IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EMAIL AUTHENTICATION USING CRYPTOGRAPHY

[1]Dr. Balaji K, [2]Ashwini P, [3]Likhitha P, [4]Jagadevi, [5]Gnanapriya -- (MCA 1st year)

[1]Professor, Department of MCA, Cambridge Institute of Technology CITech, Bengaluru, India, [2,3,4,5] Student, Department of MCA, CITech, Bengaluru, India

ABSTRACT

Setting up an email account involves confirming ownership through a link sent to the provided email address. Personal questions, like favorite colors or pets' names, may also be asked for added security. Email services monitor login locations and usage patterns to detect suspicious activity. Two-factor authentication adds an extra layer of security by sending a code to the user's phone. Account recovery processes often include sending a reset link to an alternate email or mobile number. During email sessions, encryption and session management techniques are used to protect user data. Automatic logout may occur after a period of inactivity to prevent unauthorized access. These measures collectively ensure email account security and user verification.

INTRODUCTION

Cryptography is the digital lock for our secrets, transforming information into unreadable code that only the intended recipient can decipher, ensuring privacy and security in our digital world. Rooted in ancient techniques of secret writing, cryptography has evolved into a sophisticated science, employing mathematical algorithms to encode and decode messages. From the Enigma machine of World War II to the complex encryption schemes of today, its application spans military, governmental, and commercial domains. By transforming plaintext into ciphertext and back again, cryptography ensures the confidentiality, integrity, and authenticity of data. As we embark on this exploration of cryptography, we delve into its history, principles, and practical applications, unveiling the mysteries behind its enduring relevance in the modern age of information.

Confirmation emails with clickable links are sent during sign-up to confirm ownership. Personal questions may be asked during sign-up or password recovery to verify identity. Suspicious activity, like unusual login locations, prompts additional verification steps. Two-factor authentication enhances security by requiring a code sent to the user's phone. Account recovery processes involve resetting passwords via alternate contact methods or security questions. Encryption and session management are used to secure data during email sessions. Automatic logout may occur to prevent unauthorized access due to inactivity.

WHAT IS CRYPTOGRAPHY

Cryptography is the practice of encoding and decoding information to keep it secure from unauthorized access. It involves converting plain text into ciphertext using algorithms, making it unreadable to anyone without the proper key. Encryption ensures that sensitive data, like passwords or financial transactions, remains confidential during transmission. It also verifies the integrity of the data, ensuring it hasn't been tampered with. Cryptography plays a crucial role in cybersecurity, protecting against hackers and ensuring privacy in digital communication. It's like using a secret language between trusted parties, where only those with the key can understand the message. Cryptographic techniques include symmetric encryption, where the same key is used for both encryption and decryption, and asymmetric encryption, which uses different keys for each operation. Cryptography is used in various applications, from securing online banking to protecting government communications. It continues to evolve to counter emerging threats and vulnerabilities. In essence, cryptography is the safeguard that keeps our digital world safe and secure. There are three types of Cryptography- Symmetric key Cryptography, Asymmetric key Cryptography, and Hash functions.

Symmetric Key Cryptography

Symmetric key Cryptography is also called as secret-key cryptography, in this type of Cryptography, we use only one key. By using this single key sender and receiver can encrypt and decrypt a message. This key system is faster and simple, but the problem is key exchange between sender and receiver is somehow should be in secure manner. The most famous symmetric key cryptography systems are Data Encryption System (DES) and Advanced Encryption System (AES). An example for Symmetric Key Cryptography is Blowfish.

Hash Functions

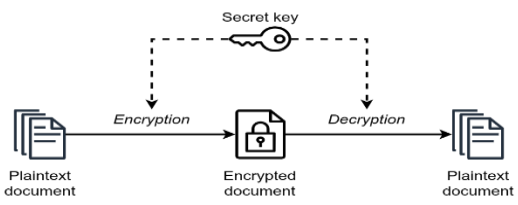
Hash function also known as message digests and one-way encryption, and they are the algorithms that in some sense and no use of any key. Rather, a fixed-Length hash value is figured out based upon the plaintext that makes it is not possible for either the contents or length of the plaintext to be recovered. Hash functions are mainly used to provide a digital fingerprint authentication of a file's contents, often used to ensure that the file has not been altered or changed by an intruder or virus. Hash algorithms that are popularly used nowadays include Message Digest Algorithms (MDA) and Secure Hash Algorithms (SHA).

