RESEARCH PAPER ON DATA ENCRYPTION

ABSTRACT

In today's world of mobile phones data has become paperless and sharing of it has become wireless, therefore data security has become vulnerable thus cryptography provides a better way of data security through encryption and decryption ways. From buying small items in online shops to buying a big property or storing important information, digital signatures, watermarking, steganography, and other applications are nowadays done through the internet which consists of large amounts of data and wireless networks. Hence network security is one of the main concerns as the world changes into a digital world. Hence cryptography is essential in today's internet world. We will learn about cryptography and various types of cryptography.

I. INTRODUCTION

The science or art of cryptography involves rules and procedures for making messages unreadable in order to keep communications private. The word has a specific meaning in Greek, which is "hidden prose" or "hidden writing." Today, however, the messages are extremely well protected by encryption, ensuring that the data delivered is safe in a way that the intended recipient can read this data. When it comes to applications and internet usage for online banking, shopping, social networks, and other purposes, the world of today is more dependent on network connection. The necessity of cryptography increases with the rapid advancement of networking technology. Data security is therefore necessary when communicating sensitive information. The concept of encryption/decryption algorithms is employed, where encryption encrypts the plain message and converts it to cypher text, and decryption converts the cypher text back to plain text. In actuality, the advancement of encryption and the development of computers went hand in hand. Cryptography attracted the curiosity of Charles Babbage, whose Difference Engine concept before the development of modern computers. Germans employed the electromechanical Enigma machine to encrypt messages during World War II, and Alan Turing famously headed a British team that created a comparable device to break the code, providing some of the foundations for the first modern computers. In the process of encryption and decryption in cryptography, a key is used.

How Cryptography Works

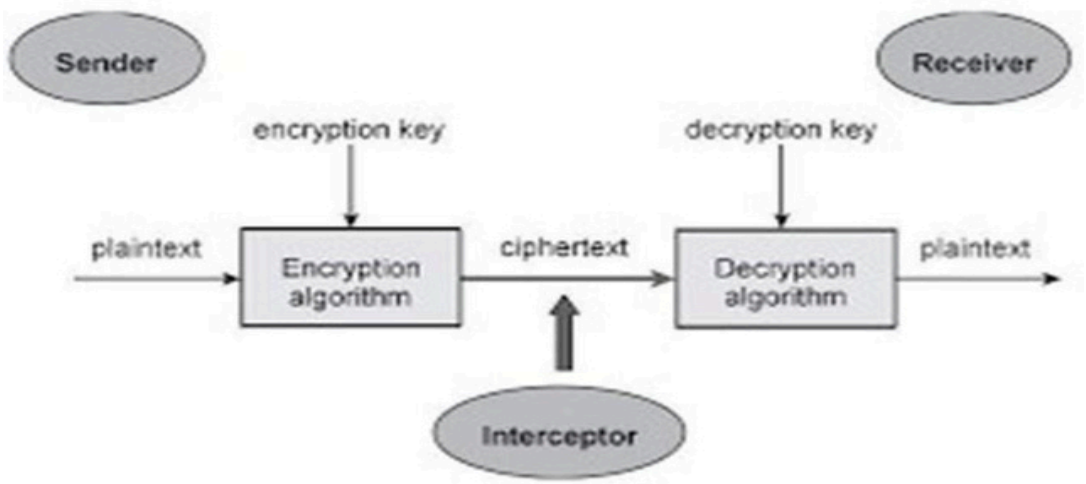

Figure 1: Working of Cryptography

Through the use of encryption, plaintext is transformed into information that is only accessible to the intended recipients. This information shouldn't be accessible to anyone else; thus, they shouldn't be able to comprehend it. Encryption procedures involve the conversion of plaintext into ciphertext. To turn a ciphertext into a

plaintext, decryption practices are followed. Hence the two main methods present in cryptography are Encryption and Decryption. At the Sender side the plaintext which he must send it is converted to the ciphertext through the Encryption method. There are various types of Encryption that are present which are discussed later in the further sections. That converted Ciphertext is transmitted to the receiver through wireless or wired networks. Then at the receiver side the Cipher text is converted back into Plaintext using the Decryption method. This is how cryptography works.

How Encryption Works

When the data is sent to the client in the form of Plaintext it is converted to a code and passed. The receiving device then converts this into the message which is a different method known as decryption. The entire process is done by the servers of the sender and the client devices.

