Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Product key activation for software products using Collatz Conjuncture and asymmetric key cryptography

K.R. Raghunandan [a], Lokesh Gagnani [b], K. Amarendra [c], B.V. Santhosh Krishna [d]

[a] *Dept of CSE, N.M.A.M Institute of Technology, Nitte, Affiliated to VTU, Karkala, Karnataka, India*
[b] *IT Dept, SVBIT, Gandhinagar, India*
[c] *Dept of CS&IT, K L University, Vijayawada, India*
[d] *Department of ECE, New Horizon College of Engineering, Bengaluru, Karnataka, India*

ARTICLE INFO

Article history:
Received 21 October 2020
Accepted 27 October 2020
Available online xxxx

Keywords:
Asymmetric cryptography
MAC address
Product key
Serial key
Collatz Conjuncture

ABSTRACT

Nowadays, almost all software products are sold online. But there is a danger of unauthorized users using the product. For this reason, every company employs a product activation system where only authorized users that have a unique key called the product key can use the application. But attackers always find a way to get past the authorization. For example, they use a key generator that generates a random key that matches the format of the product key and can be used to activate the product. Therefore, to avoid this, we need improved product activation programs that can safeguard the product from unauthorized users. This paper proposes an improved key verification system to make sure that the product can be used on one system only. Every system has a unique MAC address, and that's what we use as the foundation for our method. The main contribution of this work is the effective use of a system's MAC address, which in turn boosts the security of the project. The necessary procedure consists of retrieving a MAC address from the user's system. Now, a serial key is derived by performing specific operations on the MAC address, which is then converted into a more straightforward, user-friendly product key while encryption and decryption take place during the transmission of keys between client and server. Looking ahead, this work can lead to better and consistent use of MAC addresses in key generation techniques, which is something that hasn't been explored enough.

Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

1. Introduction

Product key Activation is a verification strategy required by some software to make sure that the product is being redeemed by its rightful owner. Key verification restricts the free distribution of duplicated or reproduced software. Un-activated software cannot be used by a customer until the product key specified by the client is verified and validated by the product setup. Activation permits the software to unlock and allow complete utilization of all its tools and functionalities. Activation can keep going on forever, or it can have a time limit, requiring renewal or re-activation for proceeding with the use [32] Figs. 1-3.

Typically, the software distributor sends the client a unique serial number. At the point, when the client installs the product, it requests the client to get a few more add-ons that the application demands. The application acquires permissions that apply to that client's permit, and a failure to do so might result in a lockdown of the software, rendering it useless. Some activation systems also make use of communication and verification of a key over the internet. The drawback of this method is that attackers might use a key generator to illegally acquire a product key, which they can then use to activate the product. To combat this, sometimes, the software might also take the user's location as a factor for authorizing the user [33]; this adds another level of authorization to the product activation.

There are also some methods where the hardware of the system is used as the chip to chip authentication systems for integrated circuits [3]. There are also licensing software whose primary function is authorizing systems to use particular software and to create an agreement between the developer and end-user. It also specifies that the product must be obtained lawfully. It stores hardware information in a server, and the server also acts as a key verifica-

E-mail address: raghunandan@nitte.edu.in (K.R. Raghunandan)

https://doi.org/10.1016/j.matpr.2020.10.907
2214-7853/© 2020 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

tion station [4]. Using hardware as an authenticator is very beneficial since it will be difficult for attackers to replicate hardware components. The proposed method uses the MAC address to achieve the same level of security.

The problem of illegal product key distribution has caused the rates of piracy to exponentially increase, which is why it has become imperative to tackle this problem. The main objective of this work is to make sure that the product activation key is authentic and exclusive to the user and a particular system, this is done to ensure that the possibility of redistribution or sharing of a product key is eliminated. Asymmetric cryptography techniques are applied to ensure those above by retrieving the MAC address of the system using which the product has been bought [5], performing specific mathematical operations on it, and then encrypting it so that the key can be activated only on one system. The idea is to convert MAC address into a serial key on the client-side, which is then encrypted, sent to the server-side where it is decrypted using a private key. This serial key is then converted to the product key, which is sent to the rightful client using the email ID specified at the time during which the product was bought.

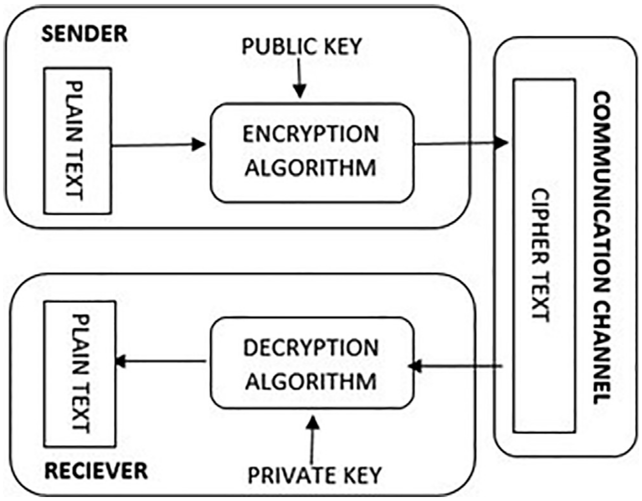


Fig 1. Asymetric Key Cryptography.