Asymmetric Key Cryptography

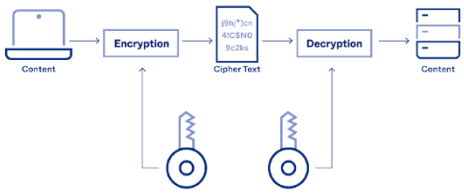
Public-key cryptography is also known as Asymmetric key cryptography, and we use two keys in this type of cryptography. This cryptography is different from and is more secured than symmetric key cryptography. In this key system, each user encrypts and decrypts using two keys or a pair of keys (private and public keys). Each user keeps the private key secret and the public key is distributed across the network so that everyone can use those public keys to send a message to any other user. We can use any of those keys to encrypt the message and can use the remaining key for decryption. An RSA algorithm is sample of asymmetric key cryptography.

CRYPTOGRAPHIC ALGORITHMS

- ✓ Secret key (symmetric key) Cryptography- SKC uses a single key for both encryption and decryption.

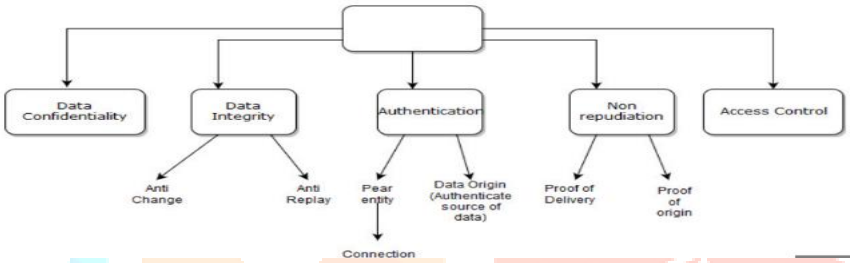


- ✓ Public key (asymmetric key) cryptography-PKC uses two keys, one for encryption and the other for decryption.



✓ Hash Function (one-way cryptography)-Hash Function have no key since the plaintext is not redeemable from the cipher text.

PURPOSE OF CRYPTOGRAPHY



(i) Data confidentiality is the prevention of transmitted data from passive attacks. Respect to the content of a data transmission, several levels of protection can be identified This requires that an attacker not be able to observe the source and destination prevalence, length or other features of the traffic on a communications facility.

Different services of data confidentiality are Connection Confidentiality, The prevention of all user data on a connection. Connectionless Confidentiality, The prevention of all user data in a one data block. Selective-Field Confidentiality, The confidentiality of selected area within the user data on a connection or in a single data block. Traffic Flow Confidentiality, the precaution of the information that might be derived from the examination of traffic flows.

(ii) Data Integrity: it is designed to protect data from modification, insertion, deletion and replaying by adversary. As with confidentiality, integrity can put into a flow of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total flow protection.

(iii) Authentication: The authentication service is to satisfy the recipient that the message is from the source that it claims to be from it provides authentication of the sender or receiver during the connection establishment. Two specific authentication services are defined in X.800. Peer Entity Authentication Used in association with a logical connection to provide confidence in the individuality of the entities connected. Data Origin Authentication in a connectionless transfer, provides self-assurance that the source of received data is as claimed.

(iv) Non repudiation: Non repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent the receiver can prove that the assumed sender in fact sent the message. Similarly, when a message is received, the sender can prove that the assumed receiver in fact received the message.

• Non repudiation, Genesis Proof that the message was sent by the specified party

• Non repudiation, Destination that the message was received by the specified

(v) Access Control: Access control is the ability to protect against the unauthorized access to data in this, each entity trying to gain access must first be identified, or authenticated. So that access rights can be customized to the individual.

AUTHENTICATION

Authentication is the mechanism of identifying users that request access to a system, server, network, website, app, or a device. The major goal of authentication is to confirm that a user is who they claim to be. For example, User A has access to only pertinent information and is not able to see User B's personal informal. Unauthorized users are put a stop from accessing sensitive data with user authentication. Authentication upgrade security by allowing any Organizational admin to manage a single user's identity and access. The fundamental authentication used for identity and access control verification is username and password, with various types of authentication techniques- Password Based Login, Multifactor Authentication (MFA), Bio-metric Authentication, Certificate-based authentication, and Token-Based Authentication.

Authentication is part of three-step process for obtain access to digital resources:

- Identification – who are you?
- Authentication – Prove it.
- Authentication – Do you have permission?

EMAIL AUTHENTICATION

A key point of the email delivery is the email authentication. ISPs and several email servers, in general, decide the reliability and authenticity of your email based on the email security policies that you have in place. Further, Authentication is a hi-tech method for identifying spam and verifying that an email is actually sent by the sender, which refers to the technological standards. ISPs and organizations utilize these technical standards to stop the harmful emails such as phishing and spam. Hosted Email Security is a non-maintenance required solution that provides constantly updated prevention against threats.

SYSTEM ARCHITECTURE DESIGN

In this section, the general and detail architecture of Hosted Email Security (HES) are presented.

