Arabic Origins of Cryptology

(The discovery of Ancient Manuscripts)

University of Oxford, April 26th 2018

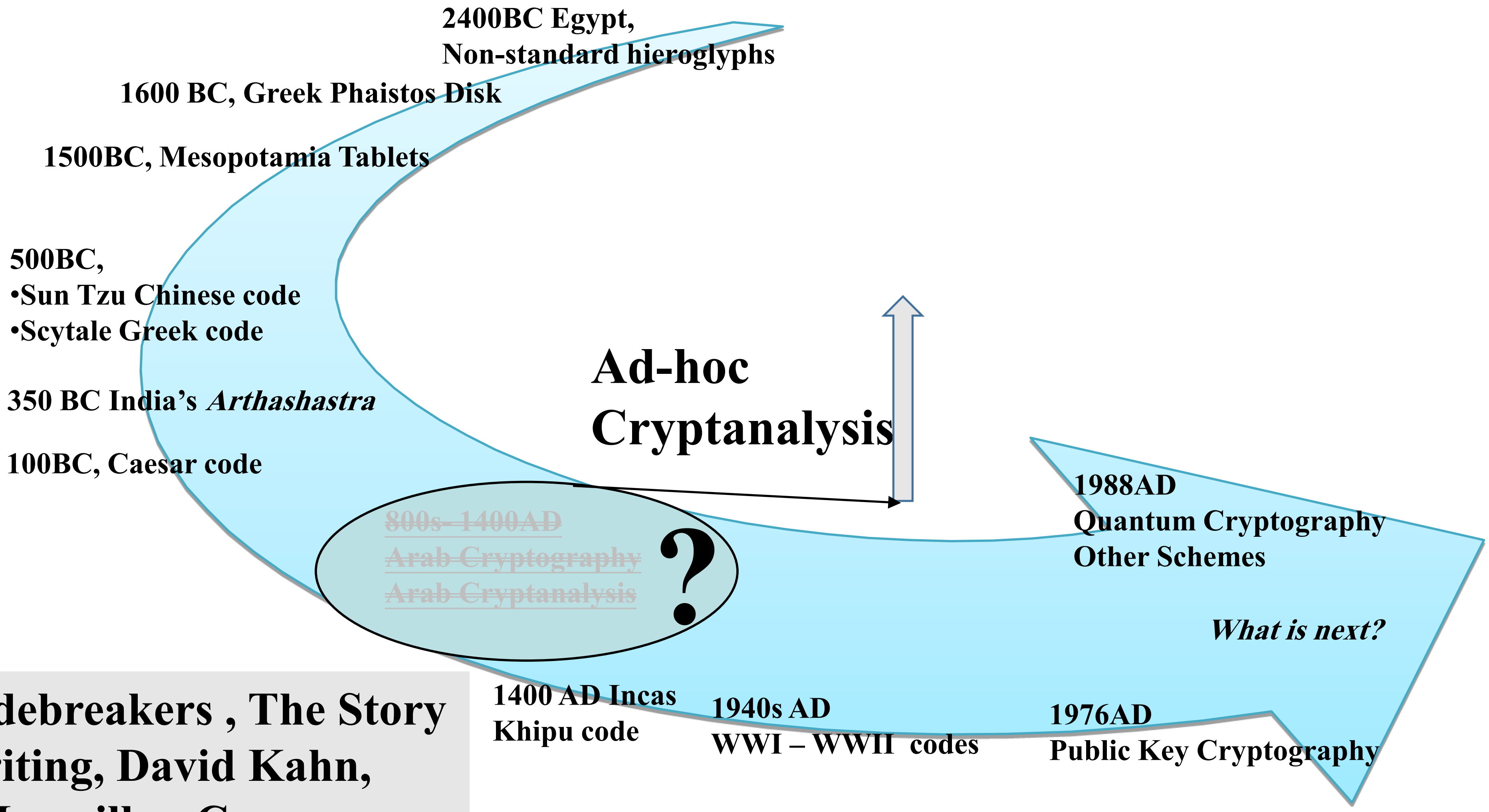
Mohammed I. Al-Suwaiyel
King Abdulaziz City for Science and Technology,
Riyadh, Saudi Arabia

Why Use Cryptology?