1.1. MAC address

It is a unique identifier allotted to a network interface controller (NIC), which allows its use as a physical address during communications inside a network. This utilization is standard in most IEEE 802 networking advancements, including Ethernet, Bluetooth, and Wi-Fi. As usually represented, MAC addresses consist of six groups of two hexadecimal digits without a separator or isolated by hyphens, colons. MAC addresses are allocated by the distributors and generally can be referred to as a physical address [3].

1.2. Cryptography

Implementing cryptography concepts is essential. Since it is not desirable to let attackers gain access to the product keys, different types of cryptography techniques must be employed.

Using public-key cryptography is beneficial because it is very secure since there are two separate keys compared to private-key cryptography, which implements only one key, which makes it very unreliable. Since the private key requires only one key, it means that the receiver of the message must also have the key, and therefore, the key is transmitted over unreliable channels. Attackers might obtain the private key and access the product key that is being sent to the user. Using public-key cryptography helps deliver the product key to the user safely and also makes sure that attackers do not get product keys without authorization because there is no need to transmit the private key anywhere which means the attackers will not be able to decrypt the messages easily which makes this method more secure.

Another advantage of public-key cryptography is that multiple users will be able to use the program and do so safely since the public key can be used by anyone to encrypt data, but only the owner of the public key can decrypt the data. With private cryptography, the private key must be sent to every user using the program, which makes it very unsafe. Thus, public-key cryptography

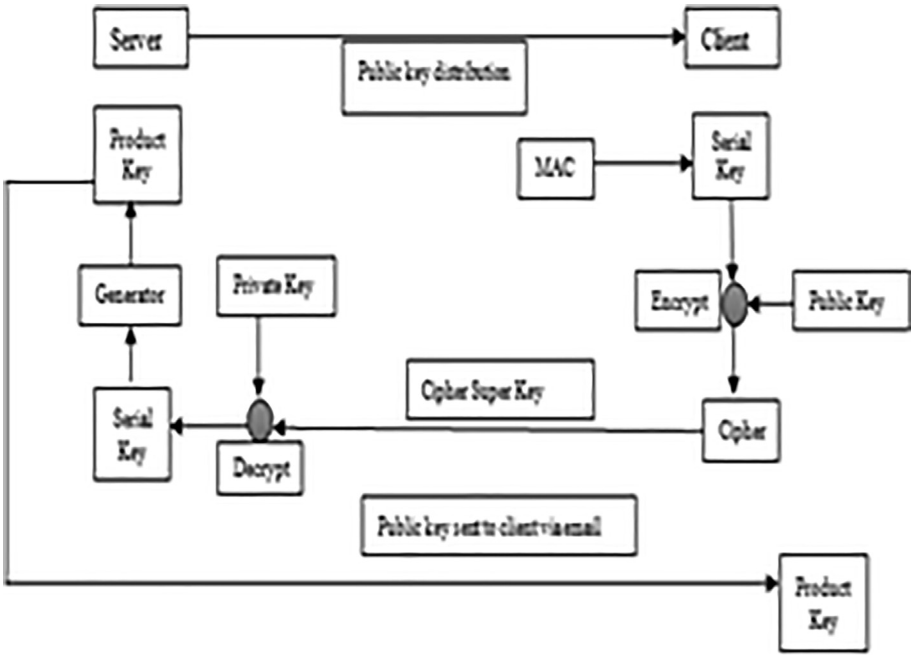


Fig 2. Proposed Methodology.

is preferred over private key cryptography. Cryptography and its importance to this paper and RSA and its advantages are explained in depth in the next section.

2. Literature survey

2.1. History of cryptography

This section provides various literature that includes essential information for this paper. The topics covered in this survey include Cryptography, Public-key cryptography and its advantages, RSA cryptosystems, product key activation, and Collatz Conjuncture. Here various literature that states the significance and importance of cryptography is discussed. Edge C. et al. [6] word cryptography is derived from the Greek words Kryptos, meaning hidden and grafein meaning to write. Mohammed Abdalbasit et al. [7] states that Cryptography is a method to accomplish the privacy of messages. The term has a particular meaning in Greek: "secret writing." These days, in any case, the protection of privacy of people and associations is achieved through cryptography at a significant level, ensuring that data sent is secure such that the approved receiver can access this data.

Saurabh Sharma et al. [8] states the innovations that took place in the field of cryptography. Public key cryptography was such an innovation that took place. It solved many security issues, but also, it didn't bring a solution to the key management problem. Swapnil Chaudhary [9] states a new form of the cryptographic algorithm named as the new hybrid cryptographic algorithm. Private key cryptography and its disadvantages are discussed.

