

Research Article

## Cryptanalysis of Arabic Poetry, ibn Tabataba Treatise

Bushra Mohamed Elamin Elnam<sup>1</sup>, Hayder Abood S. Wsmi Al-Lami<sup>2</sup><sup>1</sup>Department of Computer Science & Information, Sattam bin Abdulaziz University, Al Sulail, Kingdom of Saudi Arabia<sup>2</sup>Department of Computer & Information, Sattam bin Abdulaziz University, Al Sulail, Kingdom of Saudi Arabia

### \*Corresponding author

Bushra Mohamed Elamin Elnam

Email: [bushra\\_moh@hotmail.com](mailto:bushra_moh@hotmail.com)

**Abstract:** Cryptography has been practiced to conceal messages science antiquity by different civilizations, including the ancient Egyptian, Chinese, Indian, Mesopotamian, Greek and Roman. But in none of them was there any cryptanalysis, only cryptography existed. Cryptology, the science of both making ciphers (cryptography) and breaking them (cryptanalysis), was born among the Arabs shortly after the rise of the Arab-Islamic empire. Many Arab scholars wrote on, and excelled in practicing, both branches of cryptology. The aim of this paper is to discuss not-widely-known ibn Tabataba contributions to cryptology in poet and his effort in this field.

**Keywords:** ibn Tabataba, Cryptanalysis of Poetry, Arab cryptology, ibn Tabataba's Treatise on Cryptanalysis, Poetry Encipherment.

### INTRODUCTION

It was stated earlier that the Arabs were the first to treat cryptography and cryptanalysis scientifically. They have written on the science of cryptology and developed it, thus becoming its founders in their own right. Kahn said in [1] that cryptology was born among the Arabs. This was confirmed by the 1980 discovery of some Arabic cryptologic treatises which were found in Istanbul's Suleymanye library [2], in addition to the works of other scholars who wrote about cryptography and cryptanalysis from the Arab Middle East, such as Al Kindi (801–873), Ibn Dunainir (1187–1229), Ibn Adlan (1187–1268), Ibn ad-Duraim (1312–1361), and Al-Qalqashandi (1355–1418). All these works were written by learned men from the Abbasid, Ayyubid, Mamluk, and Ottoman Empires [3, 4].

Cryptology, the science of both making ciphers ( cryptography) and breaking them ( cryptanalysis), was born among the Arabs shortly after the rise of the Arab-Islamic empire. Many Arab scholars wrote on, and excelled In practicing, both branches of cryptology [3].

In this paper discussion to ibn Tabataba contributions in cryptology and his effort in this field from his Treatise has been explained.

### ABOUT IBN TABATABA'S LIVE

Muhammad ibn 'Ahmad ibn Muhammad ibn 'Ahmad ibn 'Ibrahim Tabataba al-Alawi Abu al-Hasan was born in Isfahan and died there in AH 322/AD 934. Sources do not give detailed accounts of his life, but they are agreed that he was a leading literary authority, and a great poet and researcher. A renowned personality of widely-circulating poetry, he was well known for his intelligence, sagacity, serenity of mind, and seriousness of purpose [5].

### ABOUT IBN TABATABA'S WORKS

ibn Tabataba has left a number of works that tend primarily towards poetry, literature and the like. The following are the most important of his books:

- *Iyar as-si'r* (The Standard of Poetry): A book on literary criticism. Hailed by editors as significant, it has been printed and published several times, the most recent of which was in Riyadh 1985.
- *Tahdib at-tab* (Refinement of Taste): Includes an interesting poetic anthology, of his own selection, of the works of other poets.



(5) Looking out for letters that go together, such as ( ل ) and ( ج ). For example, a message ciphered using bird names, in which the letter ( ل ) is represented by "sparrow" and the ( ج ) by "crow", would have the twosome "sparrow crow" recurring more often than any else [11].

(6) Seeking three-letter and four-letter words (trigrams and tetra grams) with the letters ( ل ) and ( ج ), for the identification of these letters in a word would probably lead to the identification of the whole word [11].