We all use Cryptography every day!

Historical Milestones in Cryptology

Encryption is as old as civilization



2400BC Egypt,
Non-standard hieroglyphs

1600 BC, Greek Phaistos Disk

1500BC, Mesopotamia Tablets

500BC,

- Sun Tzu Chinese code
- Scytale Greek code

350 BC India’s *Arthashastra*

100BC, Caesar code

~~800s- 1400AD~~
~~Arab Cryptography~~
~~Arab Cryptanalysis~~

?

Ad-hoc
Cryptanalysis

1400 AD Incas
Khipu code

1940s AD
WWI – WWII codes

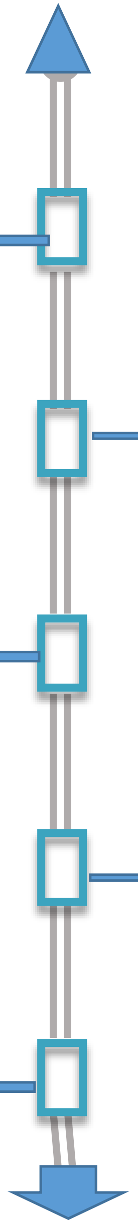
1976AD
Public Key Cryptography

1988AD
Quantum Cryptography
Other Schemes

What is next?

See: The Codebreakers , The Story of Secret Writing, David Kahn, 1967, The Macmillan Company

A Prelude



1353 AD

مفتاح الكنوز في إيضاح المرموز

Ali ibn ad-Durayhim wrote the book *“Miftah A-Kunuz fi Idah Al-Marmuz”*, (Key to Treasures on Clarifying Ciphers). The book is a major reference on Cryptology at the time.*

1412 AD

صبح الأعشى في صناعة الانشاء

Shihab al-Din al–Qalqashandi wrote on Cryptology in his encyclopedic manual for the secretaries “*Subh Al-A’sha fi Sina’at Al-Insha”.* (The Dawn of the Blind in the Writing Industry). He included “a section on codes” mostly from the book by **ibn ad-Durayhim**.

1963 AD

Clifford Bosworth, of the University of St, Andrews wrote an article in which he translated “The Section on Codes” in al -Qalqashandi's *Subh al-a‘shā*,”, and added a commentary on Arabic cryptology. **.

1967 AD

David Kahn, a prominent historian of cryptology, read the article by Bosworth, and described it as: **“perhaps the most important single article on the history of cryptology”.** * Kahn felt sorry that ibn ad-Durayhim’s book was lost at the time!

1967 AD

David Kahn wrote **"Cryptology was born among the Arabs. They were the first to discover and write down the methods of cryptanalysis.”** *

***The Codebreakers , The Story of Secret Writing, David Kahn, 1967, The Macmillan Company**

****Journal of Semitic Studies, VIII (Spring, 1963), 17-33**

The Discovery of 15 Ancient Arabic Manuscripts on Cryptology

- Some western scholars did not agree with Kahn’s statement, especially when there was no trace of ibn ad-Durayhim’s book!

- In 1979, Drs. M. Mrayati, Y. Alam and M. al-Tayyan, from the Arab Academy of Damascus, decided to verify the truth of Kahn’s statement and look for ibn ad-Durayhim’s lost book*.

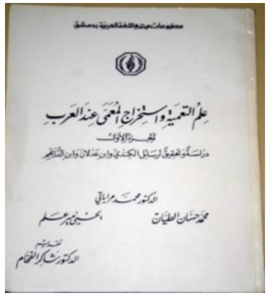
- Dr. Mrayati and his team **discovered** a treasure!! Not only they found **ibn ad-Durayhim’s book**, but they also discovered more than 15 Arabic manuscripts on Cryptology written by Arab Scholars in the period 2nd to 8th Hijri centuries, i.e. 9th to 15th centuries AD.

