ALGORITHM PROBLEMS INCONVENTIONAL CRYPTOGRAPHY

[1]Dr G.Vani, [2] B.Pallavi

[1]Asst. Professor, Dept CSE, Sreenidhi Institute of Science and Technology
vanig@sreenidhi.edu.in

[2]Asst. Professor, IT Dept., SreenidhiInstitute of Science and Technology
pallavir@sreenidhi.edu.in

Abstract

Cryptographyconverts original information into secret codes, allowing the proposed receivers to recover the original content. Military operations, secret government services, and diplomatic services have used cryptography for years to provide security functions like data confidentiality, integrity, and origin authentication.

Index Terms: ***Cryptography, original information***

1.1. INTRODUCTION

Cloud computing storage is a growing prototype with computing capabilities in a virtual environment. Data security in the cloud is essential for outsourcing data to the cloud, so the current focus is on cryptography concepts used in cloud computing technology. Losing direct access to stored data makes consumers wary of cloud services. Since the start, data privacy and security have been reasonable. According to recent reports from the US National Security Agency (NSA), PRISM [1] and Intel [2], a lack of security knowledge is slowing cloud adoption. After learning of NSA eavesdropping, 54% of German corporations question cloud security and consider it risky [3]. Info security reported [4] that brute-force and cloud-to-cloud attacks hit 48 enterprises worldwide.

Thus, cloud security must be precise to protect cyberspace, especially outsourced encrypted statistics and occasional information truthfulness and accessibility checks. However, the security mechanisms for storing encrypted data require bulky key management and access control and examine massive amounts of data. This chapter introduces secure cryptographic methods for cloud security and

confidentiality. Cloud security issues are gaining attention in applied cryptography and computer research. Consider a depository setup where customers outsource data to remote servers. Customer-wise, cloud servers are distributed in black boxes. The offered practices should protect the service provider and the customer's security by creating an effective and reliable service. This article presents formal security models and cryptography fundamentals in cloud storage.

2. CRYPTOGRAPHY MEANING

Cryptography is the art of converting the original information into secret codes and
permitstheproposedreceiverstorecuperatetheoriginalcontentofinformationandisin useformilitary operations, governmental secret services and diplomatic services from last so manyyears to deliver the security functionalities like data confidentiality, data integrity and dataorigin authentication [5].
Due to the rapid growth of computing networks, cryptography has expanded into symmetric and public key categories.

2.1. Symmetric Cryptography

The relationship distinguishes cryptographic schemes between two keys that encrypt and decrypt a message. "***The operation of symmetricorconventionalcryptographydependsonsharingasecretkeybetweentwocommunicating entities Alice and Bob* [6]*".*** $\acute{C}$ cypher text message space, $\acute{M}$ plaintext and $\acute{K}$ the key space. The symbol for the encryption algorithm is $\acute{E}$, andthedecryption algorithmby$\dot{D}$, exemplified as follows**[6]**:

- The algorithm for encryption $\acute{E}:\acute{M}\times\acute{K}\rightarrow\acute{C}$accepts the plaintext message as input*m*,besides the hidden key*k*, and returns the encoded text$\acute{C}$. $\acute{E}$frequently randomized.
- The deciphering algorithm $\dot{D}:\acute{C}\times\acute{K}\rightarrow\acute{M}$accepts as input the encrypted message *c*,*k*and returns the unencoded text *m*. $\dot{D}$is always predetermined.
  The equation defines symmetric cryptography.:

$$\forall m \in \acute{M}, k \in \acute{K}, \dot{D}(\acute{E}(m, k)k) = m \quad \ldots\ldots (1.1)$$

- Encryption and decryption rely on substitution and transposition in symmetric key cryptography. The first symmetric key algorithms were Caesar, Hill, Playfair, and the One-Time Pad. In the 1970s, Horst Feistel devised the Data Encryption Standard and the Feistel Cipher. Later in 2001, Vincent Rijmen and Joan Daemen created the Rijndael Cipher and Advanced Encryption Standard.