FIGURE 1. General Architecture of HES.

Figure 1 Demonstrates the general architecture HES. Only authorized sender may access to the system. Sender log-in to access the System. The system authorizes the sender. Next, Sender looks around for the file, delivery it into the system and enter the symmetric key. The symmetric key is shared with the recipient. The system encrypts the file. After the file is encrypted, the file is delivered through email to the recipient. Once the recipient decrypts the file, the sender is given notice via email.

The security architecture of Hosted Email Security is shown in figure 2. The file is encrypted using the recipient public key and creates a ciphertext. The ciphertext then is encrypted using both shared symmetric

keys. The mechanism implies in as: C = E (k, E (pk, M)), here C is ciphertext, k is the symmetric key, M is the file, and pk is public key.

Once the recipient received the file, the recipient decrypts the file using the shared symmetric key then with that private key. The mechanism implies in as: M = D (sk, D (k, c)). The decryption activity for the recipient is the reverse order from the sender. Upon the victorious of recovering the file, the system sends the notification victory to the sender.

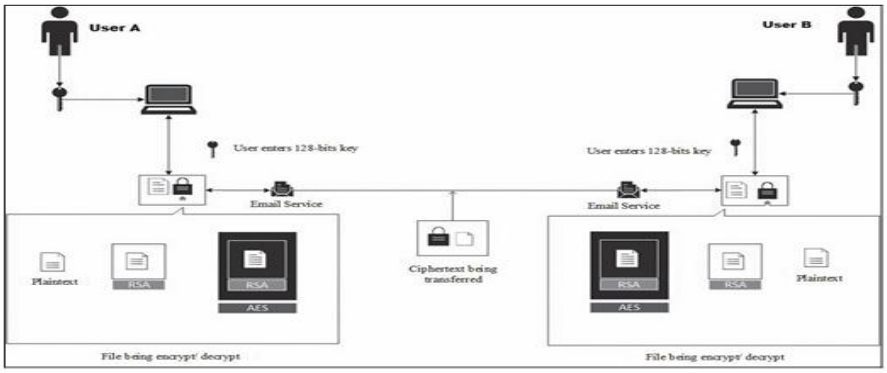


FIGURE 2. Security Architecture of HES.

HOW TO AUTHENTICATE EMAIL

(i)**Use consistent sender addresses**: Be consistent with from address and friendly from name you use, it can be enticing to have subscribers open a message out of interest, but trust in a message starts with a recipient easily realizing the sender as a brand they assure. Persistently changing from names and from addresses makes your recipients more permitting to phishing.

(ii) **Authenticate your IP addresses with SPF**: Sender Policy Framework be set as SPF and compares the email sender's actual IP address to list of IP addresses approved to send mail from that domain. The Sender Policy Framework record is added to a sender's domain name system (DNS) and contain a list of authorized IP addresses. Sender's utilizing Twilio SendGrid's instinctive security.

(iii) **Configure DKIM signatures for your messages:** DKIM stands for Domain keys Identified Mail is an authentication standard that cryptographically signs the messages you send so that receiving servers are assured there was no difference of the message in transit. When you set up an authenticated domain with Twilio SendGrid, we will utilize that domain to sign your messages.

(iv) **Domain-based Message Authentication, Reporting & Conformance:** DMARC stands for Domain-based Message Authentication, Reporting & Conformance and it is a protocol that uses SPF and DKIM to further prevent phishers from spoofing messages.

(v) **Prepare for BIMI:** Brand Indicators for Message Identification (BIMI) is an extra bit of goodness atop the authentication cake that provides and even stronger inbox trust experience for your recipients.

CONCLUSION

In today's digital landscape, where information flows freely and communication happens at the click of a button, the importance of keeping our data safe and secure cannot be overstated. Cryptography, which is like a digital lock and key, plays a crucial role in ensuring the confidentiality, integrity, and authenticity of our information.

From ancient times to the modern era, cryptography has evolved from simple techniques of hiding messages to complex mathematical algorithms. This evolution has been driven by the need to protect sensitive information from prying eyes and malicious actors. In the realm of email security, authentication mechanisms such as SPF, DKIM, and DMARC act as gatekeepers, ensuring that only legitimate emails make their way to our inboxes. These measures not only safeguard against spam and phishing attacks but also foster trust and reliability in digital communication.

REFERENCE

https://phdservices.org/latest-research-topics-in-cryptography-and-network-security/

https://www.packetlabs.net/posts/cryptography-attacks/

https://sendgrid.com/en-us/blog/how-to-authenticate-your-email-in-5-steps

https://www.miniorange.com/blog/different-types-of-authentication-methods-for-security/