800s- 1400sAD
Arab Cryptography
Arab Cryptanalysis
?

*An interesting account of their journey in Arabic can be found at: http://www.alukah.net/library/0/843/

The Discovery of 15 Ancient Arabic Manuscripts on Cryptology

- In 1987 Dr. Mrayati and his team edited and analyzed 15 manuscripts; and published them in 900 pages as two volumes in **Arabic.***



مطبوعات مجمع اللغة العربية بدمشق

علم التعمية واستخراج المعمى عند العرب

الجزء الأول

دراسة وتحقيق لرسائل الكندي وابن عدلان وابن الدريهم

الدكتور محمد مرياتي

محمد حسان الطيان يحيى مير علم

تقديم
الدكتور شاكر الفحام

- In 2002 the King Abdulaziz City for Science and Technology, KACST, sponsored the translation of these 15 manuscripts into English, and started to publish them in **nine volumes** in collaboration with the King Faisal Center for Research and Islamic Studies, KFCRI. (**Volumes 1 – 6 already published**)

مطبوعات مجمع اللغة العربية بدمشق

علم التعمية واستخراج المعمى عند العرب

«التشفير وكسر الشفرة»

الجزء الثاني

دراسة وتحقيق لثماني رسائل مخطوطة

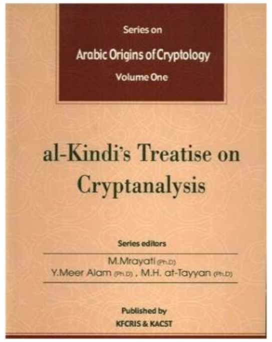
الدكتور محمد مرياتي

الدكتور يحيى مير علم الدكتور محمد حسان الطيان

تقديم
الأستاذ الدكتور شاكر الفحام

- The discovered manuscripts clearly:

1. Showed that the Arabs laid the formal foundations of Cryptology as a science,
2. Proved beyond any doubt Kahn's statement,
3. Corrected the history of Cryptology and Pushed back its origins by more than five centuries.



Series on
Arabic Origins of Cryptology
Volume One

al-Kindi's Treatise on Cryptanalysis

Series editors
M.Mrayati (Ph.D)
Y.Meer Alam (Ph.D) , M.H. at-Tayyan (Ph.D)

Published by
KFCRIS & KACST

* The two Arabic volumes can be downloaded, free of charge from KACST at: http://publications.kacst.edu.sa/SystemFiles/Books_Pdf/300.pdf

The Translated Manuscripts on Cryptology*

Volume	Manuscript
١ ـ رسالة في استخراج المعمى	**Ya'qub al-Kindi's** Treatise "*Risalah fi Istikhraj al Mu'amma*", (Treatise on Decrypting Cryptographic Messages). The oldest extant manuscript on cryptanalysis **written in the 9th** century AD. The manuscript is **about 1200 years old!**
٢ ـ رسالة في حل التراجم	**Ali ibn Adlan** Treatise "*al Mu'allaf Lil Malik al Ahraf*". (A Manual for King al-Ashraf) , a real manual of cryptanalysis written at the beginning of the 13th century AD.
٣ ـ مفتاح الكنوز في إيضاح المرموز	**Taj ad-Din ibn ad-Durayhim's** Treatise *"Miftah A-Kunuz fi Idah Al-Marmuz"*, (Key to Treasures on Clarifying Ciphers). which covered the bulk of information known of this science at the mid of the 14th century AD.
٤ ـمقاصد الفصول المترجِمة عن حل الترجمة	**Ibrahim ibn Dunaynir** Treatise "*Maqasid al-fusul al-mutarjima an Hall at-tarjama*", (Expositive chapters on cryptanalysis). A large and elaborate treatise on cryptology. It was written at the beginning of the 13th century.

