BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN(Print):2348-0513; ISSN(Online): 2454-471X;
Vol. 3, Issue 9, Sep 2015, 95-100
© BEST Journals

INTRODUCING A NEW CRYPTOGRAPHIC SCHEME: AK CIPHER

ABHISHEK DADHWAL & KOMAL RAJPAL

Master of Computer Applications (MCA), Guru Gobind Singh Indraprastha university (GGSIPU), Delhi, India

ABSTRACT

Disclosure of information or leakage of data in an untrusted environment may lead to unauthenticated access to the confidential information and systems security. Whenever a message is transmitted by a sender to a receiver, it means to have a complete protection from ground to up so that no attacker may gain any access to private information. The information exchange, now a days, underlie most modern security protocols. Many schemes have been applied since the security has been considered as the key agreement. [1]For instance-sending sensitive information like social security, passport or credit card numbers, via email is necessary, at such points encrypted message sending is considered. A key is, therefore, provided for encryption process of the sender's message and encrypted message is then decrypted at the receiver's side. In this way a secure message is transferred. Formalisation of a proposed technique, AK Cipher, combines two strong techniques and guarantees two times safer sending and receiving which has been shown practically.

Different security channels and tools have been provided to prevent unauthorized access for the exchange of data between two parties. Thus, granting information secrecy and authenticated access. Nevertheless, proposed technique improves encryption security.

KEYWORDS: Integrity, Security.

Encryption: Encoding a plain text to convert it into cipher text.

Decryption: Decoding a cipher text to obtain the original message.

Authentication: Sender's message must be received by right receiver.

Integrity: No modifications or alterations with the data must be done.

[3]Plaintext: The intelligible message which will be converted into an unintelligible (encrypted) message.

[3]Ciphertext: A message in encrypted form.

[3]Key: A parameter used in the encryption and decryption process.

[3]Cryptosystem: A system to encrypt and decrypt information

INTRODUCTION

[2]A cracker is a hacker who uses the knowledge of hacking for malicious practice.

Cryptosystems play an important role in data hiding and temporary manipulations so as to prevent the breaching of various authentications and data exposal. Various mechanisms over time have evolved for the denial of uncovering the information to any third party or unauthorized access. Various imposed techniques which are classified under KEY cryptography are:

- One time passwords(OTP) Technique
- Transposition Cipher Technique
- Vernam cipher Technique

All these competitive schemes are proficient to address the security issues correctly. A special pattern is followed in all of the above techniques which include a KEY attachment with the original message.

METHODOLOGY

Introduced technique, AK CIPHER, incorporates an extract from two algorithms. Specialized elicitation of user's message from the matrix form is combined with the additional characters, key, for level 1 encryption and a new key is again entered by the user for level 2 encryption which is blended with level 1 encryption.

This Methodology Certainly simple, secure, efficient, and robust. It also exemplifies flexibility with the testament of time efficiency.

Proposed Algorithm

Step1: Read First key Value Entered by the user.

Step2: Read the Message to be Sent, Entered by the user.

Step3: Calculate the Length Parameter for Both Key and Message.

Step4: Calculate the Size of the matrix.

Step5: If (Matrix Size >Message Size)

Key Length is set to Matrix Size

Else

Automatic Increment in the Matrix Size On the Basis Of Key.

Step6: First Encryption Scheme is Applied On the Plain text To be Send, Using First Encryption technique

Step7: Encrypted Message Is Considered as New Plain Text.

Step8: Read Second key (0-9) Entered by the User

Step9: Calculate the Size of Second key.

Step10: Calculating the Length of Second Entered Key

Step11: if (Length of New Plain Text=Length of Second Key) then Second Key will be Considered as Final key.

Step12: else if (Length of New Plain Text > Length of Second Key) then Automatic Generation of keys up to length of New Plain Text Considered as Final key.

Step13: else (Length of New Plain Text < Length of Second Key) then Automatic Rejection of Keys, matched till Length of New Plain Text Considered as Final key.

Step14: Perform the Xor Operation Between New Plain Text and Final Key,Results into Cipher Text.

Step15: Display Final Encrypted Message.

Step16: The Decryption of the Same Cipher Text is carried out in the Reverse Way as the Encryption is done.