Different encryption algorithms are available for the method. Encryption can work differently in many cases.

For Example: If sender wants to send the message “abc” Consider the message “abc” is mapped to “zyx” which is called as the cipher text. This mapping information may be stored in the key.

a ➡ z

b ➡ y

c ➡ x

This is how the encryption algorithm works.

It can be done in various methodologies and logics. There are many types of Encryption Algorithm.

II. ASYMMETRIC-KEY ALGORITHM

Asymmetric key which is also called public key encryption is an encryption method where a pair of keys are used for encryption. The pair is composed of a public key and a private key where the public key is issued to every device and the private key is used to convert cipher text into plain text on the decryption side. Asymmetric key is extremely used to secure exchange of communication and information on the internet. RSA algorithm is used to encrypt asymmetric keys and for reliable and secure transactions on the internet. Asymmetric is a bit slower when compared to symmetric because of the complex computations on cryptography of asymmetric keys. SSL is one of the best-known examples where the asymmetric key plays an important role for safe and secure communication on the internet. In this paper, we suggest a method for information confidentiality and authentication that will guarantee

implementing the RSA algorithm

authentication and privacy of data during transportation. The RSA algorithm is widely used in asymmetric cryptography for encryption and decryption of information.

Confidentiality refers to shielding a message from prying eyes, and authentication refers to the need for the receiver to be certain of the sender's identity.

Problem statement

In this cryptographic scenario, achieving authentication, secrecy, and integrity in a single step is quite challenging. The symmetric key is not as much like a shareable item in public key encryption and decryption, which are carried out with different keys. Similar to asymmetric key cryptography, which encrypts messages using symmetric keys but allows anybody to decode them with the private key. Confidentiality is difficult to preserve once authentication has been attempted. Only the intended recipient is able to decipher a communication when it is encrypted using a public key. Here, we manage secrecy, but we are unable to preserve sender authorization at the same time. To overcome this, after the private key we use public key encryption. After that, only the intended receiver would be able to decrypt the message while also being able to verify the sender's identity by decrypting the cipher message with a public key.

Explanation

Step 1: Choose two prime numbers: p = 11 and q = 13.

Step 2: Find **n = p x q** by multiplying these values, where n is referred to as the modulus for encryption and decryption. Now, we calculate n = p x q; n = 11 x 13; n = 143

Step 3: Calculate **φ(n)=(p-1) (q-1).**

Select a public key, e, where 1<e<φ and e is co-prime with φ.

Second, we calculate φ (n) = (p - 1) x (q-1) φ (n) = (11 - 1) x (13 - 1) φ (n) = 10 x 12 φ (n) = 120 Let us now choose the relative prime e of 120 as 7. Therefore, the public key is <e, n> = (7, 143) **Step 4**: Public key <e, n> is used to encrypt a plaintext message m. The following formula is used to obtain
ciphertext C from the plain text. To find ciphertext from the plain text the following formula is used to get ciphertext C. Let us choose as 65. **C = me mod n** C = 65*7 mod 143 C=45 **Step 5:** The private key is <d, n>. We utilize the following formula to determine the private key in a way that: **De = mod {(p - 1) x (q - 1)} = 1** D= 7d mod 120 = 1, which gives d = 103 The private key is <d, n> = (103, 143) **Step 6**: The private key <d, n> is used to decrypt ciphertext message c. The formula shown below is used to
compute plain text m from the ciphertext c.

m = cd mod n

m = 45103 mod 143

m=65

In this example, Plain text = 65 and the ciphertext =45

III. SYMMETRIC-KEY ALGORITHM

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. The keys may be identical, or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

