

# Real Life Applications of Cryptography

Pratik Solanki, Samruddh Uchil

(Keraleeya Samajam’s Model College, Dombivli East, Mumbai, Maharashtra, India

Email: pratik7solanki@gmail.com)

(Keraleeya Samajam’s Model College, Dombivli East, Mumbai, Maharashtra, India

Email: samruddhuchil.model@gmail.com)

\*\*\*\*\*

## Abstract:

Cryptography, a vital element in digital security, is instrumental in various real-life applications. It secures online transactions, protects sensitive healthcare data, and fortifies critical infrastructure. From bolstering cybersecurity for individuals to enabling secure communication in emerging technologies like blockchain IoT, cryptography continues to be backbone in ensuring the integrity & confidentiality of information in our interconnected world.

**Keywords —Cryptography, asymmetric, data, security, network.**

\*\*\*\*\*

## I. INTRODUCTION

Cryptology, an extensive field dedicated to the exploration of secure communication techniques, demonstrates its relevance across diverse industries and everyday scenarios. Its impact is instrumental in safeguarding information, fortifying the security of systems, and enabling confidential communication within our progressively digitized environment. In our digitally driven society, where information traverses the globe in an instant, the need for robust security measures is paramount. Cryptography, a field steeped in history, has emerged as the linchpin in our defense against cyber threats. This paper sheds light on how cryptography, once confined to military and intelligence circles, has become an integral part of our daily lives. Cryptography finds practical use in numerous everyday situations to protect communication and data. It's present in popular messaging like WhatsApp, digital signatures, and the secure connections of HTTPS. Its applications extend to banking transactions, email security, safeguarding homes, and beyond. Real-world instances include using Hardware Security Module Encryption (HSM) for cash withdrawals, ensuring

secure information transfer on the internet with HTTPS, and employing SSL encryption for email communication. The potential applications also stretch to fields such as cloud-based storage, smartphones, and Internet of Things (IoT) devices, showcasing the versatility and relevance of cryptographic methods in our technologically interconnected world.

## II. WHAT IS CRYPTOGRAPHY

Cryptography is a practice and study of techniques for securing communication and information from adversaries or third parties. It involves the use of mathematical algorithms to convert readable information (plaintext) into an unreadable format (ciphertext), making it difficult for unauthorized individuals to understand the content without the appropriate key or algorithm for decryption.

The objectives of cryptography are:

**Confidentiality:** Ensure that the information remains confidential and is only accessible to authorized parties.

**Integrity:** Guarantee the integrity of the information, ensuring that it has not been altered or tampered during transmission or storage.

**Authentication:** Verify the identity of parties involved in communication, ensuring that the sender and recipient are who they claim to be.

**Non-repudiation:** Prevent the denial of actions or transactions by ensuring that the parties involved later cannot deny their participation.

### **III. WHY IS CRYPTOGRAPHY NEEDED?**

Cryptography is a fundamental necessity in our modern digital landscape for several critical reasons. Firstly, it ensures the confidentiality of sensitive information by transforming into an unreadable format, safeguarding personal, financial, and classified data from unauthorized access. Secondly, cryptography plays a crucial role for maintaining the integrity of data. Through techniques like digital signatures and hash functions, it detects and prevents tampering, guaranteeing that information remains unaltered during transmission or storage. Additionally, cryptography serves as a cornerstone for authentication, verifying the identities of users, systems, or devices. This is crucial for reducing the risks of unauthorized access and secure communication. Non-repudiation, another essential aspect, is facilitated by cryptography, preventing parties from denying their actions through the use of techniques like digital signatures. In an era where digital communication is ubiquitous, cryptography is indispensable for securing messages during transmission, as exemplified by protocols like SSL/TLS.

### **IV. TYPES OF CRYPTOGRAPHY**

Cryptography can be broadly categorized into two types:

**Symmetric Cryptography:** In symmetric cryptography, the same key is used for both

encryption and decryption. The sender & receiver shares the secret key securely. Algorithms like Data Encryption Standard and Advanced Encryption Standard are examples of symmetric cryptography.

**Asymmetric Cryptography:** Asymmetric cryptography is known as Public key cryptography, it uses a pair of keys: a public key for encryption and a private key for decryption. The public-key is distributed, while private key should be kept secret example Elliptic Curve Cryptography.

