A MODIFIED ATBASH CIPHER WITH SPECIAL CHARACTERS AND STACK IMPLEMENTATION

[*]Hassan, A., Mallam, N. J., Umar, A., Dakingari, A. U., Illo, Z. Z

Department of Mathematics, Federal University Birnin Kebbi

[*]Corresponding Author email: aliyu.hassan@fubk.edu.ng

Abstract:

This study presents a modified Atbash cipher that consists of special characters and utilizes a stack data structure to significantly enhance its security. The traditional Atbash cipher, which substitutes letters with their alphabetical inverses, is limited by its simplicity and vulnerability to frequency analysis attacks. To address these weaknesses, we introduce special characters into the cipher's alphabet and employ a stack to store and process the encrypted characters. Furthermore, we replace the conventional modulo 26 with modulo 31, increasing the cipher's key space and resistance to cryptanalysis. The modified cipher has improved the security and resistance to attacks, making it a more reliable choice for confidential communication. The integration of special characters and stack implementation adds complexity and depth to the encryption process, ensuring the confidentiality and integrity of sensitive information. This enhanced Atbash cipher has significant implications for secure communication and data protection.

Keywords: *Atbash cipher, encryption, decryption, algorithm, stack process.*

1. Introduction.

1.1 History and development of Atbash cipher

The ***Atbash*** Cipher is an ancient encryption technique that originated in the Middle East, specifically in the Hebrew tradition. Here's a brief history. In **500-600 BCE,** The Atbash Cipher is believed to have been used by the ancient Hebrews, possibly during the period of the First Temple. In **100-500 CE** The cipher is mentioned in the Jewish mystical text, ***Talmud***, and the Hebrew Bible (Old Testament). In **700-1000 CE,** Arab cryptographers, such as $\boldsymbol{Al-Kindi}$ and $\boldsymbol{Ibn\ ad-Durayhim}$, wrote about the Atbash Cipher in their works on cryptography. In **1200-1500 CE,** The cipher was used by Jewish mystics, including **Rabbi Bahya ben Asher**, to conceal hidden meanings in biblical texts. In **19th-20th centuries,** The Atbash Cipher was rediscovered and studied by Western cryptographers, who recognized its simplicity and historical significance. The name "Atbash" comes from the Hebrew words "**Atbash**", which means "**alphabet**," and

"***Atbash Qatan***", meaning "**small alphabet.**" This refers to the substitution of letters with their corresponding letters at the opposite end of the alphabet. Throughout its history, the Atbash Cipher has been used for various purposes, including:

a. Concealing secret messages
b. Protecting sacred texts
c. Encoding mystical meanings
d. Demonstrating cryptographic techniques

Despite its simplicity, the Atbash Cipher remains an important part of cryptographic history and continues to fascinate cryptographers and historians alike.

Terms used in cryptography:

I. Plaintext: The original message or data to be protected.
II. Cipher text: The encrypted message or data that is unreadable without decryption.
III. Encryption: The process of converting plaintext into cipher text to protect it from unauthorized access.
IV. Decryption: The process of converting cipher text back into plaintext to read or use the original message.
V. Cipher: An algorithm or technique used for encryption and decryption, like a secret code.
VI. Cryptography: The study and practice of secure communication by transforming plaintext into cipher text to protect it from unauthorized access.
VII. Security Analysis: Evaluating and testing cryptographic systems to identify vulnerabilities and ensure they are secure.
VIII. Stack: A data structure used in some cryptographic algorithms to store and transfor data temporarily.

1.2 The algebraic formula for encryption of Atbash Cipher

$$\boldsymbol{E_x = C = (25 - P) + 1} \qquad (1)$$

Where

$\boldsymbol{E_x}$ is the encryption function.

$\boldsymbol{C}$ is the ciphertext after encryption.