(7) Pursuing two-letter words (bigrams), such as the particles: مذ, أو, من; عن, etc. ; and imperative verbs, e.g. سل, دع, خذ, etc. Note here that al-Kindi has already indicated the importance of the occurrence frequency of bigrams or the so-called contact count [11].

(8) Tracing long words along the lines of long poetic meters such as مفاعلات, استفعال, and the like [11].

(9) Making use of the beginning of the second hemistich, so far made out, in determining the conjunctions ( و ) and ( ف ) if the context suggests words joined by means of conjunctions [12].

(10) Approximation of vocalized and neutral beats, based on the letters already identified, thus establishing a criterion for assessing the metrical measure of the cipher verse. The criterion is supposed to be equal to the letter count; otherwise the analogy should be changed over until the criterion fits the cipher exactly and evenly. By the criterion ibn Tabataba probably means scansion, i.e. the practice of marking off lines of poetry into metrical units known as feet, expressing the foot segments of a verse in terms of their metrically corresponding vocalized and neutral beats (e.g. فعولن //o/o) [12].



(11) Applying the previous criterion in revealing intractable letters, through matching it up against the letters of the alphabet until it accords closely with the intended meter, and the word is written accordingly. ibn Tabataba warns the cryptanalyst here not to focus all his/her attention on certain letters at the expense of other letters, because "that is likely to protract your toil and disrupt your execution," he says, maintaining that "cracking one letter often serves as a key by which to pierce through other letters that are still unresolved." [13].

(12) Making full use of the Arabic syntax, which calls for certain succession that is *sine qua non* for correct wording in Arabic. For example:

- A relative pronoun (e.g. الذي) requires an antecedent.
- Letters specific to verbs are not followed by nouns.
- Letters specific to nouns are not followed by verbs.
- Adverbs of time and place require the nouns by which they are governed, or to which they are annexed.
- Positions of nouns, verbs, and particles should be observed in context. ibn Tabataba notes that confusion of meaning and structure in poetic ciphers, as well as non-observance of what is easy and familiar, would in all probability lead to difficult cryptanalysis [12].

(13) Utilization of the special order of letters dictated by unusual poetic necessities. This is what is termed by Arabic language scholars "poetic license" —the acceptable deviation, on the part of the poet, from rule or conventional form of poetry to produce the desired effect, such as the use of trip tote where diptote is typically appropriate; e.g.

اعددت للحرب التي أعني بها قوافياً لم أعني باجتلابها

where the word قوافياً is used instead of the syntactically correct form

قوافي, to set up the meter. Another example is the use of a prolonged "alif" where a shortened one ought to be used, or vice versa:

سُغِنِبِنِي الَّذِي اغْنَاكَ عَنِي فَلَا فَقْرَ يَدُومُ وَلَا غِنَاءَ

in which the word ( غناء ) should have been ( غنى ), in proper Arabic [14].

(14) Trying all over again in case one letter only remains obscure of the cipher verse.

(15) ibn Tabataba sums up three requisites for efficacy in poetry cryptanalysis, i.e.:

- a. acquaintance with the general texture and constitution of the Arabic word (letter combinability), the frequently used words and those less or never used.
- b. familiarity with the Arabic syntax and grammar.
- c. adequate knowledge of versification and metrical patterns [14].

### METHODS OF ENCIPHERMENT BY SIMPLE SUBSTITUTION

Although ibn Tabataba's treatment of encipherment does not generally cut across a single type, i.e. simple substitution, it can be classified into three categories:

a) Substitution of certain generic names for letters: Of these genera he mentions birds, beasts, people, aromatic plants, tools and instruments, jewellery, etc [14].

b) Encipherment by bead threading, mentioned later by ibn Dunaynir [15].

ibn Tabataba's reference to this method here is an indication to its popularity in the fourth century of the Hegira (Ninth AD), i.e. two centuries prior to ibn Dunaynir [16].

c) Picturing different marks, through devising special signs and symbols substituted for letters, such as those used by ibn ad-Durayhim in his two practical examples [17]. To be noted is that ibn Tabataba never touches upon any of the many encipherment methods treated by his predecessor al-Kindi; he rather restricts himself to simple substitution in its simplest varieties, with the employment of word-spacers [18].

