T.C.
HASAN KALYONCU UNIVERSITY

ELLIPTIC CURVE CRYPTOGRAPHY

Prof. Dr. Recep DEMİRCİ

Berkay Gündüz

211501030

1. INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the scientific study and practice of methods for keeping data and communication safe from people who shouldn't have access to them or can change them. It entails changing information into an unreadable format (encryption) and reverting it to a readable one (decryption) via the use of algorithms and keys. Cryptography guarantees the following outcomes[1]:

1. **Confidentiality:** Ensures that only intended senders and receivers can access the data.
2. **Integrity:** Protects data from being altered without detection.
3. **Non-Repudiation:** The creator/sender of data cannot deny their intention to send information at a later stage[2]
4. **Authentication:** The identities of the sender and the receiver, along with destination and origin of the data, are confirmed.
5. **Interoperability:** It allows for secure communication between different protocols of cryptography.
6. **Adaptability:** It should be enabled so that it can be extended whenever required.

2. CIA TRIAD

In the information security community, CIA triad stands for **confidentiality, integrity** and availability. Together, these three principles form the pillars of any organiztion's security infrastructure.

3. TYPES OF CRYPTOGRAPHY

Cryptography is a sub-branch of information security along with information hiding. Information hiding is a principle in information security that focuses on concealing the internal details of a system or component (text, audio, video, image, watermarking). Cryptography contains **key-based** and **keyless** *(caesar cipher etc.)* methods in order to encapsulate data from unintended receivers.

3.1. Key-based Cryptography:

3.1.1. **Symmetric Key:** In symmetric-key cryptography, the same key is used for both

encryption and decryption of the data. This means, the sender and the receiver must both have access to the same secret key, which needs to be kept secure. Symmetric key is fast and efficient for encrypting large amounts of data, however it is a challenge to distribute the key securely.

3.1.2. **Asymmetric Key:** Asymmetric key cryptography uses two different keys: a public key (used for encryption) and a private key (used for decryption). The public key is shared openly while the private keys remain secret and is not distributed. It is slower than symmetric key method however it is way more secure for communication between parties who have never met. Examples of asymmetric-key cryptography are: RSA Algorithm, Elliptic Curve Cryptography, Digital Signature Algorithm.

4. Elliptic Curve Cryptography

Elliptic Curve Cryptography is a key-dependent method for data encryption. Elliptic Curve Cryptography (ECC) emphasizes the use of pairs of public and private keys for the encryption and decryption of data. ECC is often referenced in relation to the RSA algorithm. RSA accomplishes one-way encryption of data, such as emails and software, by prime factorization.

Elliptic Curve Cryptography (ECC) serves as an alternative to Rivest-Shamir-Adleman (RSA). It establishes security between key pairs using the mathematics of elliptic curves. RSA utilizes prime numbers, however ECC has been more favored lately because to its reduced key size and capacity to maintain security. In contrast to RSA, ECC's methodology for public key cryptography systems is based on the algebraic structure of elliptic curves over finite fields. Consequently, ECC generates keys that are mathematically more challenging to decipher.

An elliptic curve is a plane curve characterized by the equation $y^2 = x^3 + ax + b$, where a and b are constants, and x and y are variables. Elliptic curves include several intriguing mathematical characteristics that make them very appropriate for encryption. For instance, given two points P and Q on an elliptic curve, there exists a third point R such that $P + Q = R$. This attribute is referred to as "point addition."

Another significant property of cryptography is "point doubling." This involves selecting a point P on an elliptic curve and determining another point 2P such that $P + P = 2P$. We may continue to double points until we reach what is referred to as "the infinity point," denoted as O. This indicates that an endless number of keys may be produced from a single elliptic curve.

Elliptic curve cryptography often depends on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which asserts that determining x is challenging when y = g^x mod p is known, where g is a specified integer and p is a prime number.This issue is intricate due to the absence of an efficient method to determine x given y, namely without exhaustively testing every potential value of x until a suitable one is identified. Given the difficulty of solving the DDL issue, it therefore follows that determining y would likewise be challenging if x = g^y mod p is known. Consequently, it would be difficult for a someone unaware of the secret exponent y to get y from x, unless they exhaustively test every potential value until a suitable one is discovered. Consequently, if our parameters g and p are selected judiciously, it should be challenging for an individual unaware of the secret exponent x to derive x from y (or vice versa). Provided that deriving the secret exponent x from y (or the reverse) remains computationally challenging, elliptic curve cryptographic methods are applicable for digital signatures and key agreement protocols.