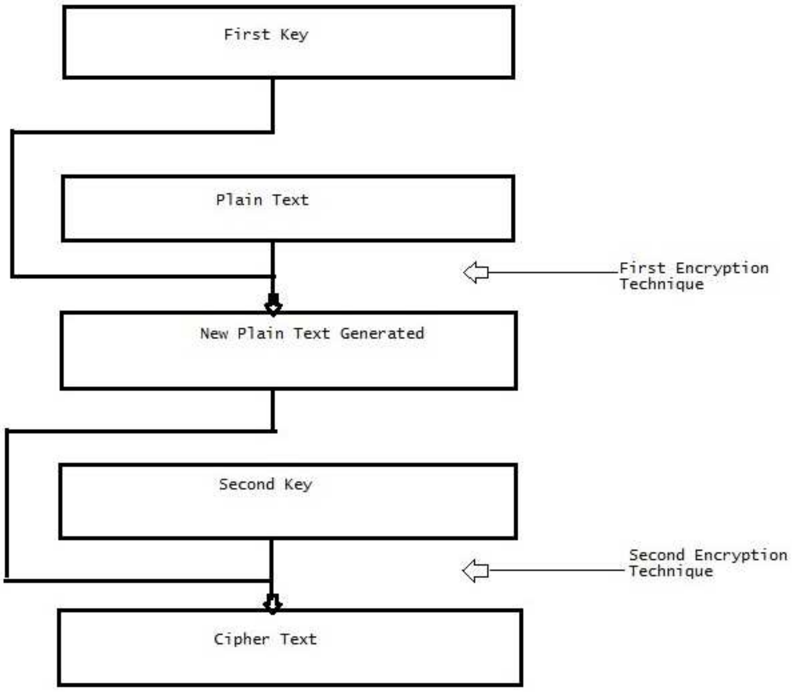
Step17: Perform the Xor Operation in Between Cipher Text and the 'Final Key'.(Level 1 Decryption is Over)

Step18: Calculate the Size of the Decrypted Text.

Step19: Use the Decrypted text within the Matrix as performing the First Encryption Scheme.

Step20: Display the Original Plain Text.

Working Phase



WORKING MODEL OF AK CIPHER

Figure 1

Comparitive Study of 'AK Cipher' with Different Encryption Techniques

Transposition Cipher

In transposition cipher, words are rearranged a fixed length row. They are then extracted column-wise to form a cipher text. [4]It is easy to implement cipher that follows a simple rule for mixing up the characters in the plain text to form the encrypted message.

- For small text messages, the ciphertext is easily deciphered by anyone who willingly try to hack the code with different key values.
- A transposition cipher doesn't change the Identity of Characters in the plain-text when it generates the cipher-text, what it just change is Character's Positions.

- [5]The main problem with this ciphers is that the actual letters are not changed, so frequency counts reveal not only trends in letter repetition but the actual plaintext letter that the Cipher text is linked to (because they are the same letter!)
- Another weakness is that if the attacker intercepted two or more messages of the same length using the same key, revealing of the actual message is not complicated then.

One Time Pad

OTP is one the most important aspect which is generally considered in password security.

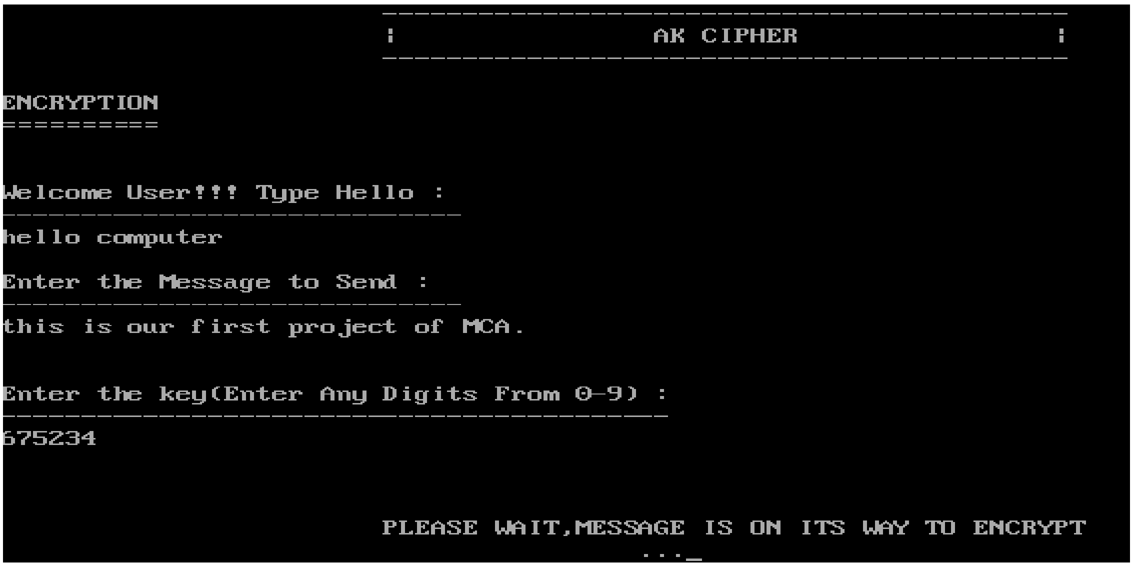
- It would be Easy to reverse engineer if once the OTP-generation algorithm is known leading to learn future Passwords, thus can break the Secure Message transmitted over Network.
- [6]OTPs have one main disadvantage, that is, they generate a file with the random OTPs. Because the file might contain 10, 20, or even 100 passwords, the user has a tendency to print this file and keep it on or in his desk. The user then uses this printout to log in to a device, choosing one of the passwords in the list and crossing it off after it is used. Anyone who has access to the user's desk can compromise his account.
- [6]In addition, if this file is printed to a network printer, it can be compromised through eavesdropping. Note that Cisco routers do not support OTP innately.
- [6]Also weakness of OTPs is that they are susceptible to eavesdropping. When the hacker knows the passwords stored in the file, he easily can gain unauthorized access to this user's account; from here, the hacker can install keystroke-capturing and backdoor programs to overcome the OTP authentication method for authorizing access to the user's device or resource.