2.2. Asymmetric Key Cryptography

Asymmetric Key Cryptography (PKC) [7] guarantees information privacy, non-repudiation, and validation while trading information over an insecure network. Unlike symmetric cryptography, where two parties must share a secret key., ***public key cryptography reliesontworelatedkeystosecuretheexchangedinformation***.Each entity shares public and private keys. Figure1.1 shows that the Private Key is kept secret.

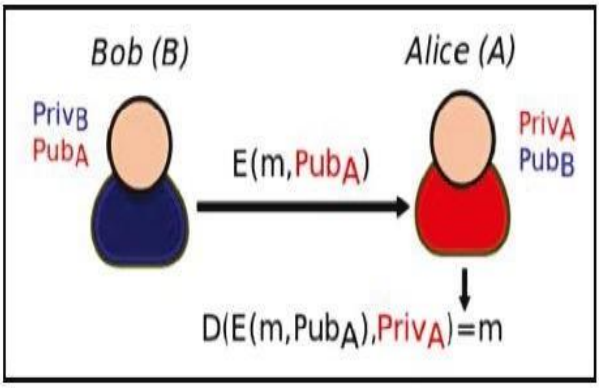

Figure1.1:WorkingMechanismof PublicKey Cryptography

Public key cryptography is based on generating pseudorandom numbers, block cyphers, and stream cyphers. In 1970, W. Diffie and M. E. Hellman conceptualized a shared secret key over an unsecured communication. R. Rivest, A. Shamir, and L. Adleman created the RSA cryptosystem in 1977, which is based on integer factorization and can be used for encryption and digital signatures. Elliptic Curve Cryptography (ECC) was introduced by Neal Koblitz and Victor S. Miller in 1985, but industrial use of this algorithm did not begin until 2004-2005. Later in 1987, Ron Rivest developed the

Rivest Cipher (RC4), which Bob Jenkins cracked in 1994. Consequently, RSA is the most popular and widely used public-key cryptosystem.

3.STANDARDCRYPTOGRAPHICMETHODS

Conventional cloud data security algorithms include the following protocols

3.1. VernamOneTimePadScheme

Gilbert Vernam developed this algorithm in 1917. According to the Vernam process pad scheme [9], ***encryption techniques assume the secret key 'k' is a random bit string as long asthemessage,m'***.One-time pads encipher a single message with a private key that must be renewed for each message. One-time pads are secure because cryptanalysts cannot decipher the encrypted message. Claude Shannon mathematically proved that the former pad scheme is very safe [10].

3.1.1.Substitution Technique

In the substitution technique, letters in plaintext are replaced with other letters, numbers, or symbols. If the plaintext is observed as a collection of bits, substitution consists of replacing the plaintext bit arrangement with the cypher text bit arrangement. These include Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, etc. [11].

3.1.1.1 Caesar Cipher

"Julius Caesar introduced the Caesar Cipher through the substitution cypher. It is the earliest substitution cypher known to humanity. The Caesar cypher entails substituting each letter of the alphabet with the letter three positions further down the alphabet [11**]**.

Example

Plaintext: *paymoremoney*

Ciphertext: *SDBPRUH PRQHB*

This algorithm is explicable as:

$$Ç = Ê(3, p) = (p + 3) \bmod 26 \quad \text{…..(1.2)}$$

Since the shift can be of any size, the general Caesar Cipher Algorithm can be written as follows:

$$Ç = Ê(k, p) = (p + k) \bmod 26 \quad \text{…. (1.3)}$$

Where the number ranges between 1 and 25. It is how the Caesar Cipher's decryption algorithm is written:

$$p = Ð(k, Ç) = (Ç - k) \bmod 26 \quad \text{…. (1.4)}$$

3.1.1.1 PlayfairCipher

3.1.1.2 Play fair Cipher

In 1854, Sir Charles Wheatstone created the Playfair cypher. The multiple-letter cypher transforms plaintext schematics into Cipher text. This technique uses a 5x5 letter matrix constructed using keywords. Figure 1.2's keyword is "monarchy." Filling in the keyword letters (minus duplicates) from left to right and top to bottom creates the matrix. The remaining letters are loaded in alphabetical order.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Figure1.2: 5 ×5Matrix toDesign the PlayfairCipher

Example

Plaintext: *meetmeat theschoolhouse*

Ciphertext:*CL KLCLRS PDIL HYAVMP HFXL IU* **[11].**"

The British and US armies used the Playfair cypher in World War I and II. Playfair cypher uses letters with 26 × 26 = 676 diagrams of letter frequencies. Thus, diagram identification and frequency analysis are more challenging [11].