Yan S.Y [10] states that private key cryptography is a type of cryptography that came into working 5000 years ago; it is a version of cryptography that utilizes common key for both encryptions of message and decryption of the message within the sender and receiver. Lee G.T [11] discusses the various limitations of private key cryptography, such as the compromise in security and authenticity. Diverse literature that provides information about public-key cryptography and why it is superior to private key cryptography is discussed here.

Delfs Hans et al. [12] proposed that public-key cryptography is a form of encryption where message sender and receiver utilize two separate keys to encrypt and decrypt messages. The secret key is not exchanged between the contact partners in public-key encryption. Goeffroy [12] states that every user owns two keys, which are a public key that everyone has and a secret key, which only the

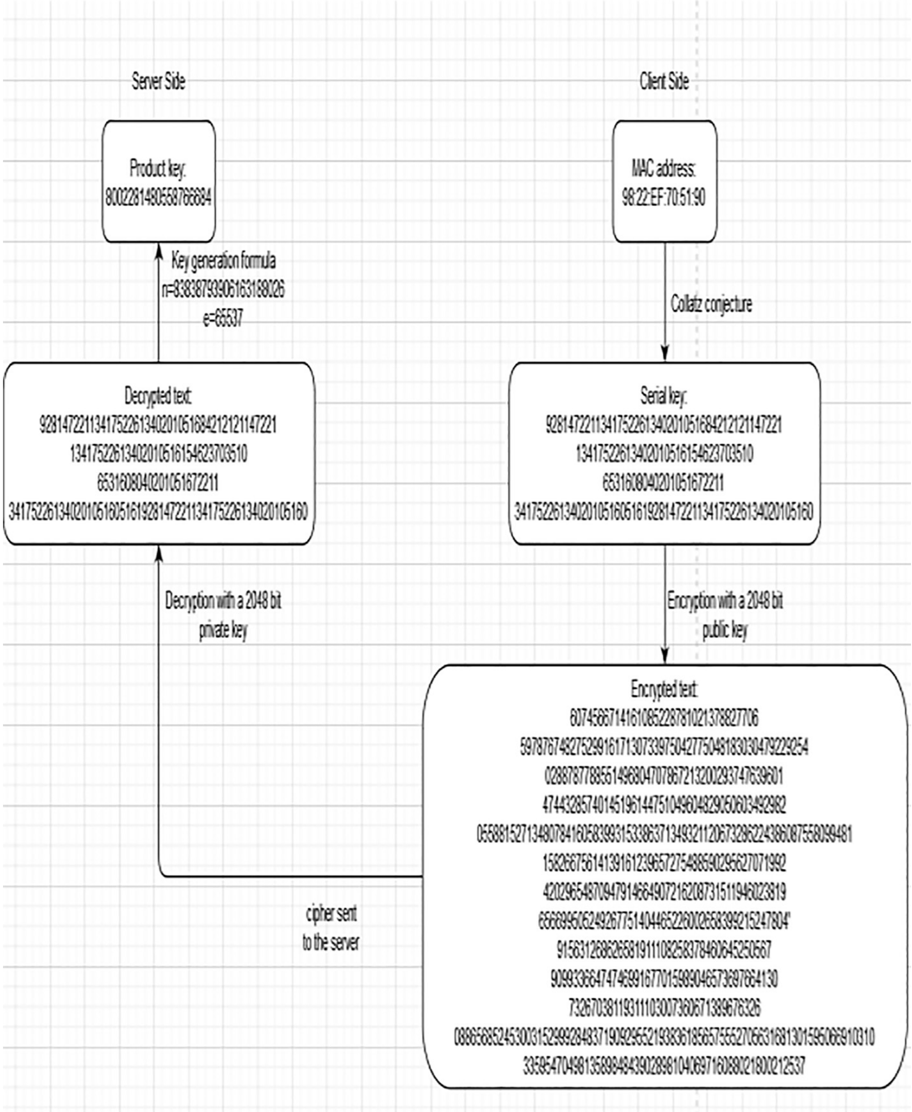


Fig. 3. Output produced in a particular system.

specified user has. Public key cryptography is much more secure and safe than others. Sako M et al. [13] discuss the factor used to represent the security of public-key cryptosystem & states that the protection provided by public-key cryptography is much higher than the security provided by the private key cryptography. Boyd Colin et al. [14] proposes the utilization of the public key cryptography in authentication and key transport advantages carried by the public key cryptography systems.

K.Shim [15] surveys the use of public-key cryptosystem in the Wireless Sensor Networks (WSN's). This paper discusses the performance of public-key cryptographic primitives in terms of the time of execution, the consumption of energy, and resource allocation. M. Malik et al. [16] focuses on the key bootstrapping protocols in the Internet of Things, focused on public-key cryptography. This paper discusses the use of public-key cryptography and the secure transmission of messages between devices, mobiles. Anagha.S et al. [17] provide a comparative analysis of the RSA algorithm and AES algorithm for the encryption of the image and hiding of the images which can be reversed.

