International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Case Study On Cryptography in the Field of Social Media

Harish A.M[1], *Ram Balaji.V*[2]

[1]UG Student Computer Science Department,Sri Krishna Arts And Science College, CBE
[2]UG STUDENT Computer Science Department,Sri Krishna Arts And Science College,CBE.
[1]E-MAIL: harisham21bds015@skasc.ac.in
[2]E-MAIL: rambalajiv21bds034@skasc.ac.in

ABSTRACT:

The article represent about Cryptography in social mediaCryptography or cryptology , is the practice and study of techniques for secure communication in the presence of adversarial behavior. Typically, cryptography is about creating and analyzing agreements that prevent third-party companies or the public from reading confidential messages various aspects of data protection such as data confidentiality, data integrity, authentication, and denial are the basis of modern encryption. Modern cryptography is at the crossroads of mathematical learning, computer science, electrical engineering, communications science, and physics. Cryptography applications include electronic trading, chip-based payment cards, digital currencies, computer passwords, and military communications.

KEYWORDS:Cryptography-secret key cryptography-Public key cryptography-hash functions-End to end encryption.

1. INTODUCTION

Cryptography helps securing the data storehouse and transmission with the thing that only intended stoner can use it. It keeps the data fully hidden from the third party who's actually present at the same time

In social media app using E2EE encryption means that only the sender and receiver can read the translated data because the key to decipher the data lies only with the end stoner. No other realities including the service provider has the capacity to decipher the data indeed though the data travels through their waiters

1.1 CRYPTOGRAPHY

Cryptography or cryptology, is the practice and study of ways for secure communication in the presence of inimical geste. More generally, cryptography is about constructing and assaying protocolsthat help third parties or public from reading private dispatches colorful aspects of information security similar as data confidentiality, data integrity, authentication, and nonrepudiation are central to ultramodern cryptography. Ultramodern cryptography exists at the crossroad of the disciplines of mathematics, computer wisdom, electrical engineering, communication wisdom, and drugs. Operations of cryptography include electronic commerce, chipbased payment cards, digital currencies, computer watchwords, and military dispatches.

TYPES OF CRYPTOGRAPHY :

CRYPTOGRAPHY CAN BE BROKEN DOWN INTO THREE TYPES:
PUBLIC KEY CRYPTOGRAPHY
SECRET KEY CRYPTOGRAPHY
HASH FUNCTIONS

PUBLIC KEY CRYPTOGRAPHY:

Public Crucial cryptography, or asymmetric cryptography, is a cryptographic system that uses crucial dyads. Each brace contains a public key and a private key. The development of similar important dyads relies on cryptographic algorithms grounded on fine problems called one- way operations. Active security requires keeping a private crucial nonpublic; a public key can be distributed openly without compromising security.

In an asymmetric crucial encryption system, anyone can cipher dispatches using a public key, but only the paired private crucial holder can clear similar encryption. The security of the system depends on the secretiveness of the private key, which shouldn't be known to anyone differently.

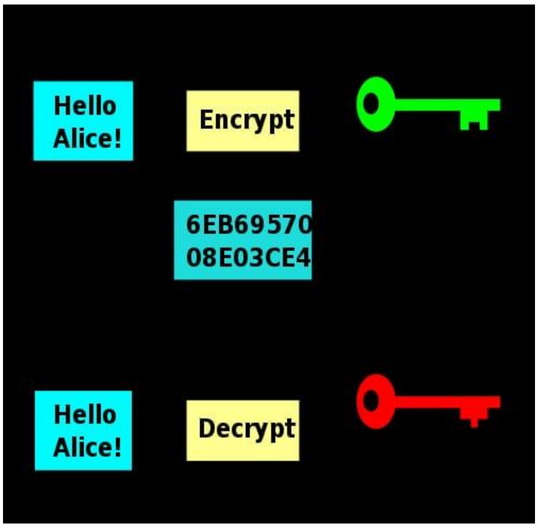

FIGURE:1 PUBLIC KEY

SECRET KEY CRYPTOGRAPHY :

The secret crucial cryptography has been used for thousands of times in a variety of ways. Ultramodern executions frequently take the form of algorithms used by computer systems in tackle, firmware or software. Utmost of the secret crucial algorithms are grounded on tasks that can be performed veritably well by digital computer systems.

Traditionally, this process uses algorithms where the key used to write an empty blank textbook communication can be calculated from the key used to decipher the translated textbook communication, on the negative.

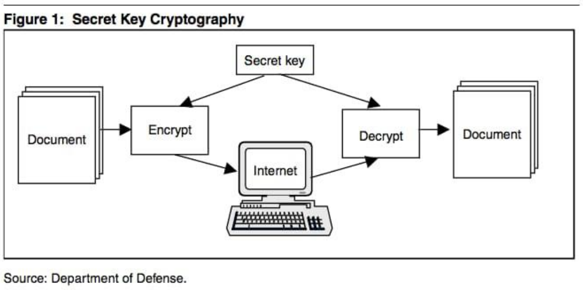
Figure 1: Secret Key Cryptography
Secret key
Document
Encrypt
Internet
Decrypt
Document
Source: Department of Defense.