3.1.1.2 HillCipher

In 1929, the mathematician Lester Hill developed the Hill Cipher. In the process of encryption, the Hill Cipher algorithm considers ***m*** consecutive plaintext letters and replaces them with ***m*** cypher text letters. The substitution is determined by ***m*** linear equations that assign numerical values to each character. (*a=0, b= 1, …z=25*)**[11]**.

For*m =3,*The Hill Cipher is expressible as:

$$Ć_1 = (ḱ_{11}ṕ_1 + ḱ_{12}ṕ_2 + ḱ_{13}ṕ_3) \bmod 26 \quad \text{…. (1.5)}$$

$$Ć_2 = (ḱ_{21}ṕ_1 + ḱ_{22}ṕ_2 + ḱ_{23}ṕ_3) \bmod 26 \quad \text{…...(1.6)}$$

$$Ć_3 = (ḱ_{31}ṕ_1 + ḱ_{32}ṕ_2 + ḱ_{33}ṕ_3) \bmod 26 \quad \text{…..(1.7)}$$

Alternatively, this may be stated as follows:

$$Ć = ḰP \bmod 26 \quad \text{….} \quad \textbf{(1.8)}$$

Where$Ć$ and$Ṕ$-3-length column vectors (signifying the plaintext and ciphertext)

$Ḱ$ - 3 × 3 Matrix (signifying the

encryption key)**Example**

Plaintext:'pay more money'utilizing the encryption key,

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Vector represents the first three letters. [15 0 24].

Then$K$ [15 0 24]=[375819 486]mod26 =[11 13 18]=*LNS*

Therefore,theciphertext: *LNSHDLEWMTRW*

In the process of decryption, the inverse of the matrix can be expressed as:

Theinverse$K^{-1,}$ Matrix K*, is described by the equation*:

$$KK^{-1} = K^{-1}K = I. \quad \textbf{(1.9)}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Where I is

$$\begin{vmatrix} 0 & 0 & 1 \end{vmatrix}$$

If asquarematrix$\hat{A}$hasanonzerodeterminant, thenthe inverseofthematrixis computedas:

$$[\hat{A}^{-1}]_{ij}=(-1)^{i+j}(\dot{D}_{ji})/det(\hat{A}) \qquad \text{…..(1.10)}$$

Where($\dot{D}_{ji}$)is the sub-determinant formed by removing the i^{th}rowandthej^{th}columnof$\hat{A}$and $det(\hat{A})$is thedeterminant of$\hat{A}$.

The available Hill Cipher system can therefore be expressed as:

$$\acute{C} = \acute{E}_{\acute{K}}(\acute{P}) = \acute{K}\acute{P} \bmod 26 \qquad \text{…..(3.11)}$$

$$\acute{P}=\dot{D}_{\acute{K}}(\acute{C})=\acute{K}^{-1}\acute{C} \bmod 26=\acute{K}^{-1} \quad \acute{K}\acute{P}=\acute{P} \qquad \text{…..(3.12)}$$

3.2 TranspositionTechniques

Plaintext has been permuted as part of the transposition technique. In a regular system, the plaintext shifts, causing the ciphertext to initiate a plaintext permutation. Mathematically, the characters' positions are encrypted using a bijective function and decrypted using its inverse. This method is known as the transposition technique. These transposition techniques include the Rail Fence Cipher, the Route Cipher, Columnar Transposition, Double Transposition, Disrupted Transposition, Grilles Detection and Cryptanalysis, Combinations, and Fractions, among others [11].

3.2.1.1 RailFenceCipher

The Rail Fence cypher is encoded as a rail of characters. Plaintext is written downwards on successive "rails" of an imaginary fence, then upwards when we reach the bottom. The message is subsequently read in rows [11].