In both instances, data embedding is achieved by the process of histogram shift. The RSA cryptosystem can be utilized to encrypt images and gives greater security; still, it takes longer. In contrast, the image security in the AES algorithm is relatively weak, but it takes only a limited amount of time. RSA is a revolutionary method of encryption. Its uses and its advantages are discussed here.

In Paper author [18] states the RSA cryptosystem consists mainly of two parts, namely the key generation and encryption. The RSA cryptosystem is set up by first multiplying two prime numbers, which have a high value and then the product, which is termed as n is made public. Product n acts as a public key part, and factors of the product n kept hidden & then utilized as a secret key. Main logic because of which this algorithm works is that, from the product, nth factors of product n can't be retrieved. The level of difficulty of factoring defines the level of security in RSA. Author at [19] also states the importance of RSA in cryptography studies and also discusses the contribution of the RSA algorithm in further studies of cryptography. Nicholas Tuzzio et al. [20] states the RSA algorithm has two different parts. The Key generation step creates two different pairs of keys; one is a public key; the other is a private key. The key generation consists of three stages. High value distinct prime numbers p & q are chosen randomly; thus, calculaten = p*q. Then integer is selected, 1 < e < φ(n), which is prime to φ(n). After this (n,e) is published as the public key. Then d is computed using ed≡1 mod φ (n). (n,d) which is the secret key. Yan S.Y [21] discusses all the detailed computations and mathematical preliminaries in this paper.

The encryption of the messages is done by the public key, which is generated, and the decryption is done by the secret key generated after the process of key generation. The value of Product n is used for encryption. Raghunandan et.al. proposed numerous RSA variants using the concept of Pell's equation. A novel public key cryptography technique which uses the quadratic case of Pell's equation for key generation is proposed[22]. The idea of fake modulus to resolve the limitations of the integer factorization attack is introduced in paper[23]. Dual RSA approach using Pell's equation to hide public key component is introduced in paper[24] which provides extra level of security during encryption. In paper [25] use of Pell's cubic equation for securing media information using Fisher yates algorithm is introduced. Key generation using cubic power of Pell's equation is proposed in paper[26] which is used for text encryption. Literature that provides an insight into product key activation is discussed here.

In [33], it is specified that after the user purchases the product, a request to activate the product is sent to the server. Then the server sends the respective product key to the user, and depending on the eligibility of the user, the server may send more than one offer. To check the eligibility of the user, the server works with various components of the user's system to determine it. DervisAvdic [4] proposes a 3-step process for licensing software. The first step is the generation of the license code by the back office. The second step is gathering information about the user's hardware components. The third step is verification to see if the hardware that is detected is using the product with a valid license.

Jangwoo Shin et al. [5] proposes a method for the distribution of license keys using asymmetric cryptography. In this paper, the author describes a process of distribution wherein an encryption key is embedded along with the software product so that when the user's system issues a request for a license key only that particular user can decrypt the key when he/she receives the key and activate the product. In [27] it is specified that the security information includes a first portion to be processed by a primary validation authority using first validation information and a second portion to be processed by a second validation authority using second validation information, wherein the second validation information is stored separately from the first validation information. Collatz Conjuncture and its uses are specified in this section.

The paper [28] explains the Collatz Conjuncture. The origin and the formalization of the Collatz problem and the properties of the Collatz function are mentioned in this paper. In the paper, the authors give an "efficient" algorithm for computing the number of iterations (recursive calls) of the Collatz function. In [29], the authors propose a method of image encryption by implementing the Collatz Conjuncture. In this proposed method, the authors used the Collatz Conjuncture to convert images into non-intelligible audio. By applying the Collatz Conjuncture in image encryption, the authors were able to get completely different sounds every time they encrypted an image.

3. Mathematical preliminaries

The algorithm uses various mathematical formulas to increase the level of security. The following are implemented in the proposed method Collatz Conjuncture, RSA, and a variation of RSA, which is used in the product key generator.

3.1. Collatz Conjuncture

It is a procedure of conjecture that works as follows: begin with any positive number n. At that point, each term is retrieved as follows from the previous term: if the last term is even, the next term is one half of the previous term. If the previous term is odd, then the following term is three times the previous term plus 1. The assumption is that, regardless of the estimation of n, the sequence will consistently arrive at 1[27]. This method is used to generate a unique serial key.

If × is a unit of MAC address

If × is odd then:

$$n = 3x + 1$$

Here × is unit of MAC address, and n is the value after the Collatz Conjuncture.

If × is even then:

$$n = x/2 \tag{1}$$

3.2. RSA encryption and decryption

1. Choose two distinct, high value random prime numbers *p* and *q*
2. Calculate $n = pq$

- *n* is the modulus for the public key and private keys

3. Calculate the totient: $\hat{a} \pm \cdot (n) = (p-1)(q-1)$(Euclid's Algorithm)[25]
4. Choose an integer such that $1 < e < \hat{a} \pm \cdot (n)$, and e is co-prime to $\hat{a} \pm \cdot (n)$i.e.: e and $\hat{a} \pm \cdot (n)$share no factors other than 1; $gcd(e, \hat{a} \pm \cdot (n)) = 1$

- e is released as the public key exponent

5. Calculate d to fulfill the given relation$d \equiv 1(mod\hat{a} \pm \cdot (n))$also known as Fermat's theorum[26],i.e.*:*

   $de = 1 + x\hat{a} \pm \cdot (n)$for some integer x.