$\boldsymbol{P}$ is the plaintext letter (in numerical form, where $\boldsymbol{A = 0, B = 1, C = 2, \ldots, Z = 25}$

This formula works because it essentially "mirrors" the alphabet, replacing each letter with its corresponding letter at the opposite end of the alphabet. To use this formula, convert each plaintext letter to its numerical equivalent, apply the formula in equation (1) above, and then

convert the result back to a letter. For example, to encrypt the letter "H" ($\boldsymbol{A = 0, B = 1, C = 2, \ldots, H = 7, \ldots, Z = 25}$)

$$\boldsymbol{E_x = C = (25 - 7) + 1}$$

$$\boldsymbol{C = 19}$$

The letter "$\boldsymbol{S}$" is equivalent to $\boldsymbol{19}$, so the ciphertext letter is "$\boldsymbol{S}$".

Note that this formula assumes a 26-letter alphabet, where $\boldsymbol{A = 0}$ **and** $\boldsymbol{Z = 25}$.

1.3 The algebraic formula for decryption Atbash Cipher

$$\boldsymbol{D_x = P = (25 - C) + 1} \qquad (2)$$

Where:

$\boldsymbol{D_x}$ is the decryption function.

$\boldsymbol{P}$ is the plaintext letter, in numerical form, where $\boldsymbol{A = 0, B = 1, C = 2, \ldots, Z = 25.}$

$\boldsymbol{C}$ is the ciphertext letter, in numerical form, where $\boldsymbol{A = 0, B = 1, C = 2, \ldots, Z = 25}$.

This formula is the reverse of the encryption formula, and it "mirrors" the alphabet to retrieve the original plaintext letter. To use this formula in equation (2) above, convert each ciphertext letter to its numerical equivalent, apply the formula, and then convert the result back to a letter.

For example, to decrypt the letter "S" ($\boldsymbol{A = 0, B = 1, C = 2, \ldots, S = 19, \ldots, Z = 25}$.):

$$\boldsymbol{P = (25 - 19) + 1}$$

$$\boldsymbol{P = 7}$$

The letter "$\boldsymbol{H}$" is equivalent to $\boldsymbol{7}$, so the plaintext letter is "$\boldsymbol{H}$".

Note that this formula assumes a $\boldsymbol{26 - letter}$ alphabet, where $\boldsymbol{A = 0\ and\ Z = 25}$.

Here are examples of situations where the Atbash Cipher was used for security purposes, along with the interpretations.

1. Ancient Hebrew Scriptures (500 BCE): The Atbash Cipher was used to conceal secret messages and meanings in the Hebrew Bible (Old Testament). Background reason: To protect sacred texts from unauthorized interpretation and maintain spiritual secrecy.

2. French Resistance (WWII) (1940s): The Atbash Cipher was used to send encrypted messages to London, coordinating efforts and communicating with Allies. Background reason: To evade Nazi detection and ensure secure communication during wartime.

3. MI6 (British Intelligence) (WWI): The modified Atbash Cipher was used to secure communication with agents in the field. Background reason: To protect sensitive information from enemy interception and ensure operational secrecy.

4. Ancient Greek Diplomacy (300 BCE): The Atbash Cipher was used to encrypt diplomatic messages between Greek city-states. Background reason: To maintain confidentiality and prevent rival states from intercepting sensitive information.

5. Masonic Communications (18th century): The Atbash Cipher was used by Freemasons to encrypt messages and maintain secrecy within their organization. Background reason: To protect their rituals, symbols, and membership lists from outsiders and maintain the secrecy of their fraternal order.

In each of these situations, the Atbash Cipher provided a simple yet effective means of securing information and maintaining confidentiality, often in situations where secrecy was crucial for safety and success.

Here are examples of Atbash Cipher that was used to encrypt information.

1. French Resistance (WWII)

Original Message: `LIBERTE`

Encrypted Message: `OGUXJLW`

Background: The French Resistance used the Atbash Cipher to send encrypted messages to London, coordinating efforts and communicating with Allies.