### **V. CRYPTOGRAPHY TECHNIQUES**

**Encryption Algorithms:** Mathematical algorithms that transform plain text into cipher text using keys.

**Hash Functions:** Algorithms that generate fixed-size outputs (hash values) from variable-size inputs. Hash functions used for data integrity verification, password, and digital signatures.

**Digital Signatures:** Digital signatures provide a way to verify authenticity and the integrity of digital messages and documents.

**Public Key Infrastructure (PKI):** A framework that manages digital keys and certificates, facilitating secure communication over the internet.

**Secure Communication Protocols:** Protocols like SSL/TLS for securing web traffic, IPsec for securing network communications, and PGP (Pretty Good Privacy) for securing email communication.

### **VI. APPLICATIONS OF CRYPTOGRAPHY**

Cryptography has numerous real-life applications across various industries and everyday scenarios. Here are some specific examples:

**Online Banking and Transactions:** Cryptography ensures the security of online banking transactions, including fund transfers, bill payments, and account

management. SSL/TLS protocols secure the communication between users and banking servers.

**E-commerce Transactions:** Cryptography secures online shopping transactions by encrypting payment information. This is crucial in protecting credit card details and ensuring the integrity of purchase data.

**Secure Sockets Layer known as SSL and Transport Layer Security known as TLS:** These cryptographic protocols are widely used to secure communication over the internet. They are integral to the security of websites, including e-commerce platforms, social media, and online banking.

**Email Encryption:** Cryptography is employed to secure email communications. Technologies like Pretty Good Privacy (PGP) and S/MIME use encryption to protect the content and attachments of emails.

**Virtual Private Networks :** VPNs use cryptographic techniques to create secure and encrypted connections over the internet. This ensures the privacy and security of data transmitted between a user and a remote server.

**Secure File Storage:** Cryptographic techniques are used to encrypt files and folders, providing an extra layer of security for sensitive data stored on computers, external drives, or cloud storage.

**Healthcare Data Security:** Cryptography is crucial in the healthcare industry to protect patient records and sensitive medical information. It helps ensure compliance with privacy regulation such as the HIPAA.

**Smart Cards and RFID Technology:** Cryptography secures smart cards and Radio-Frequency Identification (RFID) technology, which are used in access control systems, public transportation cards, and contactless payment systems.

**Digital Signatures:** Digital signatures, created using cryptographic algorithms, are used in verifying the authenticity of digital document. They play crucial role in contracts, legal documents, and electronic transactions.

**Cryptocurrencies:** Cryptocurrencies like Bitcoin and Ethereum rely on cryptographic principles to secure transactions, controls the creation of new units, and ensure the integrity of the decentralized blockchain.

**Military and Defense Communications:** Governments and military organizations use cryptography to secure sensitive communications, ensuring that information remains confidential and also protected from unauthorized access.

**Authentication in Software and Services:** Cryptographic techniques are used for user authentication, password storage, and access control in software applications, online services, and social media platforms.

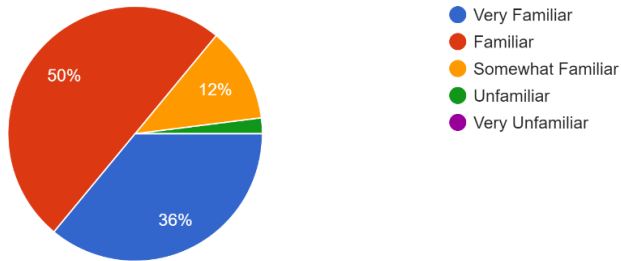
**IoT Security:** Cryptography is essential in securing communication between Internet of Things (IoT) devices to prevent unauthorized access, data tampering, and ensure the privacy of information collected by these devices.

**Anonymous Communication:** Cryptographic tools and protocols are employed to enable anonymous communication, protecting the privacy of individuals engaged in activities like online activism or whistleblowing.

