A LITERATURE REVIEW ON THE CONCEPT OF CRYPTOGRAPHY AND RSA ALGORITHM

Vipin Kumar Gupta
Guru Nanak College of Arts, Science and Commerce
2 PUBLICATIONS **0** CITATIONS

ISSN 2394 - 7780

A LITERATURE REVIEW ON THE CONCEPT OF CRYPTOGRAPHY AND RSA ALGORITHM

[1]Prof. Suman Upadhyay and [2]Prof. Vipinkumar Gupta
[1]S. M. Shetty College of Science, Commerce & Management Studies, Powai
[2]Guru Nanak College of Arts, Science and Commerce, Mumbai 400037

ABSTRACT

In the digital era, being hacked is a common happening worldwide. With communications over the cloud, the privacy of data sent and received, is vulnerable. Cryptography is being a protector by safeguarding the data communicated. In today's world where everything is possible to get hacked or being tempered while communicating between sender and receiver, in such situation we do want anyone else to access our data or private messages. With digital currencies a.k.a. cryptocurrencies on the rise, it is of utmost priority to build a stronger anti-hack mechanism to protect them. The block-chain, that protects the digital currencies, is fundamentally based on cryptography. This research paper will review cryptography, its types and how RSA algorithm works.

Keyword: *Cryptography, Sender Receiver, Encryption, Decryption, cipher, key, blockchain*

OBJECTIVE

To understand the concept and techniques of cryptography used in communication, transactions and data transfer.

LITERATURE REVIEW

What is cryptography, where in concept of cryptography are been used, how cryptography works and which all algorithm are used in securing the private messages and working of RSA algorithm.

INTRODUCTION

Cryptography is a process of developing various techniques and protocols to prevent anyone from accessing and acquiring knowledge of the data from the private message during a communication process. Cryptography is important because it allows you to protect securely data that one doesn't want anyone else to have access to, it is used to protect secrets of the corporate world, secure classified information and to safeguard personal information against things like identity theft. It is derived from Greek word Kryptos which means hidden and Graphein means to write.

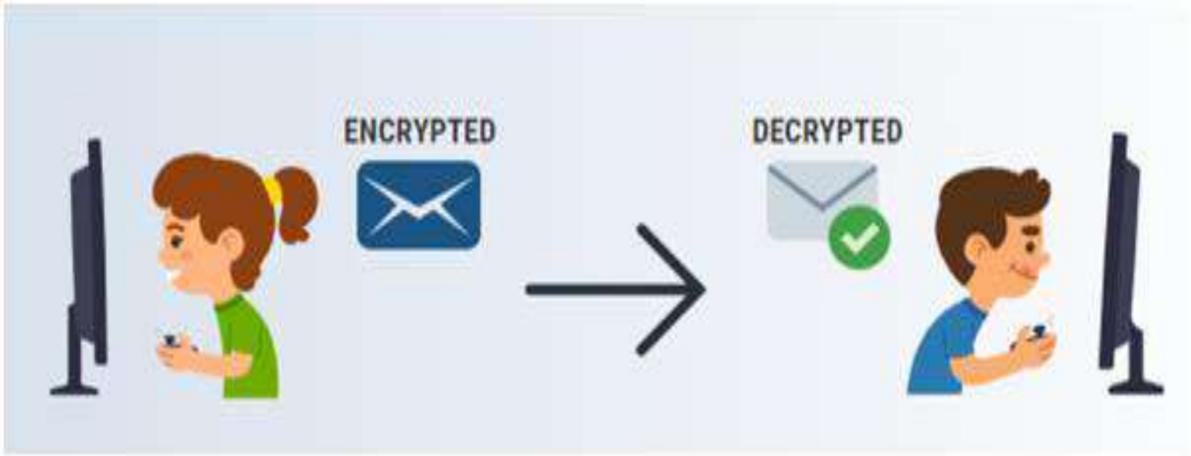


Figure 1: Cryptography

To start with cryptography, we need to know following terminology:

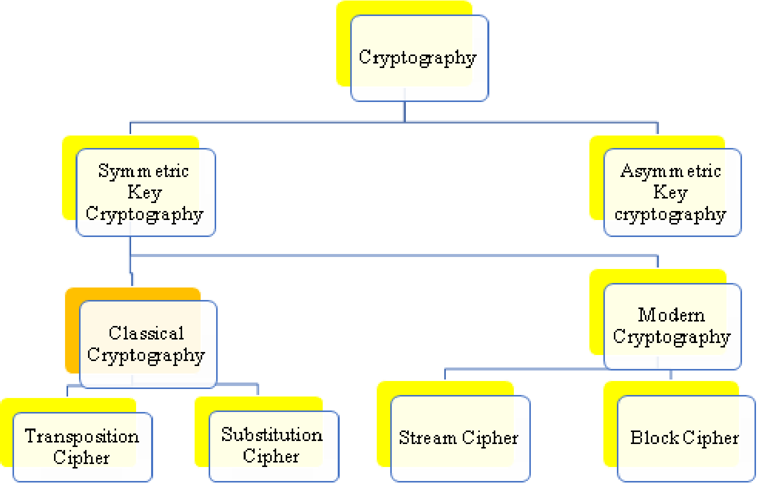
Encryption: A process of plain text (normal text) to a cipher/coded text (random sequence of bits)

