IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 5, June 2020

Cryptogram Builder

S Sravya Sri[1], Zahra Saktiwala[2], Deepti Rathore[3], Sapna Painkra[4]

B.E. Final Year Student, Computer Science and Engineering, Government Engineering College, Bilaspur[1-4]

Abstract: Nowadays, secrecy of personal information has become the utmost concerning factor in maintaining privacy over the internet and also protecting data from paranoid personas. As internet is gaining momentous command over market and also in the lives of trillions of individuals, threats to the shared data have tremendously increased. The necessity to secure such shared data has leaded us to the idea of developing a system that would provide such functionalities. Cryptogram builder is an android application which uses a collection of most popular cryptographic algorithms to generate encrypted messages and to decrypt the same on the receiver end. The word Cryptogram itself concludes the whole meaning of this very project. Cryptogram is a mystery word or code or puzzle that is a specific encrypted version of a text or data, whose formation is done using a certain cipher in order to maintain its secrecy from any malicious discrepancies of any kind of confidential message.

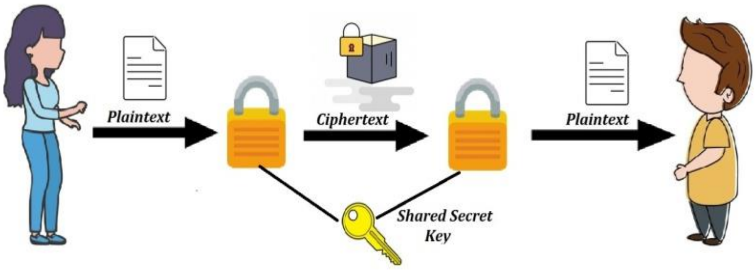
Keywords: Cryptography, Advanced encryption standard, Data encryption standard, Rivest-Shamir-Adleman Encryption algorithm, Message Digest, Privacy, Secrecy, Cipher, Encryption, Decryption.

I. INTRODUCTION

With the extent of modernization and technology the risk towards our data is rapidly increasing. Technology has become an important aspect in people's life, to exchange information we are highly dependent on Smartphone services. As multimedia documents/data are widely exchanged over internet, mostly through our smart devices, data security has become prominent. Is it really safe to use the simple Messaging system or instant messaging services provided by phones, web and other mobile communication devices? And the potential answer to this is a clear no, because most of our personal information which we tend to expose while chatting can be potentially visible to the eavesdroppers anywhere along its internet path or within the network. So use of cryptography in our everyday life has become a crucial factor.

II. WHAT IS CRYPTOGRAPHY

Cryptography is an act of hiding and securing information through the use of codes, generated using ciphers so that only the intended recipient can read and decode it.



Features of Cryptography

1. Confidentiality: Cryptography supports confidentiality of information, as it is accessible only to the user for whom it is intended.
2. Integrity: Integrity is a cryptographic feature which enables the data to be whole and undivided between the sender and the intended receiver.
3. Non-Repudiation: Cryptography prevents either parties from declining their authenticity over the data.
4. Authentication: Authentication helps in confirming the identities of sender and receiver and also in confirming destination and origin of information.

Types of Cryptography

1. Symmetric Key Cryptography : It is an Encryption mechanism where the sender and receiver uses a single common secret key which is shared among both of them for ciphering and Deciphering of message. The most popular Symmetric key Cryptographic mechanisms are AES(Advance Encryption Standard) and DES(Data Encryption Standard)

DOI 10.17148/IJARCCE.2020.9543

2. Hash Function: This algorithm does not require any key. A Hash value is calculated using the plaintext and a hash function, which makes the content of plaintext impossible to be recovered. The most popular algorithm using Hash Function and Hash value is MD5(Message Digest) algorithm.
3. Asymmetric Key Cryptography: Asymmetric Key Cryptography uses pair of keys i.e. a public key which is visible to all the end users and a private key which is known only to the sender for encryption and decryption of algorithm. The most popular algorithm Asymmetric key cryptography is RSA(Rivest – Shamir-Adleman) Algorithm.
Cryptogram Builder uses the collection of all these three types of Cryptography.

III. CRYPTOGRAPHIC ALGORITHMS USED

A. DES Algorithm

Data Encryption Standard is a symmetric block cipher algorithm, which takes a plain text as input in block of 64 bits and convert it into ciphertext using keys of 48 bit. DES in actual uses an effective key of 56 bits length using which in key generation phase it creates sixteen 48 bit keys. In order to generate the ciphertext, DES algorithm uses 16 rounds of Encryption using a different key for each round. The 16 round encryption used are in feistel structure. The main Advantage of DES is its 56 bit key that arises 2^{56} possibilities of key which makes it highly impossible to find the correct key using Brute Force attack.