Original Message: `MEET ME AT MIDNIGHT`

Encrypted Message: `GXGGX GX ZXGZXGX`

Background: The French Resistance used the Atbash Cipher to coordinate secret meetings and operations with Allied forces during World War II.

2. Masonic Communications

Original Message: `SECRET`

Encrypted Message: `GVXZRG`

Background: Freemasons used the Atbash Cipher to encrypt messages and maintain secrecy within their organization, protecting their rituals and membership lists from outsiders. In each example, the Atbash Cipher replaces each letter with its corresponding letter at the opposite end of the alphabet (A becomes Z, B becomes Y, etc.).

3. WWI Military Communication

Original Message: `ATTACK AT DAWN`

Encrypted Message: `ZGGVXG ZG OXGV`

Background: British military forces used the Atbash Cipher to encrypt tactical messages during World War I.

4. Naval Operation (WWII)

Original Message: `SHIP ARRIVES TONIGHT`

Encrypted Message: `FVMXG FVXGZXGV`

Background: Naval commanders used the Atbash Cipher to encrypt messages about ship movements and arrival times during World War II.

1.4 Review of Some Related Literatures.

Atbash cipher was extensively studied by many researchers such as Jadar (2017) and Muhammad (2021), in their studies, Atbash cipher with Autokey was studied in order to have a maximum security for securing the data over any transmission media, also, the study of improved cryptographic techniques were been studied by multiple authors, such as Massoud (2009), Kashish (2013), Yekini (2014), Rajput (2014), Shahid (2014), Pooja (2017), Sriramoju (2017), Hassan (2021), Hassan (2024), studied an improved classical cryptographic techniques and their studies provides a fundamental background into the area of modern cryptography, In another presentations, studies on cipher combination was also conducted by different authors, which include Mishra (2013), Kasturia (2017), Azzam (2017), Fahrul (2017), Alhassan (2021), Kuriakkottu (2021) and Hassan (2023) all in the process of improving cyber security against unauthorized access to data.

2.0 Materials and Method

In this work, the classical Atbash cipher table for encryption and decryption process will be expanded to include special characters which will be used to encrypt and decrypt any information of which its access to unauthorized subject will be rejected.

Table 1: Classical Atbash Cipher Table

A	B	C	D	E	F	G	H	I	J	K	L	M

0	1	2	3	4	5	6	7	8	9	10	11	12
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
M	L	K	J	I	H	G	F	E	D	C	B	A

The above table is used in Atbash cipher algorithm to encrypt a message and also decrypt the message using the same table. But a proposed modified table will be introduced in the next chapter.

2.1 Proposed Cryptosystem

In this section, a proposed cipher algorithm is introduced, which will update the classical Atbash cipher algorithm into a more resilience system, which prevents it from cyber attackers. The table below, comprises classical English letters and special characters.

Table 2: Modified Atbash Cipher Table

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
@	$	+	#	*	Z	Y	X	W	V	U	T	S	R	Q	P

Q	R	S	T	U	V	W	X	Y	Z	*	#	+	$	@
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

The above table is a modified classical Atbash cipher table which then, were used for the encryption and decryption process.

2.2 Cipher Algorithm

In this chapter, the encryption function and decryption function will be discussed.

a. Encryption Process.

The encryption process will be conducted in two steps.

Step1. Apply of stack process into the plaintext data.

Step2. Apply the encryption of modified Atbash cipher into the stacked data.

And, in algebraic representation, the encryption process can take place in the following ways.

$$C: P \rightarrow S_x \rightarrow E_x \qquad (3)$$

Where,

C Is cipher text.

P : is a plaintext.

S_x : Is stack process

E_x : Is the encryption technique of modified Atbash cipher.

$E_x = (31 - P) + 1$

b. Decryption Process

The decryption process will take place in two steps.

Step1. Apply the decryption of modified Atbash cipher into the cipher text to produce stacked data.

Step2. Reverse the stack process to produce the plaintext which will be readable when word spacing is used.