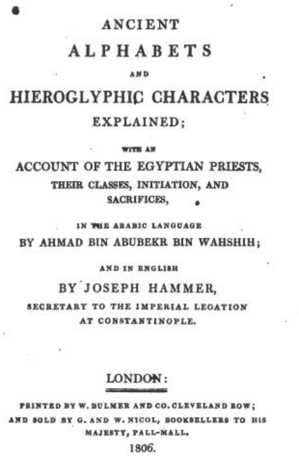
- ***Arabic Origins of Cryptology – Volumes 1 – 6, M. Mrayati et al.*** *KACST and KFCRI* ***2003 - These volumes can be downloaded from*** ***http://publications.kacst.edu.sa/SystemFiles/Books_Pdf/302.pdf***

The Translated Manuscripts on Cryptology*

Volume	Manuscript
5- رسائل استخراج المعمى من الشعر والنثر	➢ **Ibn Tabataba,** 322AH / 934 AD, wrote a treatise on Cryptanalysis *"Risalat Istikhraj al-Muamma min al-Shiir",* (A Treatise on Cryptanalyzing Poetry) ➢A Treatise on the Cryptanalysis of Poetry by the author of "*Adab al Shuaara*", (The Art of Poets), written 350 – 627 AD. ***Author name unknown*** ➢Two manuscripts by **Muhammad al-Gurhumi**, on Poetry Cryptanalysis, and on Prose Encryption: *"Kitab al-Gurhumi", (The book of al-Gurhumi),* and *"Risalat al–Gurhumi",* (al-Gurhumi Treatise).
6- رسالتان في حل التراجم البسيطة والمعقدة - رسالة البرهان في وجوه البيان لابن وهب الكاتب	➢ "*The two essays*" on cryptanalysis, written 350 – 627 AD, **author unknown.** ➢ **ibn Wahab Alkatib** 10th century treatise "*al-Burhan fi Wujuh al-Bayan*", (Demonstration of Eloquence Aspects), on Encryption and Cryptanalysis.

* *Arabic Origins of Cryptology – Volumes 1 – 6, M. Mrayati et al. KACST and KFRIS 2003 – …*
These volumes can be downloaded from http://publications.kacst.edu.sa/SystemFiles/Books_Pdf/302.pdf

The Translated Manuscripts on Cryptology (Three Volumes not Published Yet)