### AN EXAMPLE OF POETRY ENCIPHERMENT

The example given by ibn Tabataba concerns itself with the encipherment of a well-known line of poetry by 'Imru' al-Qays:

قفا نَبِك من ذكرى حبيبٍ ومنزل      بسقط اللوى بين الدخول فَحَوْمَل

by simple substitution (category (a) above). Encipherment has been performed as follows:

**Table 1: shows the Encipherment of of poetry by 'Imru' al-Qays**

Letter	Bird Name	Letter	Bird Name
ق	peacock	ي	Buzzard
ف	pheasant	ح	Crow
ا	Hawk	و	Raven
ن	falcon	ز	Francolin
ب	harrier	ل	Grouse
ك	merlin	س	Bobwhite
م	Eagle	ط	Ringdove
ذ	Saker	د	Pigeon
ر	vulture	خ	Duck

It is worthy to remark that the arrangement of bird names has suffered confusion in the cipher text of the original manuscript, probably owing to a scribe's omission. However, the arrangement has been set right here in light of the plaintext as follows: peacock pheasant hawk falcon harrier Merlin eagle falcon saker merlin vulture buzzard crow harrier buzzard harrier raven eagle falcon francolin grouse harrier bobwhite peacock ringdove hawk grouse grouse raven buzzard harrier buzzard falcon hawk grouse pigeon duck raven grouse pheasant crow raven eagle grouse, the number of names is identical to the number of letters of the verse( i.e.44 ) [19].

### MANAGEMENT OF POETRY ENCIPHERMENT

By this management is meant the placement of cipher words on an endless circle, from which all poetical meters relevant to that circle disengage themselves, provided that those words are capable of such disengagement. Also the first word of the cipher verse is not identified each word of it is a potential start.

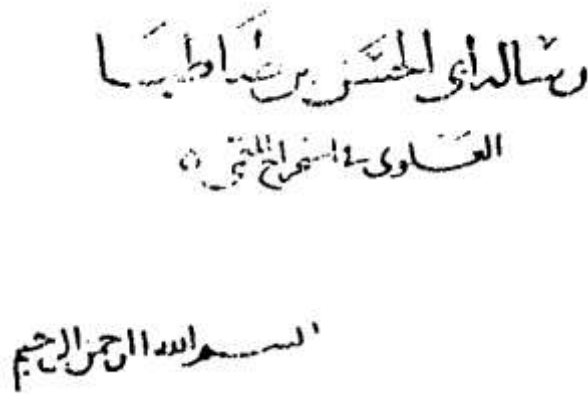
ibn Tabataba illustrates his point with a verse whose composition and metrical units fit in quite harmoniously with the meters peculiar to the circle of the similar. This is the third of the metrical circles, so named because all its parts are similar seven-bit feet adding up to 21 bits in all. Three meters develop or emanate from this circle, i.e. hazag , ragaz and ramal, as shown in the following figure [19];



Likewise, skipping the second syllable prompts the emergence of the third alternative (ramal) whose letters are written next to the second starting from the third syllable. This verse is:  
 ماجدٌ بحرِ جَوَادٍ سابقِ بدرِ كريمِ

ibn Tabataba stresses the point that in this type of cipher, letter cryptanalysis should be performed before looking out for the meter. He maintains that meter may straighten by whatever word it starts something likely to cause ambiguity to the cryptologue through driving him/her to mistakenly believe that their cryptanalysis is correct as long as the meter is sound, while in fact it is not. The previous example is a case in point [21].

**PHOTOCOPIES OF IBN TABATABA'S TREATISE**



**Fig-3: A photocopy of the title page of ibn Tabataba's Treatise**  
 (Document No. 5300, as-Sulaym niyya Ottoman Archives, Istanbul, Turkey)[22]



**Fig-4: A photocopy of the first page of ibn Tabataba's Treatise**  
 (Document No. 5300, as-Sulaym niyya Ottoman Archives, Istanbul, Turkey)[23]



**Fig-5: A photocopy of the last page of Ibn Tabataba's Treatise**  
 (Document No. 5300, as-Sulaym niyya Ottoman Archives, Istanbul, Turkey)[24]

**CONCLUSIONS**

There were some discoveries about Arab Contributions in Cryptography especially in poet . Here we have described Ibn Tabataba's Treatise , but there remain a lot more to discover in our academic libraries, personal libraries, and also in all places where our Arabic cultural treasures are still imprisoned.