In DES Algorithm, the plaintext of 64-bits is passed into for initial permutation and then it is forwarded into the rounds. There are total 16 rounds and each round uses a different round key. The 56-bit key is compressed and transposed to generate 16 48-bit keys which are supplied to each round. The resultant of each round is passed onto the next round finally passing it for final permutation which generates a final 64-bit ciphertext.

Data Encryption Standard	
Block Size	56 bits + 8 parity bits = 64 bits
Key Size	56 bits
Rounds	16 rounds
Algorithm Structure	Fiestel Cipher

B. AES Algorithm

Advance Encryption Standard is also known by its original name Rijndael. AES is Symmetric key block cipher based on Substitution, Permutation network and performs all its computation in bytes rather than in bits. AES takes 128 bit data as an input and utilizes 128/192/256 bit key for encryption and decryption. AES uses varying number of rounds based on the key length i.e. 10 rounds for 128 bit key, 12 rounds for 192 bit key and 14 rounds for 256 bit key.
The main advantage of AES lies in the key length option, as it becomes harder to cyptanalyze. This makes AES stronger and less susceptible.

In AES Algorithm, the plaintext of 128-bits is passed in for pre-round transformation. Then the transformed plaintext is forwarded to further round operations. The number of rounds is decided on the basis of key length i.e. 10 rounds for 128 bit key, 12 rounds for 192 bit key, 14 rounds for 256 bit key. The cipher key is passed to key generator which generates 128 bit round keys. In each round the plaintext undergoes permutation – substitution processes. After all operation the final round generates 128 bit ciphertext.

Advanced Encryption Standard	
Block Size	128 bits
Key Size	128/192/256 bits
Rounds	10/12/14 rounds
Algorithm Structure	Permutation –Substitution Network

C. RSA Algorithm

RSA is an asymmetric key cryptographic algorithm which utilizes two different keys a public key and a private key. This is why it is also known as public key cryptography as one of the key is available to everyone. The private key and public key are calculated using Extended Euclidean Algorithm. The main advantage of RSA is that it enables safer distribution of key. It is most widely used encryption algorithm.

RSA algorithm uses two keys, a private key and public key. The public key is known to everyone. The message is encrypted using public key can only be decrypted by private key.
Key Generation
Select two distinct large prime numbers randomly, say p and q
Compute $n = pq$
Calculate Euler's totient $ø(n) = (p-1)(q-1)$

DOI 10.17148/IJARCCE.2020.9543

Select an integer ***e*** such that	$gcd\ (ø\ (n), e) = 1 \text{ and } 1< e < ø(n)$
Now, Calculate	$d \equiv e^{-1} mod\ ø\ (n)$
Public Key will be given as,	$(PU) = \{e, n\}$
Private Key will be given as,	$(PR) = \{d, n\}$
For Encryption,	
Let the Plaintext be	$M \quad M<n$
Then Cipher text is computed as	$C = M^{d}(mod\ n)$
For Decryption	
The Cipher text is	C
The Plaintext is obtained by	$M = C^{e}(mod\ n)$