- d is kept as the private key exponent

After following the above steps, the message can be encrypted and decrypted.

3.2.1. Encryption

$$F(m, e) = m^e modn = c \tag{2}$$

Here the message is m, e is the public key and c is the cipher

3.2.2. Decryption

$$F(c, d) = c^d modn = m \tag{3}$$

3.3. To generate product key

Step 1: Decrypt the encrypted text and obtain the serial key.

Step 2: Take the serial key as plain text/message and apply the following formula on it.

$$F(m, e) = m^e modn = c \tag{4}$$

Here the message is m (serial key), e is the public key and c is the cipher

In this, a very small n value is used; this gives the ability to control the size of the product key. In the proposed method, a 10-digit n value is used, which means that the product key is always ten digits or lower.

Step 3: After the product key is generated is sent to the client/user.

3.4. Research methods

In this section, the method of product key generation in the proposed method is discussed and how it is implemented. The following diagram depicts the various stages of the program. The purpose of this algorithm is to generate a product key that is unique to every user and acts as an extra layer of security for the content of the product.

The product key is generated after being subjected to 6 stages of operations and constant manipulation of the MAC address. This product is only unlocked after it is entered by the user, and it matches the product key generated. During the process of creating a product key, it is passed from the client to the server-side, which might provide a window of opportunity to an external user who wishes to intercept the information illegally. To stop this from happening, the serial key, when being passed to the server-side from the client-side, is encrypted before being moved using the RSA algorithm.

STEP 1: Converting MAC address to Serial Key

First, the MAC address of the user's system is retrieved by the program, which is then converted to a serial key using an algorithm called the Collatz Conjuncture. Then, every bit of MAC address is applied to Collatz Conjuncture to produce a serial key (using the formulas specified in the equations section).

Consider an example where: -The MAC address retrieved is 98:22:ef:70:51:90. The serial key generated using Collatz Conjuncture(eq. (1)) is:

928147221134175226134020105168421212114722113417 52261340201051615462370351065316080402010516722113417 522613402010516051619281472 21134175226134020105160.

STEP 2: Encrypting the Serial Key

RSA algorithm is an asymmetric cryptography algorithm used to send messages securely. Once the serial key is generated (Using Collatz Conjuncture), we make use of the RSA's encryption formula (Eq (2)) to encrypt it utilizing the server's public key. The public key is known to everyone and is used to encrypt the messages. The messages encrypted by the public key can be decrypted only with the appropriate (server's) private key.

Example: - The encrypted serial key

6,074,566,714,161,085,228,781,021,378,827,706,597, 876,748,275,299,161,713,073,397,504,277,504,818,303,047,922,925,402,887,877,885,514,968,047,078,672,132, 002,937,476,396,014,744,328,574,014,519,614,475,104,960,482,905,060,349, 298,205,588,152,713,480,784,160,583,993,153,386,371,349,321,120,673, 286,224,386,087,558,099,481,158,266,756,141,391,612,396,572,754,885,902,956,270,719,924,202,965,487,094, 791,466,490,721,620,873,151,194,602,381,965,669,950,524,926

775,140,446,522, 600,265,839,921,524,780,491,563,126,862,658,191,110, 825,837,846,064,525, 056,790,993,366,474,746,991,677, 015,989,046,573, 697,664,130,732,670, 381,193,111,030,073,606,713,896,763,260,886,568, 524,530,031,529,992,848,371,909,295,521,938,361,856,575,552,705,631,681,301,595,066,910,310,335,954,704,981,358,984,843,902,898,104,069,716, 088,021,800,212,537

STEP 3: Decrypting the Serial Key

After the server has received the encrypted serial key, it is then decrypted by using RSA's decryption formula (Eq. (3)), i.e., the server's private key is used. The serial key obtained has to be then converted into the product key.

Example:-Decrypted text integer: 9,281,472,211,341,752,261,340,201,051,684,212,121, 147,221,134,175,226,134, 020,105,161,546,237,035,106,531,608,040,201,051,672,211,341,752,261, 340,201,051,605,161,928,147,221,134,175,226,134,020,105,160

STEP 4: Serial Key to Product Key Conversion

The serial key is converted into the product key by making use of RSA's encryption formula. During the conversion process, the cipher text (serial key) received by the server is in-fact considered as the plain text (message) in the formula 5.

Example: -Product key generated is: 8,002,281,480,558,766,684

The only difference being, the value of 'n' used in the formula is significantly smaller than the value of 'n' used during the encryption process. It is done to reduce the size of the generated product key, which also makes it a lot more user friendly.