Algebraic representation, the decryption process can take place in the equation (4) below.

$$P: D_x(E_x) \rightarrow S_x^- \qquad (4)$$

Where,

$D_x(E_x)$: Is the application of modified Atbash decryption function into the cipher text which will produce stacked data.

S_x^- : Is the reversal of stack process.

P : Is the original message to be produced.

$D_x = (31 - C) + 1$

2.3 Practical Application

In this chapter a classical Atbash cipher will be used to encrypt a data and also, alternatively, the modified Atbash cipher will be used to encrypt the data and compare the results

A. Classical Atbash Cipher.

$$\boldsymbol{E_x = C = (25 - P) + 1}$$

$$\boldsymbol{D_x = P = (25 - C) + 1}$$

The above equations are used for encryption and decryption respectively.

Example. To encrypt the information below using Atbash Cipher.

PLAINTEXT: ATTACK IMMEDIATELY ON GREEN SIGNAL.

CIPHER TEXT: ZGGZXPRNNVWRZGVOBLMTIVVMHRTMZO

The above cipher text, indicate the result of applying equation (1) into the plaintext.

B. Modified Atbash Cipher

$$\boldsymbol{E_x = C = (31 - P) + 1} \quad (5)$$

$$\boldsymbol{D_x = P = (31 - C) + 1} \quad (6)$$

Equations (5) and (6) are the modified algorithm of equations (1) and (2), which will be used for encryption and decryption respectively.

Example. To encrypt the information below using modified Atbash Cipher.

PLAINTEXT: ATTACK IMMEDIATELY ON GREEN SIGNAL.

STACK: LANGISNEERGNOYLETAIDEMMIKCATTA

CIPHER TEXT: T@RYWMRNYRQGT*L@W#*SSWU+@LL@**

The above cipher text, indicate the result of applying equation (5) into the plaintext.

3. Conclusion:

This study successfully modified the Atbash cipher, rendering it resistant to frequency analysis attacks on English letters. By introducing enhancements to the traditional cipher, the modified code effectively thwarts attempts to decipher the encrypted text using frequency analysis. This achievement fulfills the primary objective of the study, significantly bolstering the security of the Atbash cipher. The modified cipher now offers improved protection against cryptanalysis, ensuring the confidentiality and integrity of encrypted information. The successful modification demonstrates the potential for enhancing classic ciphers to meet modern security demands.

4. Recommendation:

This study successfully modified the traditional Atbash Cipher, yielding a more secure ciphertext comprising alphabets and special characters. To further enhance its practicality, we recommend exploring the implementation of this improved Atbash Cipher in computer-aided programming. This would significantly streamline the encryption and decryption processes, saving time and effort. By leveraging programming capabilities, the modified Atbash Cipher can be easily integrated into digital platforms, facilitating efficient and secure communication. Moreover, computer-aided implementation would enable rapid encryption and decryption, making it an ideal solution for applications requiring swift and secure data exchange. Future studies should focus on developing user-friendly software or algorithms that can seamlessly execute the improved Atbash Cipher, paving the way for its widespread adoption in various fields. By doing so, we can unlock the full potential of this enhanced cipher and ensure the confidentiality and integrity of sensitive information in the digital era.

Reference

Alhassan, M. J; Hassan, A; Sani, S. and Alhassan, Y. (2021). A Combined Technique of an Affine Cipher and Transposition Cipher Quest Journals Journal of Research in Applied Mathematics Volume **7**. Issue **10** pp: 08-12

Azzam A and Sumarsono (2017), A Modifying of Hill Cipher Algorithm with 3 Substitution Ceaser Cipher. Proceedings International Conference of Science and Engineering, Indonesia.**1**: 157-163.