1. AES (ADVANCED ENCRYPTION STANDARD)

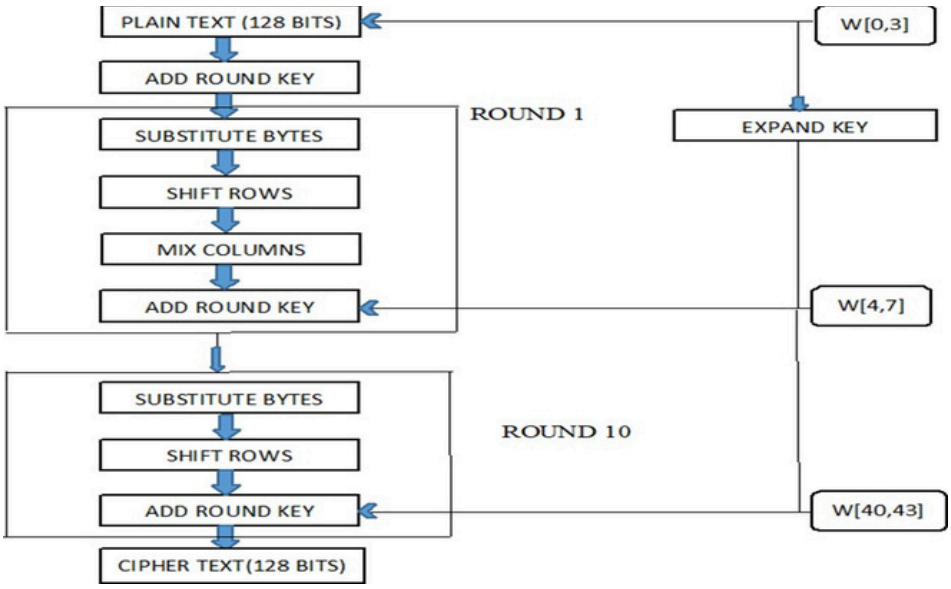

Figure 2: Working of AES

AES employs 128, 192, or 256-bit keys and enables 128-bit symmetric block messages. AES can have anywhere between 10 and 14 rounds, depending on the size of the key and the blocks. Figure uses a 128-bit key to depict the encryption overview of this protocol. For a key size of 128 bits, there are ten rounds of encryption. With the exception of the last round, which has a mix-column stage, all rounds are similar. As input into one 16-byte block of input data, one 128-bit plaintext is received from the left. After an initialization stage, the plaintext is produced as 16 bytes, m0 through m15, and then sent into round 1.

2. IDEA (International Data Encryption Algorithm) IDEA is a 128-bit block cipher that uses a 64-bit long plaintext. In the first round, it can use keys K1 to K6, in the
second round it can use keys K7 to K12, and finally in the last round an output transformation is needed with four subkeys (K49 to K52). The output produced by the output transformation stage is the final output. The final output is created by linking the components C1 through C4. IDEA has a total of eight rounds. Each round consists of a series of operations using six keys on the four data blocks. The subsequent steps of each round's addition and multiplication are not simple, but they are addition module 216 (65536) and multiplication module 216 + 1 (65537). Sub-key generation for a round – 1. Bit positions 1-96 of the key are used in the first round. Bits 97 to 128 are still unused. Round 2 receives
them.

2. In the second round, bits 97–128 are utilized as the first bits; as a result, a circular left shift of 25 bits arises, and bits 26–89 are now used. Bits 90–128 and 1–25 are still empty.
3. In the third round, previously unused bits 90-128 and 1–25 are used for the first time, followed by a 25-bit circular left shift and bits 51–82. Bit positions 1-50 and 83-128 are still empty.
4. Bit positions 83-128 and 1-50 are used in the fourth round.
5. In the fifth round, a left-circular shift of 25 bits appears and bit position 76-128 and 1-43 are used. Bit position 44-75 remains unused.
6. The fifth round's unused bits are utilized. In the sixth round, there is a left circular shift of 25 bits, leaving bit positions 37–100 empty.
7. In the seventh round, the sixth round's unused bits, namely 37-100, are employed for the first time, and a circular left shift of 25 bits appears at positions 126-128 and 1-29. Bit 30-125 is still not in use.
8. The key is disabled and the unused bit position 30-125 from round seven is used.

It is a one-time activity. It happens toward the finish of the eighth round. Along these lines 64digit esteem is separated into four sub-blocks (express R1 to R4) and four subkeys are utilized here. The decoding system is comparable to the encryption cycle. There are a few modifications in the age and plan of subkeys. The decoding subkeys are inverse of the encryption subkeys.