Example,

Plaintext: 'WE ARE DISCOVERED. FLEE AT ONCE' and using three

"rails"W. . . E . . . C . . . R . . .L. . . T . . . E
. E.R .D .S .O .E.E .F.E .A.O . C.
. . A . . . I . . . V . . . D . . . E . . . N .

.Ciphertext:WECRLTEERDSOEEFEAOCA IVDEN**[11]**

3.2.1.2 RouteCipher

Route cypher, a transposition cypher, writes the plaintext in a grid of given dimensions and reads it in a key-defined pattern.

Example,

Plaintext:'WEAREDISCOVERED.FLEEAT ONCE'

Plaintext Grid Dimension:

W R I O R F E O
EEE S V E L A N
JADCEDETCX

Ciphertext:EJXCTEDECDAEWRIORFEONALEVSE

"Spiral inwards, clockwise, starting from the top right" is key. Route Cipher uses more keys. Union Forces used Route Cipher during the Civil War [11].

3.2.1.3 ColumnarTransposition

This transposition method writes the message in rows of a fixed length and reads it column by column in a scrambled order. Keywords define row width and column permutation.
Regular columnar transposition cyphers fill empty spaces with nulls, but irregular ones leave them blank. The keyword-ordered message is read in columns.
Example,
Keyword: ZEBRAS(lengthis6)
Thus, the rows are 6, and the permutation is '6 3 2 4 1 5'.

Plaintext: WE ARE DISCOVERED. FLEE ATONCE.
In aregularcolumnartransposition,

6 3241 5
W E A R E
DISC O V
ERRD F L
EEE T O N
CEEQK J EU

Ciphertext: 'EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE', provided the five nulls attheend,i.e.,QKJEU.

irregular columnar transposition,

63241 5
W E A R E
DISC O V
ERED F L EE
A T O N CE

Ciphertext:EVLNACDTESEAROFODEECWIREE

Divide the message length by the key length to decrypt the ciphertext [11]. "

3.2.2 ChallengeswiththeConventionalCryptographyAlgorithms

Modern data centres may not be secure enough with conventional cryptographic schemes. These methods fail when storing or outsourcing much data. Security, bandwidth, memory, and power consumption affect distributed service availability and performance in cloud computing storage environments [12]. Challenges include:

- Due to a long time it takes to exchange keys in the Vernam algorithm [9], the secret key's length cannot be the same or longer than the length of the message.

- In a security model for a service provider that cannot be trusted [13], the customer usually encrypts data before sending it to isolate servers. So, using traditional asymmetric algorithms is too hard when you have much data, and the amount of computation that can be done on the client side is significantly reduced.

- Classical Asymmetric Algorithms [13] necessitate the deployment of public key infrastructure (PKI) and certificate management functions to generate and distribute certificates to authenticated entities. In addition, clients must periodically download revocation lists from the Certification Authority to confirm the validity of certificates. Consequently, both bandwidth consumption and availability requirements deteriorate.

- Using Symmetric Cryptographic Schemes to encrypt client-side data prevents the service provider from gaining access to the decryption keys. However, with flexible data sharing among users, the confidentiality [12] provision becomes more intricate. In other words, it requires the efficient distribution of decryption keys among authorized users. The challenge is to define a group revocation that does not require updating the remaining group members' secret keys. Therefore, the complexity of crucial administration is reduced.

- Substitution techniques (Caesar Cipher) are particularly vulnerable to brute force attacks and are also deterministic [11].

- Transpositiontechniquesareeasilyrecognizedbecauseithasthesameletterfrequenciesas the originalplaintext. Therefore, thesearenot secure**[11]**.

As these traditional cryptographic tools are predominantly deterministic, they are not adaptable and do not permit operations over encrypted data, such as the search for encrypted texts. Search is a helpful method for retrieving data on remote servers that have been outsourced. Apple Spotlight [14] and Google Desktop [15] are two examples of applications that index data to facilitate a quick search.