Decryption: Inverse process of encryption, conversion of to a cipher/coded text to plain or decoded text

Cipher: The mathematical function, i.e. a cryptographic algorithm which is used to convert plain text to cipher text

Key: Information that is required to induce the output of the cryptographic algorithm

Classification of Cryptography



Symmetric Key Cryptography

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The most popular symmetric key system is the Data Encryption Standards (DES). The symmetry key cryptography is primarily used in banking applications where personally identifiable information needs to be encrypted. Symmetry cryptography helps in detecting bank fraud and boosts the security index of these payment gateways in general. They are also helpful in protecting data that is not in transit and dress on servers and data centres, these centres house a massive amount of data that needs to be encrypted with a fast and efficient algorithm so that when the data needs to recalled by the respective service, there is assurance of minor to no delay. While browsing the internet we need symmetry encryption to browse secure https websites so that we get all around protection. It plays a significance role in server authenticity, verifying website, exchange of necessary encryption keys required and generating a session using those keys to ensure highest level of security. This helps in preventing the rather insecure https website format.

Symmetry key cryptography uses a single key for both encryption and decryption of information. The key needs to be kept secretly and be available with both sender and receiver. Strength of encryption depends on the key size being used.

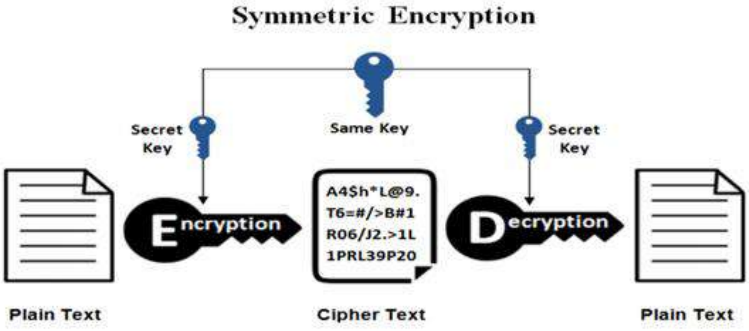


Figure 2: Symmetric Cryptography

Asymmetric Key cryptography: Two different keys are used in Asymmetric Encryption. Private key is used for encrypting the information and public key is used for decrypting the same.

Asymmetric encryption uses a double layer of protection. There are two different keys in play here, a private key and a public key. A public key is used to encrypt the information before transmission and the private key is used to decrypt the data post transmission. This pair of keys must belong to the receiver of the message. The public key can be shared via messaging, blog posts, key servers and there are no restrictions for it as one can see this image below two keys are working in the system. The sender first encrypts the plain text using the receiver's private key after which we received the cipher text, the cipher text is then transmitted to the receiver without any other key. On getting the ciphertext, the receiver uses his/her private key to decrypt the ciphertext and get the plaintext back. There has been no requirement of any key exchange throughout this process. Therefore, solving the most glaring flaw faced in symmetric key cryptography. The public key is known to everyone and cannot be used to decrypt messages and the private key which is known to everyone cannot decrypt messages. It doesn't need to be shared with anyone. The sender and the receiver can exchange personal data using the same set of keys for as often as possible.

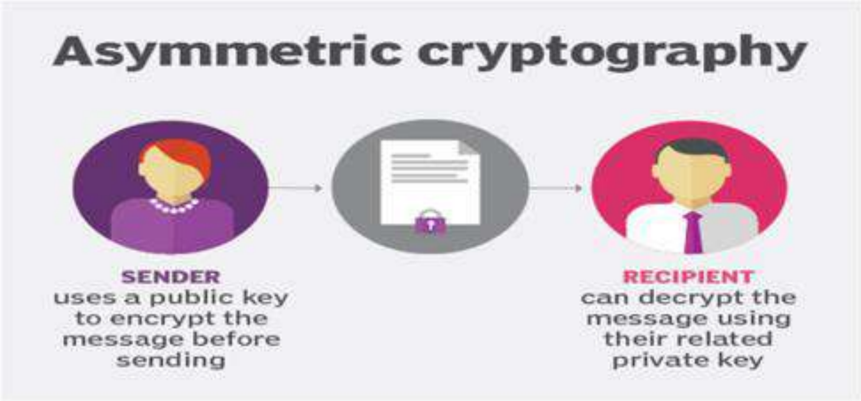

Asymmetric cryptography
SENDER
uses a public key to encrypt the message before sending
RECIPIENT
can decrypt the message using their related private key

Figure 3: Asymmetric Cryptography

RSA Encryption Algorithm\ Rivest-Shamir-Adleman Algorithm

Digital signatures have become part and parcel of the everyday correspondence in the corporate sector. The pandemic has further accelerated the need for digital wears to become mainstream in the business world. While DSL (Data Standard) Algorithm which is exclusively used for verification and transmission of signatures, the RSA algorithm can also be used for general data encryption and decryption as well. Functioning on similar public key cryptography architecture. It is seen as a more complex solution to bolster security.