STEP 5: Generated product key is sent to the client via email

The product key generated is sent to the client using the email ID provided by them during the time of the transaction.

STEP 6: Verification of Product Key received by the client

After the product key is received by the client, they enter it into the website. The authenticity of the entered product key is checked by the backend of the website, making sure that the product key is new and unique for each user. That is, making sure the product is being redeemed by the same system on which it was initially bought by checking the target system's MAC address.

4. Results and discussion

The results generated by using the proposed methodology are as follows: -

We implemented the program using python IDLE and tested the application using various MAC addresses. To show the variation of the product keys and to show the avalanche effect, we gave the program MAC addresses that differed only by 1 bit. The graph provided in the next section shows the avalanche effect.

4.1. Client side

The results generated by using the proposed methodology are as follows: -

User Interface

Fig. 4 shows the home page of the user interface in which the client has to add three fields which are Name, Payment id and Email Address. Once the client enters these details and clicks on the enter button, the product is sent to the given email address by the server side. Fig. 5 shows the product key sent by the server to the client via email. the page which is displayed after the email has been sent by the server side. This page is provided to enter the product key by the user and then when the user presses enter it is verified whether the product key entered by the user matches with the original product key. Output displays “Product activated” if the product key matches or else results with “Invalid product key” if the product key doesn’t match Fig. 6.

4.2. Avalanche effect

Avalanche effect is one of the required properties of the encryption algorithm. Avalanche effect is a concept associated with modifying a bit in a public key how the graph charts successful changes in the cipher text against the original public key[31,32]

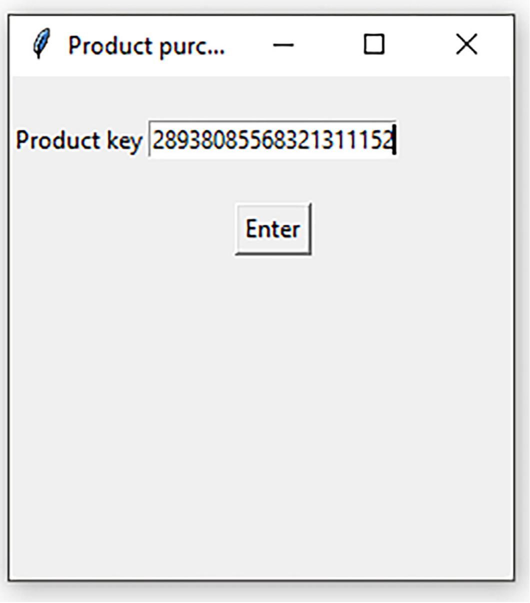
In the above graph, the data is as follows:

Original MAC: 98:22:ef:70:51:90

product key:80022814805558766684

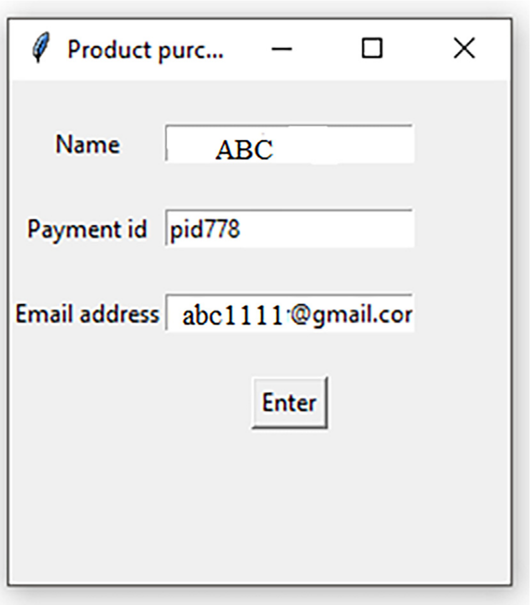
These are the product keys generated after changing each bit in the mac address:

Bit changed(right to left): product Key:



Product key 28938085568321311152

Fig. 4. home page of the user interface.



Name ABC

Payment id pid778

Email address abc1111@gmail.cor

Fig. 5. the product key sent by the server to the client via email.

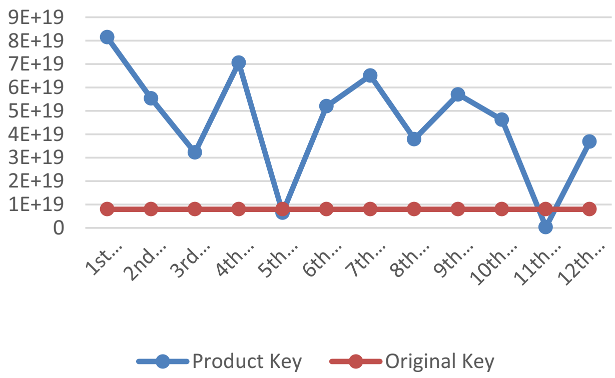


Fig. 6. Avalanche effect.