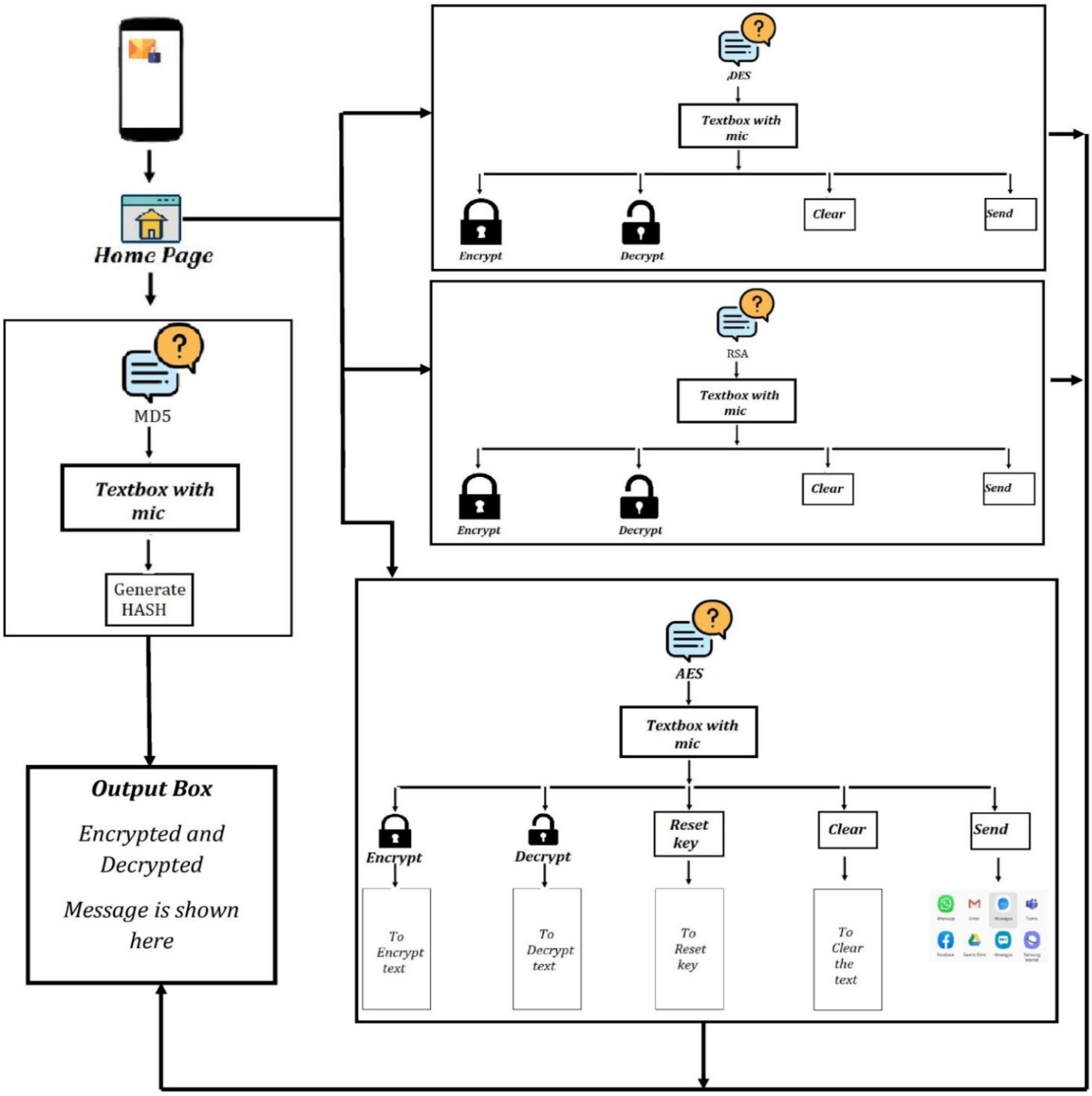
D. MD5 Algorithm

MD5 Algorithm is developed by Ron Rivest. It is used to produce a 128 bit Message Digest. MD5 takes 512 bit blocks of plain text and divides it into sixteen blocks, each of size 32 bits. Further passing it by five steps it produces Message Digest. MD5 is a widely used Hash Function producing algorithm.
MD5 Algorithm takes a message in a 512 bit block which is further dived into 16 blocks of 32bit each and generates a 128 bit message digest by following 5 steps:
Step 1: padding of bits is done to make the length of actual message 64 bits less than 512.
Step 2: Appending length, 64 bits are appended at the end.
Step 3: MD5 buffer is initialized which of 4 word length.
Step 4: The message is processed into 16 word blocks.

IV. ARCHITECTURE AND WORKING

Cryptogram builder is an android application which uses a collection of most popular cryptographic algorithms to generate encrypted messages and to decrypt the same on the receiver end.
Steps to be followed for using this application for Encryption.

- When you click on the app icon, it launches the Home page.
- The Home page of Cryptogram Builder provides four options that are AES, DES , RSA and MD5.
- User can select anyone of the provided option to encrypt the message he/she intent to.
- If option selected is AES, app launches to a new AES page.
- The user can type or speak to enter the message.
- Once the message is entered he could encrypt it by clicking on encrypt button.
- The AES encrypted message gets generated in the output box.
- Now, the user can send this encrypted message using the send button to any of the other services like email, messaging, Bluetooth, watsapp and so on.
- Before Encrypting If the user wishes to reset key, he could press the reset key button.
- On pressing reset key app would be directed to a new page, where he could enter and confirm the new key.
- If option selected is DES, app launches to a new DES page.
- The user can type or speak to enter the message.
- Once the message is entered he could encrypt it by clicking on encrypt button.
- The DES encrypted message gets generated in the output box.
- Now, the user can send this encrypted message using the send button to any of the other services like email, messaging, Bluetooth, watsapp and so on.
- But their no reset key option in DES as DES algorithm uses only fixed length key.
- If option selected is RSA, app launches to a new RSA page.
- user can type or speak to enter the message.
- Once the message is entered he could encrypt it by clicking on encrypt button.
- The RSA encrypted message gets generated in the output box.
- Now, the user can send this encrypted message using the send button to any of the other services like email, messaging, Bluetooth, watsapp and so on.
- If option selected is MD5, app launches to a new DES page.
- MD5 is used for generating hash value/message.
- Here also the user can enter text by typing or by speaking.
- By clicking on the Hash Button Message Digest gets generated.
- Now the user can use this Hash code.