The RSA algorithm is a public key signature algorithm developed and named after the developers Ron Rivest, Adi Shamir and Leonard Adleman. Their paper was first published in 1977 and the algorithm uses logarithmic functions to keep the working complicated enough to withstand brute force and streamlined to be fast post deployment.

The figure below shows the process of verifying signatures using RSA

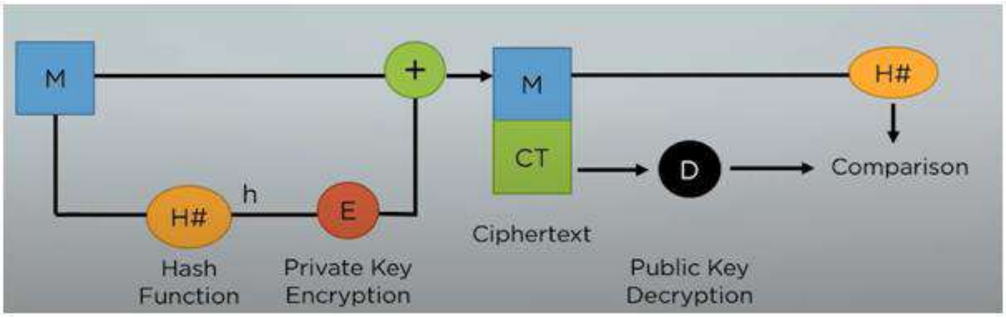


Figure 4: Process of Verifying signatures using RSA algorithm

The main case of RSA is encryption and decryption of private information before being transmitted across communication channel. This is where the data encryption come into play. When using RSA for encryption and decryption of general data. It reverses the key set usage unlike signature verification, it receives the receiver's public key to encrypt the data and uses the receiver's private key in decrypting the data. Thus, there is no need to exchange any key in this scenario. There are two broad components when it comes to RSA cryptography, one of them is key generation. Key generation employs a step of generating the private and the public key that are going to be used for encrypting and decrypting the data. The second part is encryption and decryption functions. These are ciphers and steps that need to be run when scrambling the data or recovering the data from the ciphertext.

Process for generating keys and encrypting and decrypting the information

1. Two large prime numbers are chosen (p and q)
2. Compute $n = p * q$ and $z = (p - 1) * (q - 1)$
3. Choose a number e where $1 < e < z$
4. A number d is selected so that ed mod z $= 1$ and calculated as d=$d = e^{-1} \, mod \, z$
5. Public key is (n, e) and the private key is (n, d)←---- Key Generated

6. If the plain text is m, encrypted ciphertext c is calculated as $c = m^e \ mod\ n$
7. Under similar assumptions, the plaintext can be calculated as $m = c^d \ mod\ n$

Example to make it more understandable

1. Choose p and q as 7 and 13 respectively, so that $\mathrm{n = p * q = 91}$
2. We can select value of e to be 5 since it satisfies $1 < e < (p-1)(q-1)$
3. Value of d can be calculated as

$$ed\ mod\ (p-1)(q-1) = 1$$

$$5d\ mod\ 72\ \ = 1$$

$$\Rightarrow d = 29$$

4. Public key is $(\mathrm{n,e}) = (91, 5)$ and Private key $= (\mathrm{n,d}) = (91, 29)$
5. Let plain text be m be 10 then

   Ciphertext $\mathrm{c = m^e\ mod\ n} = 10^5\ mod\ 91 = 82$

   Plaintext $m = c^d\ mod\ n = 82^{29}\ mod\ 91 = 10$

Advantages of RSA algorithm

- RSA algorithm depends upon receiver's public key so that one don't have to share any secret key to receive the messages from others. This was the most glaring flaw faced by symmetric algorithms which were eventually fixed by asymmetric cryptography structure
- Since the key pairs are related to each other, a receiver cannot intercept the message, since they didn't have private keys to decrypt the information. If public key can decrypt the information, the sender cannot refuse signing it with his private key. Without admitting the private key is not in fact private anymore.
- The encryption process is faster than the DSA algorithm
- Data will be temper proof in transit since meddling with data will alter the usages of the keys, the private key won't be able to decrypt the information. Hence alerting the receiver of any kind of manipulation in between the receiver must be aware of any third party who possesses the private key. Since they can alter the data in mid transit, the cases of which rather are low.

CONCLUSION

The key generation is slower in RSA. Many systems across the world tend to reuse the same keys so that they can spend less time in key generation and more time on actual ciphertext management.

REFERENCES

- Abdalbasit Mohammed Qadir and Nurhayat Varol, A Review Paper on Cryptography, https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography, 23 october 2019
- Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi, Research on Various Cryptography Techniques, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019
- https://www.youtube.com/watch?v=vf1z7GlG6Qo
- https://www.youtube.com/watch?v=5jpgMXt1Z9Y&t=843s