New types of symmetric encryption schemes, known as ***block cyphers***, were developed to address the shortcomings of the standard algorithm. These algorithms encrypt data blocks with minor keys of predetermined bit lengths. Many block cyphers rely on permutations. Data Encryption Standard (DES) [7] and Advanced Encryption Standard (AES) [7] are the most well-known algorithms. Several cloud service providers, such as the US-based Amazon Simple Storage Service S3 [16], use the latter extensively. Cloud storage researchers emphasize data security more while considering proposed algorithms' impact on cloud performance. Thus, modern symmetric encryption algorithms satisfy several cloud security requirements, including cloud availability and compliance, making them suitable for processing large outsourced data streams.

Conclusion

ThechapterexplainstheexistingAESandRSAcryptosystemsandemphasizesthecomputationalrequirementofbothalgorithms.Thelogarithmicmethodtodothefactorization inRSAhasalsobeenanalyzed.AESandRSAimplementationhasbeendiscussedforboth theOS(Windows10&UbuntuLTS16.04)andperceivedthat AESandRSAalonecould notprovidebetterdatasecuritytothecloud.A hybrid data security algorithm has to be proposed to enhance the security and privacy of factorization concerns.

REFERENCES

[1] EladYoran. "NSA Surveillance: First Prism, Now Muscled Out of Cloud."https://www.darkreading.com/cloud-security/nsa-surveillance-first-prismnow-muscled-out-of-cloud/d/d-id/1112686,November 26, 2003.[April28, 2018]

[2] Louis Columbus. "2017 State Of Cloud Adoption And Security."https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#7b03a69b1848,April 23,2017.[April28th, 2018]

[3] Robin Harris. "NSA Spying Poisons the Cloud Market: Survey."https://www.zdnet.com/article/nsa-spying-poisons-the-cloud-market-survey/, November8, 2013.[April28th, 2018]

[4] BruteForceAttack, "CloudSecurity,"InfosecurityMagazine.https://www.infosecurity-magazine.com/cloud-security/[April28th, 2018]

[5] InternationalOrganizationforStandardization,"InformationProcessingSystems,"ISO/IECJTC1/SC 7, 1stedition,ISO 8807:1989.1989 https://www.iso.org/obp/ui/#iso:std:iso:8807:ed-1:v1:en[April28th,2018]

[6] W. Diffie and M. Hellman, "New Directions in Cryptography,"*IEEE TransactionsonInformation Theory*,vol. 22, no. 6,pp. 644-654, November1976.

[7] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES andRSA for Security,"*Global Journal of Computer Science and Technology Network,Web&Security,*vol. 13,no. 15, 2013.

[8] Mandeep Kaurand ManishMahajan,"UsingEncryptionAlgorithmstoEnhancethe DataSecurityinCloud,"*InternationalJournalofCommunicationandComputerTechnologies,*vol. 12, no. 3, pp.56-59, 2013.

[9] G.S.Vernam,"CipherPrintingTelegraphSystemsforSecretWireandRadioTelegraphic Communications,"*IEEEJournal*, vol.55, pp. 109-114,1926.

[10] C.E.Shannon,"CommunicationTheoryofSecrecySystems,"*BellSystemsTechnicalJournal*, vol. 28, pp.656-715, 1948.

[11] P.PooniaandP.Kantha,"ComparativeStudyofVariousSubstitutionandTranspositionEncryptionTechniques,"*InternationalJournalofComputerApplications*, vol. 145, no. 10, pp. 24–27, July2016.

[12] Birendra Goswami and S. N. Singh, "Enhancing Security in Cloud computing usingPublic Key Cryptography with Matrices,"*International Journal of EngineeringResearchand Applications (IJERA),*vol. 2,no. 4, pp. 339–344, 2012.

[13] L.Weietal.,"SecurityandPrivacyforStorageandComputationinCloudComputing,"*Journal of InformationSciences,*vol.258, pp.371-386,2014.

[14] Acronis Technical White Paper, "Network Spotlight Best Practices," 2011.https://www.acronis.com/sites/default/public_files/product_documentation/Network
-Spotlight-Best-Practices-
07142011.pdf.[April10th, 2018]

[15] B.Turnbull,B.BlundellandJ.Slay,"GoogleDesktopasaSourceofDigitalEvidence," *InternationalJournal ofDigital Evidence*,vol. 5,no. 1,Fall 2006.