1st (98:22:ef:70:51:91) 81,468,231,738,262,776,011
2nd (98:22:ef:70:51:a0) 55,410,159,012,135,933,914
3rd (98:22:ef:70:52:90) 32,247,282,312,834,519,690
4th (98:22:ef:70:61:90) 70,613,806,947,959,177,858
5th (98:22:ef:71:51:90) 6,509,906,189,986,885,886
6th (98:22:ef:80:51:90) 51,982,026,067,146,377,020
7th (98:22:ee:70:51:90) 65,112,653,651,591,448,890
8th (98:22:ff:70:51:90) 37,965,365,883,336,520,728
9th (98:23:ef:70:51:90) 57,034,371,028,485,901,328
10th (98:32:ef:70:51:90) 46,217,223,073,107,650,546
11th (99:22:ef:70:51:90) 362,788,305,703,657,816
12th (a8:22:ef:70:51:90) 36,834,689,788,535,930,876

a bit is changed by just one digit

Eg: 1st bit changed

98:22:ef:70:51:90 -> 98:22:ef:70:51:91

The graph shows a comparison between the original product key and the modified product key. It represents the avalanche effect.

4.3. Sensitivity analysis of key

A very slight change of the MAC address automatically leads to a different product key when compared to the original. Hence the product keys generated are highly sensitive. The graph above shows the difference in product key when each digit of the MAC address is changed (One bit at a time) starting from the rightmost bit, this means that every time a bit of the MAC address is changed, the product key generated as a result of the new MAC address is significantly different from the product key generated from the original MAC address, this ensures that no patterns are developing.

5. Conclusion

The use of the RSA algorithm in the encryption and decryption process between the client and the server during the transmission of messages increases the security of the system. Adding different levels of encryption in the form of conversion of MAC Address to the serial key, then conversion of the serial key to product key makes it more difficult for the attacker to retrieve the message, thus making the system more secure. This project, because of its different levels of encryption, makes it more reliable in the transmission of the key from the client-side to the server-side. Another advantage of the project is that it uses the MAC Address of the client-side to form the serial key which is then converted into product key on the server-side; this use of MAC Address is an advantage because the MAC address is different for different systems thus improving the authenticity of the system.

CRediT authorship contribution statement

K.R. Raghunandan: Conceptualization, Methodology. **Lokesh Gagnani:** Software, Data curation, Writing - original draft. **K. Amarendra:** Visualization, Investigation, Supervision. **B.V. Santhosh Krishna:** Software, Validation, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[32] Dr. Mohammed Abbas Fadhil Al-Husainy “MAC Address as a Key for Data Encryption” International Journal of Computer Science and Information Security, 2013Department of multimedia systems, faculty of science and information technology, Al-Zaytoonah University of Jordan. Amman, Jordan

[33] Lanning, Van Stephen (Bellevue, WA, US) Mackey, Michelle C. (Kirkland, WA, US) Thoresen, Taj Lamon(Issaquah, WA, US)PRODUCT ACTIVATION/ REGISTRATION AND OFFERELIGIBILITY, MICROSOFT CORPORATION, Redmond, WA (US),2009

[3] Ioannis Karageorgos, Mehmet M. Isgenc1, Samuel Pagliarini, Larry PileggiChip-to-Chip Authentication Method Based on SRAM PUFand Public Key Cryptography Journal of hardware and software security,2019

[4] Dervis Avdic Department of Electrical and Information Technology Faculty of Engineering, Licensing Activation LTH, Lund University SE-221 00 Lund, Sweden,2016

[5] Jangwoo Shin et al. proposed “Systems and Methods for Software License distribution using Asymmetric Key Cryptography,” 812/8813122011

[6] C. Edge, D. O’Donnell, Introduction to Cryptography, Enterprise Mac Security, Apress, Berkeley, CA, 2016.

[7] Mohammed, Abdalbasit & Varol, Nurhayat. (2019).A Review Paper on Cryptography 1-6.10.1109/ISDFS.2019.8757514

[8] Sharma S., Mishra N.K. (2011) New Innovations in Cryptography and Its Applications. In: Mantri A., Nandi S., Kumar G., Kumar S. (eds) High-Performance Architecture and Grid Computing. HPAGC 2011. Communications in Computer and Information Science, vol 169. Springer, Berlin, Heidelberg

[9] Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryptography Algorithm.

[10] S.Y. Yan, Secret-Key Cryptography, Cyber cryptography: Applicable Cryptography for Cyberspace Security, Springer, Cham, 2019.

[11] G.T. Lee, Public Key Cryptography, Abstract Algebra. Springer Undergraduate Mathematics Series, Springer, Cham, 2018.

[12] H. Delfs, H. Knebl, Public-Key Cryptography, Introduction to Cryptography. Information Security and Cryptography, Springer, Berlin, Heidelberg, 2015, Year, 11442, 2019, Page 66.

[13] K. Sako, Public Key Cryptography, in: H.C.A. van Tilborg, S. Jajodia (Eds.), Encyclopedia of Cryptography and Security, Springer, Boston, MA, 2011.

