digital as of the time this is written and all such opinions are subject to change. No representation or warranty, express or implied, is given by Morgan Creek Digital as to the accuracy of such opinions, and no liability is accepted by such persons for the accuracy or completeness of any such opinions.

No Warranty
Neither Morgan Creek Capital Management, LLC nor Morgan Creek Digital warrants the accuracy, adequacy, completeness, timeliness, or availability of any information provided by non-Morgan Creek sources.

This information is neither an offer to sell nor a solicitation of an offer to buy interests in any investment fund managed by Morgan Creek Capital Management, LLC or its affiliates, nor shall there be any sale of securities in any state or jurisdiction in which such offer or solicitation or sale would be unlawful prior to registration or qualification under the laws of such state or jurisdiction. Alternative investments involve specific risks that may be greater than those associated with traditional investments.

Forward-Looking Statements
This presentation contains certain statements that may include "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. All statements, other than statements of historical fact, included herein are "forward-looking statements." Included among "forward-looking statements" are, among other things, statements about our future outlook on opportunities based upon current market conditions. Although the company believes that the expectations reflected in these forward-looking statements are reasonable, they do reflect all assumptions, risks and uncertainties, and these expectations may prove to be incorrect. Actual results could differ materially from those anticipated in these forward-looking statements as a result of a variety of factors. One should not place undue reliance on these forward-looking statements, which speak only as of the date of this discussion. Other than as required by law, the company does not assume a duty to update these forward-looking statements. Past performance is no guarantee of future results. The illustrations are not intended to predict the performance of any specific investment or security.

General
This is neither an offer to sell nor a solicitation of an offer to buy interests in any investment fund managed by Morgan Creek Capital Management, LLC or its affiliates, nor shall there be any sale of securities in any state or jurisdiction in which such offer or solicitation or sale would be unlawful prior to registration or qualification under the laws of such state or jurisdiction. Any such offering can be made only at the time a qualified offeree receives a Confidential Private Offering Memorandum and other operative documents which contain significant details with respect to risks and should be carefully read. Neither the Securities and Exchange Commission nor any State securities administrator has passed on or endorsed the merits of any such offerings of these securities, nor is it intended that they will. This document is for informational purposes only and should not be distributed.

Risk Summary
Interests in the Morgan Creek Digital Fund IV, LP ("Fund") are speculative and involve a significant degree of risk. Cryptocurrencies and related businesses have limited performance histories, can be extremely volatile, and are not subject to many of the regulatory oversights over which other investable assets are subject. An investment in the Fund is suitable only for sophisticated investors and requires the financial ability and willingness to accept the high risks and limited liquidity inherent in the Units.

There can be no assurance that the Fund will be successful or that losses will not be incurred by the Fund. Each investor in the Fund must have the ability to bear the risk of loss of their entire investment and must be prepared to bear such risks for an extended period of time. Investors are strongly urged to consult with their professional advisors and to carefully review the risk prior to investing.

Performance Disclosures
There can be no assurance that the investment objectives of any fund managed by Morgan Creek Capital

Management, LLC will be achieved. Past performance is not indicative of the performance that any fund managed by Morgan Creek will achieve in the future. Although Morgan Creek Capital Management, LLC has been presented with co-investment opportunities in the past, there can be no assurance that Morgan Creek will be presented with similar opportunities in the future. Further, there can be no assurance that co-investment opportunities will be available in the future.