Steps to be followed for using this application for Decryption.

- When you click on the app icon, it launches the Home page.
- The Home page of Cryptogram Builder provides four options that are AES, DES , RSA and MD5.
- User can select anyone of the provided option to decrypt the message he/she intent to.

- AES
  - At the receiver end, the received encrypted code of message can be decrypted by copying it into the textbox and using decrypt button.
  - In AES the receiver needs to reset the key to the key value used by sender in encrypting the message before proceeding for decryption.
- DES
  - At the receiver end, the received encrypted code of message can be decrypted by copying it into the textbox and using decrypt button.
- RSA
  - At the receiver end, the received encrypted code of message can be decrypted by copying it into the textbox and using decrypt button.

DOI 10.17148/IJARCCE.2020.9543

V. CONCLUSION

The main objective of this system is adding security to the messages before transferring them into a communication system. This Android-based application has been developed using AES DES RS MD5 Algorithms which helps a user to transfer their messages securely. Encryption and decryption of message are done by using AES DES RSA & MD5 Algorithm. Encryption and Decryption is the most feasible way for preserving the actual meaning of a message by hiding it in some code format from intruders any network environment. Security is a topmost factor that is considered everywhere and this is what Cryptogram builder does. It helps in providing Security, Integrity, Confidentiality, and Authentication while transferring a message.

ACKNOWLEDGMENT

In the first place, we would like to express our heartfelt gratitude to our project guide **Prof. Prince K Sahu,** Assistant Professor, Department of Computer Science and Engineering, GEC Bilaspur, for his committed guidance, valuable suggestions, and sustained help from the very early stage of this project work that made us to look every nook and corner of this project work, for the successful completion
We are very much great full to the respected Principal **Dr. B.S. Chawla** and **Prof. Sourabh Yadav**, Head of Department (Computer Science and Engineering), of GEC, Bilaspur for providing the facilities to carry out the project work

REFERENCES

[1]. Nishika and Rahul Kumar Yadav, "Cryptography on Android Message Applications – A Review" International Journal on Computer Science and Engineering (IJCSE), ISSN 0975- 3397, Volume 5, No. 05, pp. 362-367,2013.
[2]. Rohan Rayarikar, Sanke tUpadhyay and Priyanka Pimpale," SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications, Volume 50– No.19, pp. 0975 – 8887, July 2012.
[3]. Asst. Prof.Dr.Jane J. Stephan and Zahra Salah Dhaief," SMS Encryption by Using Android Operating System", Iraqi Commission for Computers & Informatics (ICCI), Iraqi Journal for Computers and Informatics (IJCI) Vol (1) Issue (1), 2014.
[4]. Bhimrao Patil, "SMS Security Using RC4 & AES" Indian J.Sci.Res. 11 (1): 034-038, 2015.

BIOGRAPHIES

Ms. S Sravya Sri pursuing Bachelor of Engineering [2016 – 2020] with major in Computer Science and Engineering from Government Engineering College, Bilaspur (C.G.) affiliated to Chhattisgarh Swami Vivekananda Technical University, Bhilai, India. Proficient in C, C++, Java and Android developer.

Ms. Zahra Saktiwala pursuing Bachelor of Engineering [2016 – 2020] with major in Computer Science and Engineering from Government Engineering College, Bilaspur (C.G.) affiliated to Chhattisgarh Swami Vivekananda Technical University, Bhilai, India. Proficient in C, C++, Java and Web developer.

Ms. Deepti Rathore pursuing Bachelor of Engineering [2016 – 2020] with major in Computer Science and Engineering from Government Engineering College, Bilaspur (C.G.) affiliated to Chhattisgarh Swami Vivekananda Technical University, Bhilai, India. Proficient in C, Java and Android Developer.

Ms. Sapna Painkra pursuing Bachelor of Engineering [2016 – 2020] with major in Computer Science and Engineering from Government Engineering College, Bilaspur (C.G.) affiliated to Chhattisgarh Swami Vivekananda Technical University, Bhilai, India. Proficient in C and C++.

DOI 10.17148/IJARCCE.2020.9543