Badamasi, B. L., Sani, S., Ahmad, S. T and Hassan, A (2023). Using Big Data to Determine Potential Dropout of Students in Some Selected Tertiary Institutions in Kebbi State, Nigeria. International Journal of Innovative Science and Research Technology. ISSN: 2456-2165. **8**(10). Pp 1-6

Fahrul I, K., Hassan F, S., Toras P and Rahmat W. (2017), Combination of Ceaser Cipher Modification with Transposition Cipher. Advances in Science Technology and Engineering Systems Journal. **2**(5): 22-25.

Hassan, A (2024) A modified Ceaser Cipher. Journal of mathematical sciences and computational mathematics. doi.org/10.15864/jmscm.5304. **5(3)**:275-281.

Hassan, A., & Abdullahi, U (2024) Security analysis and modification of a Ceaser cipher. Journal of mathematical sciences and computational mathematics. doi. Org / 10. 15864 /jmscm.5304. **5(4)**:480-487.

Hassan, A., Garko, A., Sani, S., Abdullahi, U and Sahalu, S (2023). Combined Techniques of Hill Cipher and Transposition Cipher, Journal of Mathematics Letters. **1**(822) pp 1-8, DOI:10.31586/jml.2023.822

Hassan, A (2024) Analysis and modification of Viginere cipher. Journal of mathematical sciences and computational mathematics. doi. Org / 10. 15864 /jmscm.5304. **5(4)**:502-510.

Hassan, A; Alhassan, M. J; Alhassan, Y. and Sani, S. (2021). Cryptography as a Solution for a Better Security International Journal of Advances in Engineering and Management (IJAEM :**3(12)**. pp: 849-853

https://www3.nd.edu/~busiforc/handouts/cryptography/letterfrequencies.html

Jadar, C & Debashis, D (2017) Atbash cipher design for secure nano communication using QCA doi.10.1680/jnaen.16.00001.

Kashish G and Supriya K. (2013) Modified Ceaser Cipher for a Better Security Enhancement. International Journal of Computer Application.**73**:26-31

Kasturia, P and Maheswa, K (2017). Critical Analysis of Various Cryptographic Algorithms. Journal of Ultra Computer & Information Technology. **8(1)**, pp 5-9

Kuriakkottu A. R. (2021). Use of Transposition Cipher and its Types. International Journal of Research and Engineering, Science and Management **4(11)**, 164-165

Muhammad, F & Rosmini, H (2021) Perpeduan algoritma kriptografi Atbash dan autokey cipher dalam mengamankan data. Jurnal media informatika Budidarma. **5(3)**:806-812.

Pooja S and Pintu S. (2017), Enhancing security of Ceaser cipher using "Divide and Conquer Approach". International Journal of Advance Research in Science and Engineering. **6(02)**:144-150.

Rajput Y., Naik D. and Mane C. (2014), An improved cryptographic technique to encrypt Text message using double encryption. International Journal of Computer Applications **86(6)**:24-28.

Shahid B. D. (2014), enhancing the security of Ceaser cipher using double substitution method. International Journal of Computer Science and Engineering Technology. **5**: 772-774.

Sriramoju A. B (2017), modification affine ciphers algorithm for cryptography password, Programmer Analyst, Ramstad Technologies, EQT Plaza 625 Liberty Avenue, Suite 1020, Pittsburgh, Pennsylvania - 15222, USA.

Umar, M., Hassan, A., Abdullahi, I & Muhammad Shehu, Z (2024) Permutation of National Identification Number for a Better Security in Communication Channel. International Journal of Innovative Science and Research Technology ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1655. **9**(4) Pp:3096-3099

Umar, M., Hassan, A., Abdullahi, I & Muhammad Shehu, Z (2024) Transposition Cipher as a Solution for a Better Bank Verification Number (BVN) Security in Communication Channel. International Journal of Innovative Science and Research Technology ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654. Volume 9, Issue 5, pp:3090-3095

Yekini, N. A., Aigbokhann, E. E & Okiki, F. M (2014) Cryptograpgy system for online communication using polyalphabetic substitution method. International jurnal of advanced networking and applications **6(1)**:2151-2157.