FIGURE :2 SECRET KEY

1.2 HASH FUNCTIONS:

A cryptographic hash function (CHF) is a fine algorithm that displays ungraspable size data (generally appertained to as" communication") in a small fixed size list ("hash value","hash", or" communication alarm"). It's a one- way operation, that is, a function in which it's insolvable to reverse or reverse a computation. Immaculately, the only way to find a given hash communication is to try a important input hunt to see if it produces the same product, or to use a rainbow table of matching hashtags. Cryptographic hash functions are a introductory tool for ultramodern cryptography

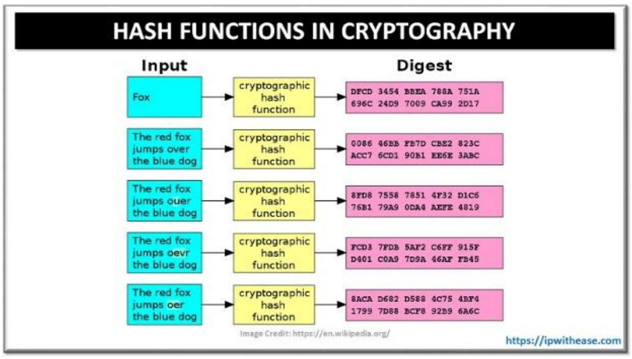
HASH FUNCTIONS IN CRYPTOGRAPHY
Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C
Image Credit: https://en.wikipedia.org/
https://ipwithease.com

FIGURE: 3HASH FUNCTIONS

People are saying that the biggest problem with social media is the way in which it's run. People says that it opens up a huge eventuality for cyber bullying, and that this can be seen in the same way as traditional attacks om people’s sequestration. Still, what numerous people don’t know about society is that at it’s core, social media has always been a tool for cybersecurity

Social media network have grown exponentially inrecent times. with the availability and visibility of these platforms, it’s no surprise that there has been asignificant increase in cybercrime, Still, this presents a big occasion for businesses to cover themselves and their data using cryptography The blog post takes you through the introductory of how to apply cryptography on your social media regard it covers simple tips on how to avoid common miscalculations utmost people make when setting up their own accounts, similar as not using strong word or participating private dispatches with unintended donors. From there, we go into more advanced settings similar as how to enable two factor authentication (2FA) .

2. END-TO-END ENDRYPTION :

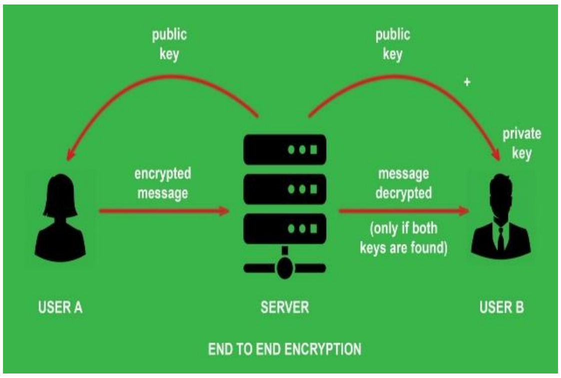

FIGURE:4:END TO END ENCRYPTION

End-to- end encryption (E2EE) is a system of communication where only the communicating druggies can read the dispatches. In principle, it prevents implicit eavesdroppers – including telecom providers, Internet providers, vicious state bodies, and indeed the provider of the communication service – from being suitable to pierce the cryptographic keys demanded to decipher the discussion.

End-to- end encryption is intended to help data being read or intimately modified, other than by the true sender and philanthropist (s). The dispatches are translated by the sender but the third party doesn't have a means to decipher them, and stores them translated. The donors recoup the translated data and decipher it themselves.

To guard your particular data

- Don't post your information on the internet. You may not suppose it's a big deal, but these websites are designed to get you to willingly hand out your information and preferences just by logging onto their spots. Then are some way you can take

- use private browsing mode when you 're doing your quests. This will keep you from in adverentely looking at the spots you 're hunt in through

- use a secure word to your account. You may have heard numerous times that watchwords are passkeys, but how frequently do we change them? To help identity theft, change it regularly with a minimum of three different watchwords per security operation and makesure that they're long and more also 8 characters in length. There are also online services that can induce arbitrary word for you

SOME OF THE ENCRYPTION SOFTWARE :

- AxCrypt decoration
- VeraCrypt
- Nordlocker
- Kruptos 2
- Boxcryptor

AXCRYPT

It provides AES-256 encryption for decoration subscribe

VeraCrypt

It uses AES, serpent, two fish, camelia and kuznyechik as ciphers

NORDLOCKER

Elliptic- wind cryptography (ECC)

Kruptos 2

Elliptic- wind cryptography (ECC)

Boxcryptor

Asymmetric RSA and symmetric AES encryption

CONCLUSION:

The standard encryption is availablemethods have been studied and analysed. It is the same againanalyses that all strategies are important in real timecrucifixion. We have also learned the current encryptiondone on social media and phones and an urgent needencryption in the online social world. Alwaysthe new code encoding system is also developingthat is why conformist enciphering tools will always be permanentexercise at a fast and high level of safety.

REFERENCES:

1.Study on cryptography and techniques Shivani Sharma, Yash Gupta,249-252,2017
https://www.academia.edu/download/53207529/CSEIT172150.pdf
2.End-to-end encryption in messaging services and national security—case of WhatsApp messenger
Robert E Endeley
Journal of Information Security 9 (01), 95, 2018
https://www.scirp.org/html/8-7800491_81897.htm
3.Cryptography: an introduction to computer security
Jennifer Seberry, Josef Pieprzyk
Prentice-Hall, Inc., 1989
https://dl.acm.org/doi/abs/10.5555/69375
4.An overview of cryptography
Gary C Kessler
Gary C. Kessler, 2003
https://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pd
5.Introduction to modern cryptography
Jonathan Katz, Yehuda Lindell
CRC press, 2020
https://books.google.co.in/books?hl=en&lr=&id=RsoOEAAAQBAJ&oi=fnd&pg=PT12&dq=cryptography&ots=vJ9fY4zCKp&sig=7Xm9v1z5GyoDaGDbrPAWUjM-YD4