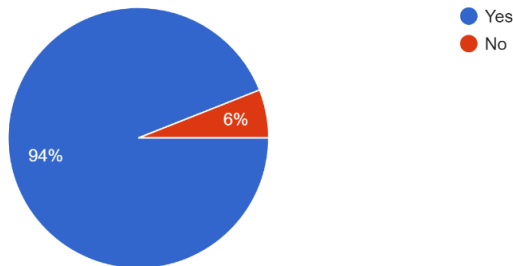
### VII. SURVEY RESULTS

So we asked some students and workers few questions related to the topic here are the results:

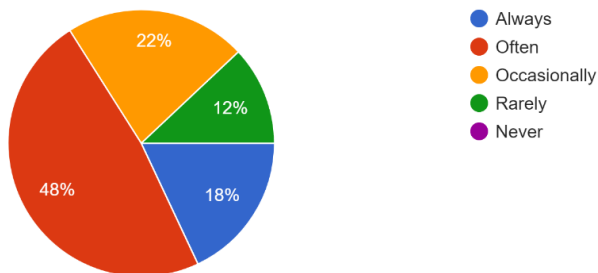
How familiar are you with the term "Cryptography"?  
50 responses



Have you ever used encryption tools or software to secure your digital communications or files?  
50 responses

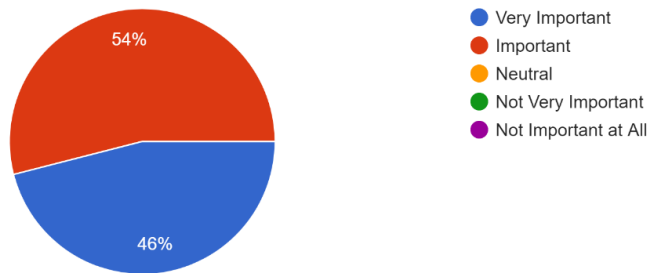


How often do you check for secure connections (SSL/TLS) when accessing websites?  
50 responses



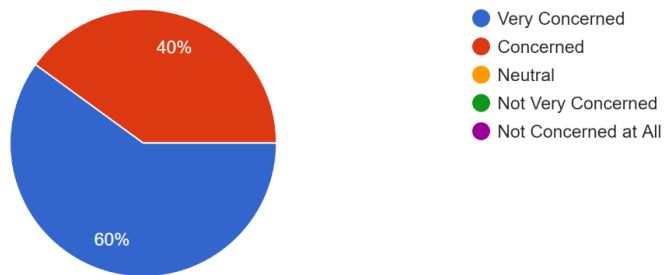
How important do you consider secure communication for online activities such as banking, shopping, or social media?

50 responses



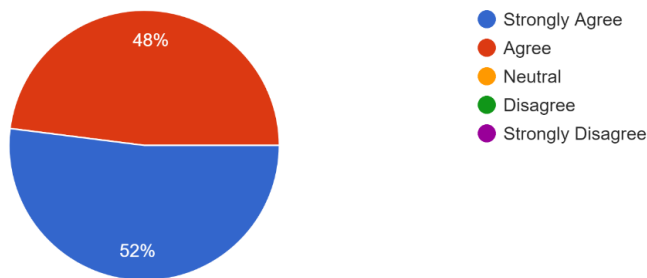
How concerned are you about the security of your personal data stored in the cloud or on online platforms?

50 responses



Do you believe that individuals have the right to private, encrypted communication?

50 responses



## VIII. CONCLUSION

The real-life applications of cryptography impact us in ways we might not always notice, but they are fundamental to our digital security. Whether it's the padlock symbol on our browsers, keeping our online transactions safe, or the encrypted messages we send, cryptography is the unsung hero of our online experiences. Its role in protecting our data, ensuring privacy, and enabling secure communication is essential for the smooth functioning of our increasingly interconnected world. As we continue to embrace the digital age, the simple yet powerful applications of cryptography serve as the invisible shield that allows us to trust and engage with the online world confidently.

Looking forward, the ongoing development of cryptographic techniques will be crucial in staying ahead of emerging threats. As technology evolves, so do the challenges, and cryptography must adapt to ensure the continued security of digital interactions. From personal privacy to financial

## REFERENCES

- [1] [Medium - Real Life Applications Of Cryptography](#)
- [2] [Ronanthewriter – Application of Cryptography indaily life](#)
- [3] [Analyticssteps – Characteristics Types and ApllicationsOf Cryptography](#)
- [4] [Resources.infosecinstitute – Basics of Cryptography](#)
- [5] [Netleon.com - cryptography-real-world-application](#)
- [6] [Bertytech - cryptography-daily-usage](#)