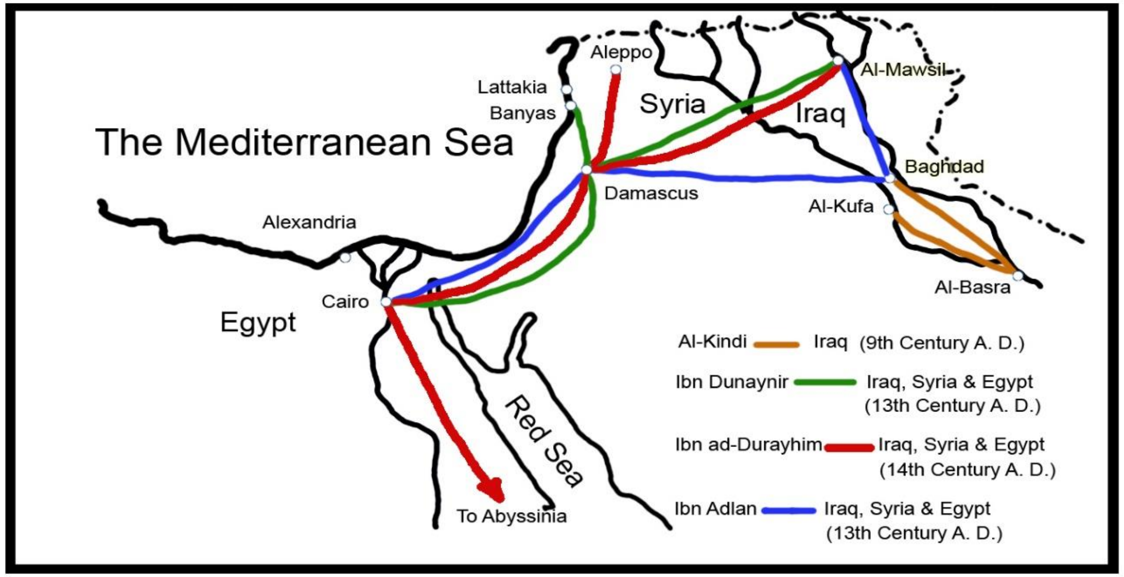
Volume	Manuscript
7 شوق المستهام في معرفة رموز الأقلام	Ahmad ibn Wahshiyyah, 291 AH / 914 AD, wrote *“Shawq al Mustaham fi Ma’rifat Rumuz al-Aqlam”*, (Seekers Joy in Learning about Other Languages written Symbols). He identified 93 alphabets and symbols, among them Hieroglyphics. He decoded about half of the Hieroglyphic alphabet, and noted that the symbols could represent sounds and meaning.
 ANCIENT ALPHABETS AND HIEROGLYPHIC CHARACTERS EXPLAINED; WITH AN ACCOUNT OF THE EGYPTIAN PRIESTS, THEIR CLASSES, INITIATION, AND SACRIFICES, IN THE ARABIC LANGUAGE BY AHMAD BIN ABUBEKR BIN WAHSHIH; AND IN ENGLISH BY JOSEPH HAMMER, SECRETARY TO THE IMPERIAL LEGATION AT CONSTANTINOPLE. LONDON: PRINTED BY W. BULMER AND CO. CLEVELAND ROW; AND SOLD BY G. AND W. NICOL, BOOKSELLERS TO HIS MAJESTY, PALL-MALL. 1806.	This manuscript was discovered earlier by Joseph Hammer in 1806. He wrote: “Though according to the Arabic title it is supposed to contain only the explanation of unknown alphabets, it gives beside a *key to the hieroglyphics*” *See page iv of: Ancient Alphabets and Hieroglyphic Characters Explained. A Translation of the Arabic Book by Ahmad ibn Wahshih, Joseph Hammer. Bulmer and Company, London, 1806.*

The Translated Manuscripts on Cryptology (Three Volumes not Published Yet)

Volume	Manuscript
8-9 - الحروف المتفرقة - - درة الغواص وكنز الاختصاص في أسرار الخواص حل الرموز ـــ وبراء الاسقام في كشف أصول اللغات والأقلام	➢ Three manuscripts on cryptanalysis, the first written by unknown author, and the second written by ibn Maslamah in 216 AH / 850 AD, and the third titled "al *Huroof al Mutafarriqah*", (The Separated Letters), written by Abu al-Qassem al- Iraqi. Date unknown. Al-Iraqi identified 70 alphabets and symbols ➢ A manuscript by Thoban al-Misri titled *"Hall ar-rumuz wa bara' al-'asqam fi kashf 'usul al-lughat wa al-aqlam"*, (Solving Symbols and curing sicknesses in clearing the origins of the Languages of the pens). He identified 200 alphabets and symbols. ➢ A section on Cryptography by Ali al-Jildaki titled *"Durrat al ghawwass wa kanz al ikhtissass fi asrar al khawass"*, (The diver's Pearl and the special treasure on the secrets of the qualities).