AK CIPHER

- With respect to Vernam Cipher, AK Cipher not only dependent on the random key generation concept but as well as surrounded by another Technique Which provides the basis for next phase encryption(Random key generation technique),Thus leads to better security of transmitted message.
- In our new technique, AK cipher, a special form of columnar transposition cipher has been shown. The plaintext is extracted using a key entered by user and the combination of this can be more difficult to break which improves security.
- AK cipher can be used to combine two pseudo-random sequences, with a result into more complex sequence.
- AK cipher generating the highly secured cipher text on the basis of change in position as well as change in the identity of the plain text characters.
- The advantage of using the 2-level encryption operation for this, is that it can be undone by carrying out the same operation again.
- While encrypting the plain text, 2nd technique is quite dependent on 1st one And at the same time both are encrypting the message individually too.

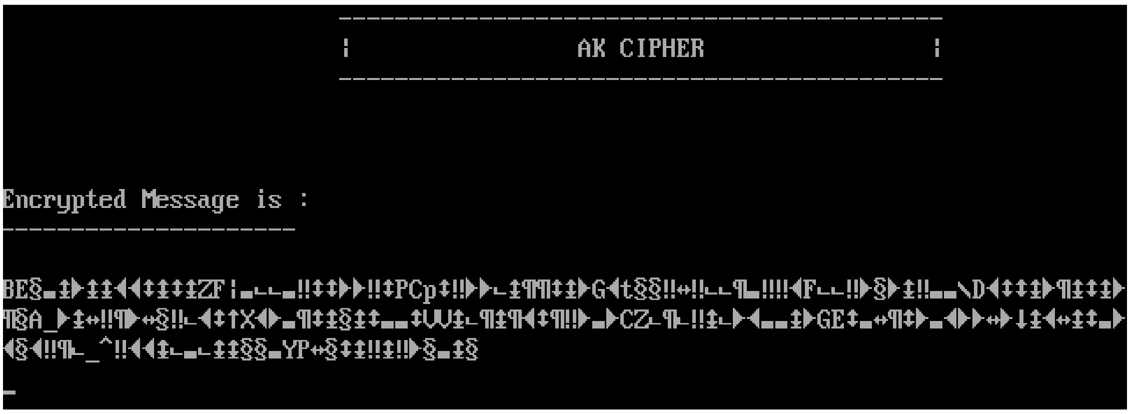
- Regardless of the plain text message (In case of Short Message)then also it is complex to determine the Key Value, therefore enforces high level security.
- Even the interception of messages of the same length is also not possible at predict at all.