5. REAL WORLD APPLICATIONS OF ELLIPTIC CURVE

As previously noted, ECC's reduced key size is ideally suited for devices that have limited CPU and memory capabilities, including mobile and IoT devices. This allows developers of web and mobile applications to create high-performance, low-latency websites and applications, all while ensuring strong data security for their users. ECC is often employed to enhance the security of wireless mobile communication protocols such as Bluetooth, Wi-Fi, and Near Field Communication (NFC).

Secure communication protocols utilize ECC for encryption, digital signatures, and key exchange. Instances encompass Transport Layer Security (TLS) utilized in secure web browsing, Secure Shell (SSH) for secure remote login, and Virtual Private Networks (VPNs) for secure network communication.

Cryptocurrency and blockchain technology: Numerous cryptocurrencies, such as Bitcoin, Ethereum, and Litecoin, employ elliptic curve cryptography for the generation of public and private key pairs, in addition to signing transactions. ECC delivers the essential cryptographic protection required to safeguard digital assets and maintain the integrity of

blockchain networks.

Smart cards and embedded systems: ECC is frequently utilized for the security of payment systems, access control systems, electronic passports, and various other applications that necessitate secure and compact cryptographic solutions.

Digital signatures and certificates: ECC is applicable for generating digital signatures, essential for verifying the authenticity and integrity of digital documents and messages. Digital signatures based on ECC are utilized in Public Key Infrastructure (PKI) systems for the issuance and validation of digital certificates.

Although ECC is relatively recent in comparison to RSA, it benefits from extensive standardization and backing from private-sector organizations and industry groups. The U.S. National Institute of Standards and Technology (NIST) has established ECC as a standard within its collection of cryptographic algorithms. Furthermore, ECC enjoys support from widely used cryptographic libraries, programming languages, and operating systems. This acceptance enhances its integration across multiple sectors including finance, healthcare, and government services.

Taking these factors into account, it can be concluded that elliptic curve cryptography enjoys significant popularity and is extensively utilized across various applications and industries. The combination of its efficiency, security, and extensive support has established it as a reliable option for secure communication and cryptographic tasks.

6. Conclusion

In conclusion, cryptography remains a critical element in ensuring the security and privacy of data in today's digital landscape. Its ability to protect sensitive information from unauthorized access and manipulation is essential across all industries, from finance to healthcare, e-commerce, and beyond. Through the use of various cryptographic techniques such as symmetric and asymmetric encryption, hashing, and digital signatures, cryptography guarantees the core security principles of Confidentiality, Integrity, Authentication, Non-Repudiation, and Interoperability.

Among these cryptographic methods, Elliptic Curve Cryptography (ECC) stands out due to its unique ability to provide strong security with smaller key sizes compared to traditional algorithms like RSA. This makes ECC especially well-suited for applications that require high levels of security with minimal computational overhead, such as mobile devices, IoT systems, and resource-constrained environments. ECC's scalability, efficiency, and robust security features are why it is increasingly used in modern cryptographic systems, including Secure Communication Protocols like TLS and SSH, Blockchain Technologies for securing cryptocurrencies, and Digital Signatures for verifying the authenticity and integrity of data.

The integration of ECC into various sectors, including government, finance, and healthcare, highlights its growing importance. As digital transactions and communications continue to evolve, the need for reliable, fast, and secure cryptographic methods becomes more pressing. ECC's adoption across industries is a testament to its effectiveness and efficiency in meeting these security needs. Furthermore, with institutions like the National Institute of Standards and Technology (NIST) endorsing ECC as a standard cryptographic algorithm, its role in shaping future cryptographic practices is set to increase even further.

Moreover, the adaptability of cryptography, including ECC, to address emerging challenges in cybersecurity is crucial. As new threats and vulnerabilities emerge, cryptographic techniques must evolve to protect data against increasingly sophisticated attacks. ECC's ability to maintain a high level of security even with reduced key sizes positions it as an ideal candidate for the next generation of cryptographic applications. This adaptability ensures that ECC and other cryptographic methods can continue to meet the security demands of tomorrow's digital landscape.

The future of cryptography, driven by innovations like ECC, is promising. With its widespread adoption and increasing standardization, ECC is expected to play a central role in securing communications, digital transactions, and data privacy for years to come. As the world becomes more interconnected, the reliance on cryptographic solutions to protect sensitive information will only grow, reinforcing the importance of cryptography as a cornerstone of cybersecurity. Thus, the continued development, implementation, and enhancement of cryptographic techniques such as ECC will remain vital in safeguarding our digital future.

7. Sources

7.1. https://www.keepersecurity.com/blog/2023/06/07/what-is-elliptic-curve-cryptography/

7.2. https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/

7.3. https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

7.4. https://www.vmware.com/topics/elliptic-curve-cryptography

7.5. https://www.academia.edu/111973994/1_Introduction_to_Cryptography

7.6. CENG-481 – Cryptography – Lecture notes