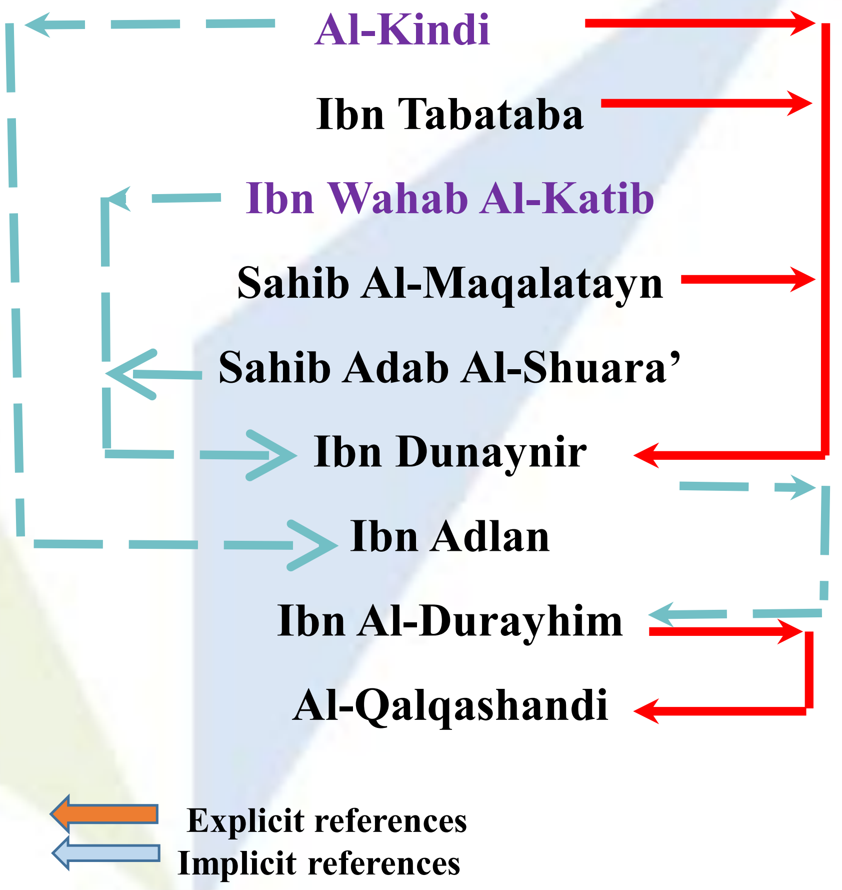
The Arab School on Cryptology

This Cryptology work was not an individual effort. The Arab scholars formed a **“School”** of Cryptology that thrived for centuries. The scholars learned from each other, built on others works, and added their own original contributions. They were very mobile, and travelled across today’s Iraq, Syria, **Egypt** and reached Abyssinia



Aleppo
Al-Mawsil
Lattakia
Banyas
Syria
Iraq
The Mediterranean Sea
Baghdad
Damascus
Al-Kufa
Alexandria
Al-Basra
Cairo
Egypt
Red Sea
To Abyssinia
Al-Kindi Iraq (9th Century A. D.)
Ibn Dunaynir Iraq, Syria & Egypt (13th Century A. D.)
Ibn ad-Durayhim Iraq, Syria & Egypt (14th Century A. D.)
Ibn Adlan Iraq, Syria & Egypt (13th Century A. D.)

Died in		Name of Manuscript Author
AH	AD	
260	873	Al-Kindi
322	934	Ibn Tabataba
350	961	Ibn Wahab Al-Katib
?		Sahib Al-Maqalatayn
?		Sahib Adab Al-Shuara’
627	1230	Ibn Dunaynir
666	1267	Ibn Adlan
762	1361	Ibn Al-Durayhim
821	1418	Al-Qalqashandi



The Beginning of the Arab Cryptology Works

- al-Kindi's Treatise, shows that the Arabs interest in their language led them to study aspects that aid in Cryptology like Linguistics, combinatorics and statistics of the Arabic alphabet and words.* The linguist al-Farahidi, (100 – 170 AH / 718 - 786 AD), used principles of ***permutations and combinations*** to list all possible Arabic words with and without vowels in his Arabic dictionary Al-Ayn

- Arab contributions to Mathematics, Astronomy and other Sciences have been studied extensively. The Arabs **translated and enriched** these sciences.