3. DES (Data Encryption Standard)

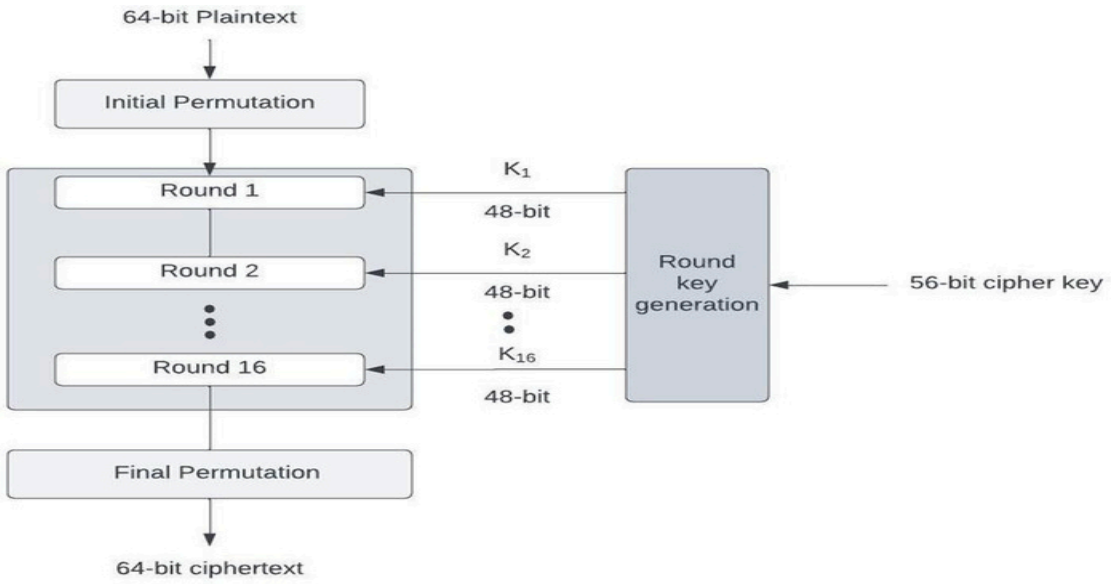

Figure 3: Working of DES

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses a 16 round Feistel structure. Begin DES Algorithm

1. Initialize. Before round 1 begins, all 64 bits of an incoming message and all 56 bits of the secret key are separately permuted (shuffled).
2. Each incoming 64-bit message is broken into two 32-bit halves denoted by Li and Ri, respectively.

3. The 56 bits of the key are also broken into two 28-bit halves, and each half is rotated one or two bit positions, depending on the round. 4. All 56 bits of the key are permuted, producing the version of the key on round i. 5. In this step a logic Exclusive-OR, and the description of function F() appears next. Then, Li and Ri are determined. 6. All 64 bits of a message are permuted.

The activity of capability F() at any round I of DES is as per the following.

1. Out of 52 pieces of ki, capability F() picks 48 pieces. 2. The 32-digit Ri–1 is extended from 32 pieces to 48 pieces so it tends to be joined with 48piece ki. The extension of Ri–1 is done by initial breaking Ri–1 into eight 4-bit lumps and afterward extending each piece by replicating the furthest left piece and the furthest right piece from left and right neighboring lumps, individually. 3. Capability F() additionally parcels the 48 pieces of ki into eight 6-digit lumps. 4. The relating eight lumps of Ri–1 and eight pieces of ki are joined as follows.

At the collector, similar advances and a similar key are utilized to switch the encryption. It is presently obvious that the 56-bit key length may not be adequate to give full security. This contention is as yet disputable. Triple DES gives an answer for this contention: three keys are utilized, for a sum of 168 pieces. It ought to likewise be referenced that DES can be carried out more productively in equipment than in programming.

IV. ANALYSIS

In this research, we examine asymmetric key cryptography's ability to protect information sharing's authenticity and confidentiality. As we previously stated, confidentiality refers to shielding a message from public view, and authentication denotes the need for the receiver to be certain of the sender's identity. Figure 1 illustrates in detail how information can be made confidential and legitimate. We put the RSA encryption and decryption technique into practice. We also examine the fact that the RSA algorithm's key generation time increases when key size is increased.

Advantages:

1. Encryption is cheap in implementing methodology.
2. Increasing the integrity of our data through encryption.
3. Consumer trust can rise because of encryption.
4. Encryption is a simple method which has many types of algorithms.
5. Encryption provides confidentiality between the data.

Disadvantages:

1. Strong encryption makes a message potentially difficult to access, even for authorized users.
2. Encryption does not provide selective access control for the user.
3. Encryption does not secure the data in case of poor design of system.
4. Encryption takes more time for the process.

V. CONCLUSION

In this paper, the method of how cryptography and encryption works are discussed with example. Then the asymmetric and symmetric key algorithms are discussed briefly. Then the types of symmetric key algorithms like AES, IDEA and DES are explained briefly with figures. Then at last the advantages and disadvantages of encryption method in cryptography are mentioned. From this we got to know about data encryption in Cryptography.