[14] C. Boyd, A. Mathuria, D. Stebila, Authentication and Key Transport Using Public Key Cryptography, Protocols for Authentication and Key Establishment, Information Security and Cryptography. Springer, Berlin, Heidelberg, 2020.

[15] K. Shim, A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks, in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 577-601, First quarter, 2016.

[16] M. Malik, M. Dutta, J. Granjal, A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things, IEEE Access 7 (2019) 27443–27464.

[17] Anagha S., Sebastian N., Rosebell Paul K. (2019) A Comparative Study of Performance and Security Issues of Public Key Cryptography and Symmetric Key Cryptography in Reversible Data Hiding. In: Abraham A., Gandhi N., Pant M. (eds) Innovations in Bio-Inspired Computing and Applications. IBICA 2018. Advances in Intelligent Systems and Computing, vol 939. Springer, Cham

[18] K. R. Raghunandan, R. Shetty and G. Aithal, Key generation and security analysis of text cryptography using cubic power of Pell’s equation. In:2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, 2017,pp.1496-1500.

[19] Raghunandan KR, Aithal G, Shetty S (2019) Secure RSA variant system to avoid factorization attack using phony modules and phony public key exponent. Int J Innov Technol Exploring Eng (IJITEE) 8(9), ISSN: 2278-3075, July 2019

[20] N. Tuzzio, M. Tehranipoor, RSA: Implementation and Security, in: M. Tehranipoor, C. Wang (Eds.), Introduction to Hardware Security and Trust, Springer, New York, NY, 2012.

[21] S.Y. Yan, Computational/Mathematical Preliminaries, Cryptanalytic Attacks on RSA, Springer, Boston, MA, 2008.

[22] K.R. Raghunandan, Ganesh Aithal, Surendra Shetty, K. Bhavya, Image encryption scheme in public key cryptography based on cubic Pells quadratic case, Indonesian Journal of Electrical Engineering and Computer Science 20 (1) (2020) 385–394, https://doi.org/10.11591/ijeecs.v20.i1.pp385-394.

[23] K. R. Raghunandhan, S. Shetty, G. Aithal and N. Rakshith, Enhanced RSA Algorithm using Fake Modulus and Fake Public Key Exponent. In: 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Msyuru, India, 2018, pp. 755-759.

[24] R. K.R., G. Aithal and S. Shetty, “Comparative Analysis of Encryption and Decryption Techniques Using Mersenne Prime Numbers and Phony Modulus to Avoid Factorization Attack of RSA,” 2019 International Conference on Advanced Mechatronic Systems (ICAMechS), Kusatsu, Shiga, Japan, 2019, pp. 152-157.

[25] Raghunandan K.R., Dsouza R.R., Rakshith N., Shetty S., Aithal G. Analysis of an Enhanced Dual RSA Algorithm Using Pell’s Equation to Hide Public Key Exponent and a Fake Modulus to Avoid Factorization Attack, In: Chiplunkar N., Fukao T. (eds) Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing, Springer, Singapore. doi. org/10.1007/978-981-15-3514-7_60, vol 1133.

[26] Raghunandan K.R., Nireshwalya S.N., Sudhir S., Bhat M.S., Tanvi H.M. Securing Media Information Using Hybrid Transposition Using Fisher Yates Algorithm and RSA Public Key Algorithm Using Pell’s Cubic Equation, In: Chiplunkar N., Fukao T. (eds) Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing, Springer, Singapore. doi. org/10.1007/978-981-15-3514-7_73, vol 1133

[27] Thomas J Laysonet.al proposed the “Secure Software Product Identifier for Product Validation and Activation.”

[28] Ş. Andrei, C. Masalagiu, About the Collatz Conjuncture, Acta Informatica 35 (1998) 167–179, https://doi.org/10.1007/s002360050117.

[29] D.M. Ballesteros, J. Peña, D. Renza, A Novel Image Encryption Scheme Based on Collatz Conjuncture, Entropy 20 (2018) 901.

[30] K.R. Raghunandhan, D. Radhakrishna, K.B. Sudeepa, A. Ganesh, Efficient audio encryption algorithm for online applications using transposition and multiplicative non-binary system, Int J Eng Res Technol 2 (6) (2013) 472–477.

[31] Raghunandan Rao, Aithal Ganesh, Shetty Surendra, Bhavya Kallapu, Key Generation Using Generalized Pell’s Equation in Public Key Cryptography Based on the Prime Fake Modulus Principle to Image Encryption and Its Security Analysis, Cybernetics and Information Technologies. 20 (2020) 86–101, https://doi.org/10.2478/cait-2020-0030.

Further Reading

[32] On Euclid’s Algorithm and the Computation of Polynomial Greatest Common Divisors W.S.BROWN Bell Telephone Laboratories, Incorporated, Murray Hill, New Jersey.

[33] L. Childs, Fermat’s Theorem, II, A Concrete Introduction to Higher Algebra. Undergraduate Texts in Mathematics, Springer, New York, NY, 1979.