Ibn Tabataba's Treatise on Cryptanalysis can be divided into five chapters as follows:

1. Tools for cryptanalyzing prose and poetry.
2. Cryptanalysis of poetry ciphers.
3. Methods of encipherment by simple substitution.
4. An example of poetry encipherment.
5. Management of poetry encipherment.

Ibn Tabataba , the author of this treatise, is a poet of great note who practiced the art of encipherment in his poetry, and was reported to have left special poetic selections in cipher. The reader will immediately realize that this treatise is so straightforward and brief that it only just needs any further elaboration. It is sufficient therefore to state the most remarkable views covered by Ibn Tabataba in each chapter, highlighting the relevant technical terms in the edited text.

**REFERENCES**

1. Kahn D. The Code breakers: The Story of Secret Writing. New York: Macmillan, 1967.
2. Schwartz KA. Charting Arabic Cryptology's Evolution," Cryptologia. 2009;33:297–304.
3. Al-Kadi IA. Origins of Cryptology: The Arab Contributions," Cryptologia. 1992;16(2):97–126.
4. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M.( 2002-2007) Series on Arabic Origins of Cryptology Volumes 1-6, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia.
5. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry: page 5, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia, 2006.
6. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry: page 7, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia, 2006.
7. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Two: Ibn Adlan's Treatise *al-mu'allaf lil-malik al-'Asraf* pages: 19,21,58 and 80, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2003.
8. Mrayati M, Meer AY, At-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology, Volume Three: Ibn ad-Durayhim's Treatise on Cryptanalysis: page 32,King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, and Mrayati, M., Alam, Y. Meer and at-Tayyan, M. H. Translated by al-Asaad, Said M.( 2005) Series on Arabic Origins of Cryptology Volume Four: Ibn Dunaynir's Book: Expositive Chapters on Cryptanalysis(Maqasid al-Fusul al-Mutargima an all at-Targama) pages: 22-25,King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia.

9. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume One: al-Kindi's Treatise on Cryptanalysis : page 100, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2002.
10. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five:Three Treatise on Cryptanalysis of Poetry : page 76, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
11. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five:Three Treatise on Cryptanalysis of Poetry : page 9, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
12. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five:Three Treatise on Cryptanalysis of Poetry : page 10, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
13. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 34, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
14. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five:Three Treatise on Cryptanalysis of Poetry : page 11, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
15. Mrayati M, Meer AY, At-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Four: ibn Dunaynir's Book: Expositive Chapters on Cryptanalysis(Maqasid al-Fusul al-Mutargima an all at-Targama): page 44 and page 134,King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2005.
16. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 12, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
17. Mrayati M, Meer AY, At-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology, Volume Three: ibn ad-Durayhim's Treatise on Cryptanalysis: pages102 and 116 ,King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2003.
18. Mrayati M, Meer AY, At-Tayyan MH. Translated By Al-Asaad, Said M. Series On Arabic Origins Of Cryptology Volume Five: Three Treatise On Cryptanalysis Of Poetry : Page 12, King Faisal Center For Research And Islamic Studies And King Abdulaziz City For Science And Technology , Kingdom Of Saudi Arabia, 2006.
19. Mrayati M, Meer AY, At-Tayyan MH. Translated By Al-Asaad, Said M. Series On Arabic Origins Of Cryptology Volume Five: Three Treatise On Cryptanalysis Of Poetry : Page 13, King Faisal Center For Research And Islamic Studies And King Abdulaziz City For Science And Technology , Kingdom Of Saudi Arabia, 2006.
20. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 14, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
21. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 15, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
22. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 20, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
23. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 21, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.
24. Mrayati M, Meer AY, at-Tayyan MH. Translated by al-Asaad, Said M. Series on Arabic Origins of Cryptology Volume Five: Three Treatise on Cryptanalysis of Poetry : page 22, King Faisal Center for Research and Islamic Studies and King Abdulaziz City for Science and Technology , Kingdom of Saudi Arabia, 2006.