EXPERIMENTAL RESULTS



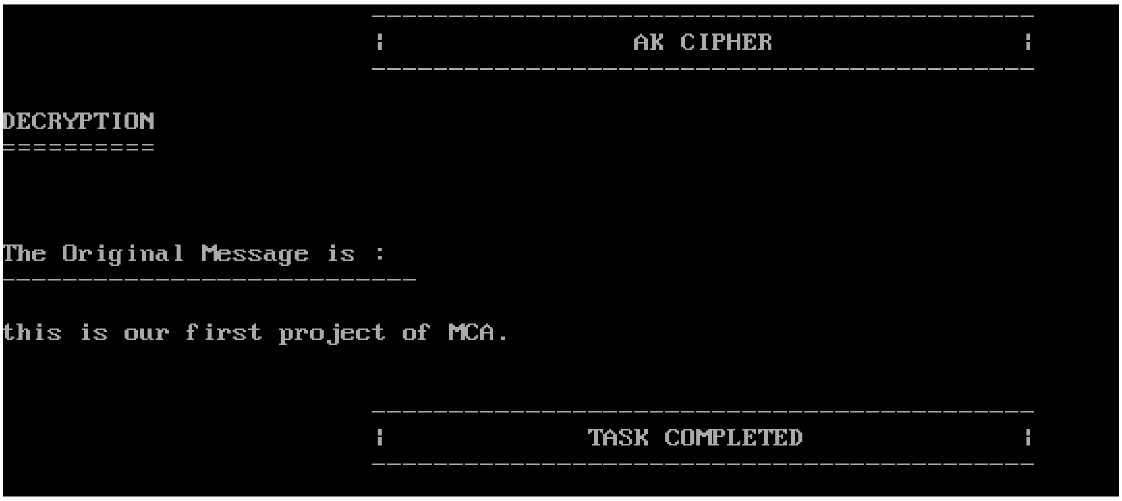
```
                        ---------------------------------------------
                        ¦                AK CIPHER                  ¦
                        ---------------------------------------------

ENCRYPTION
==========

Welcome User!!! Type Hello :
-----------------------------
hello computer

Enter the Message to Send :
-----------------------------
this is our first project of MCA.

Enter the key(Enter Any Digits From 0-9) :
-------------------------------------------
675234


                        PLEASE WAIT,MESSAGE IS ON ITS WAY TO ENCRYPT
                                         ..._
```

Figure 2



```
                      ----------------------------------------
                      ¦              AK CIPHER               ¦
                      ----------------------------------------



Encrypted Message is :
-------------------

BE§▬↨►↨↨◄◄↕↨↕↨ZF¦▬∟∟▬‼↕↕►►‼↕PCp↕‼►►∟↨¶¶↕↨►G◄t§§‼↔‼∟∟¶▬‼‼◄F∟∟‼►§►↨‼▬▬\D◄↕↕↨►¶↨↕↨►
¶§A_►↨↔‼¶►↔§‼∟◄↕↑X◄►▬¶↕↨§↨↕▬▬↕VV↨∟¶↨¶◄↕¶‼►▬►CZ∟¶∟‼↨∟►◄▬▬↨►GE↕▬↔¶↕►▬◄►►↔►↓↨◄↔↨↕▬►
◄§◄‼¶∟_^‼◄◄↨∟▬∟↨↨§§▬YP↔§↕↨‼↨‼►§▬↨§
_
```

Figure 3



```
                        ------------------------------------------
                        ¦                AK CIPHER               ¦
                        ------------------------------------------

DECRYPTION
==========


The Original Message is :
---------------------------

this is our first project of MCA.


                        ------------------------------------------
                        ¦             TASK COMPLETED             ¦
                        ------------------------------------------
```

Figure 4

CONCLUSIONS

In today's fast growing digital world, the protection of any private or the personal data is very important to any user of modern computer technology that stores or process the information in the number of ways. Security and information secrecy is being handled efficiently by different algorithms which have their own ethics. Inclusion of the above technique may counter the clever hackers and unauthenticated users from logging in. This shall overcome the problem of breach of confidential information with the innovative concept AK Cipher has come up with. The result defines a complete security and integrity of entered message using new encryption technique. This technique will lead to the safer passing of confidential information between the end users.

REFERENCES

1. http://www.nbcnews.com/id/47911119/ns/technology_and_science-security/t/why-you-need-use-encrypted-email/#.Vb9dmfmqqko
2. Introduction to Computer Security *by Charles P.Fleeger*, *Fourth Edition, Pearson Education*
3. http://courses.cs.vt.edu/~cs5204/fall00/protection/rsa.html
4. http://practicalcryptography.com/ciphers/columnar-transposition-cipher/
5. http://www.cs.uri.edu/cryptography/classicaltransposition.htm
6. http://etutorials.org/Networking/Router+firewall+security/Part+II+Managing+Access+to+Routers/Chapter+3.+Accessing+a+Router/Types+of+Authentication/
7. Information Security: The Complete Reference, Second Edition, Mark Rhodes-Ousley