- Cryptology as a science **was not translated into Arabic.** **It was completely developed** by the Arabs. It received the least attention from historians, possibly because Cryptology is one of the secret sciences about which writings are rare with very limited circulation.

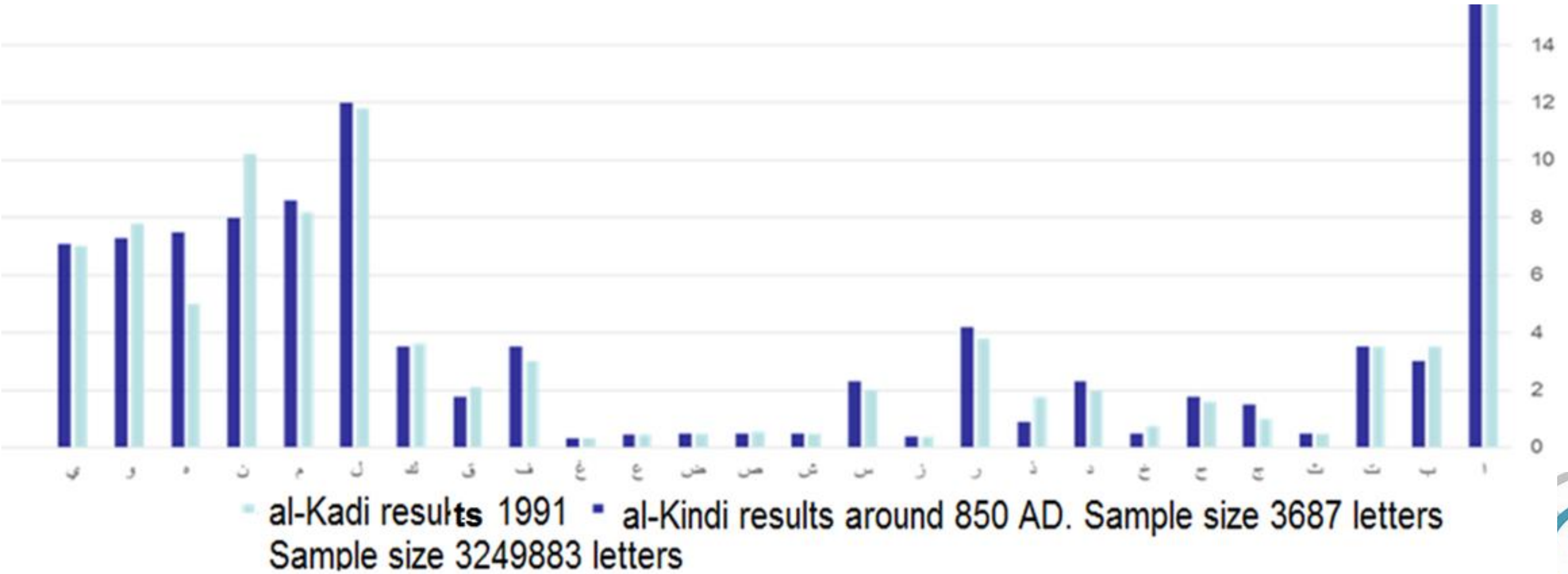
- An important seed of the Arab Cryptology works was the translation of encrypted texts in "secret" sciences like Alchemy and Magic and dead languages and communicating via poetry.

** Lyle D. Broemeling (2011) An Account of Early Statistical Inference in Arab Cryptology, The American Statistician, 65:4, 255-257, DOI: 0.1198/tas.2011.10191*

Originality of the Arab Cryptology Works

al-Kindi calculated the frequency of letters in Arabic using a text of 3667 letters, and then introduced the technique of code breaking that was later to be known as 'frequency analysis'. *

Arabic Letters Frequency by al-Kindi vs Recent Statistics

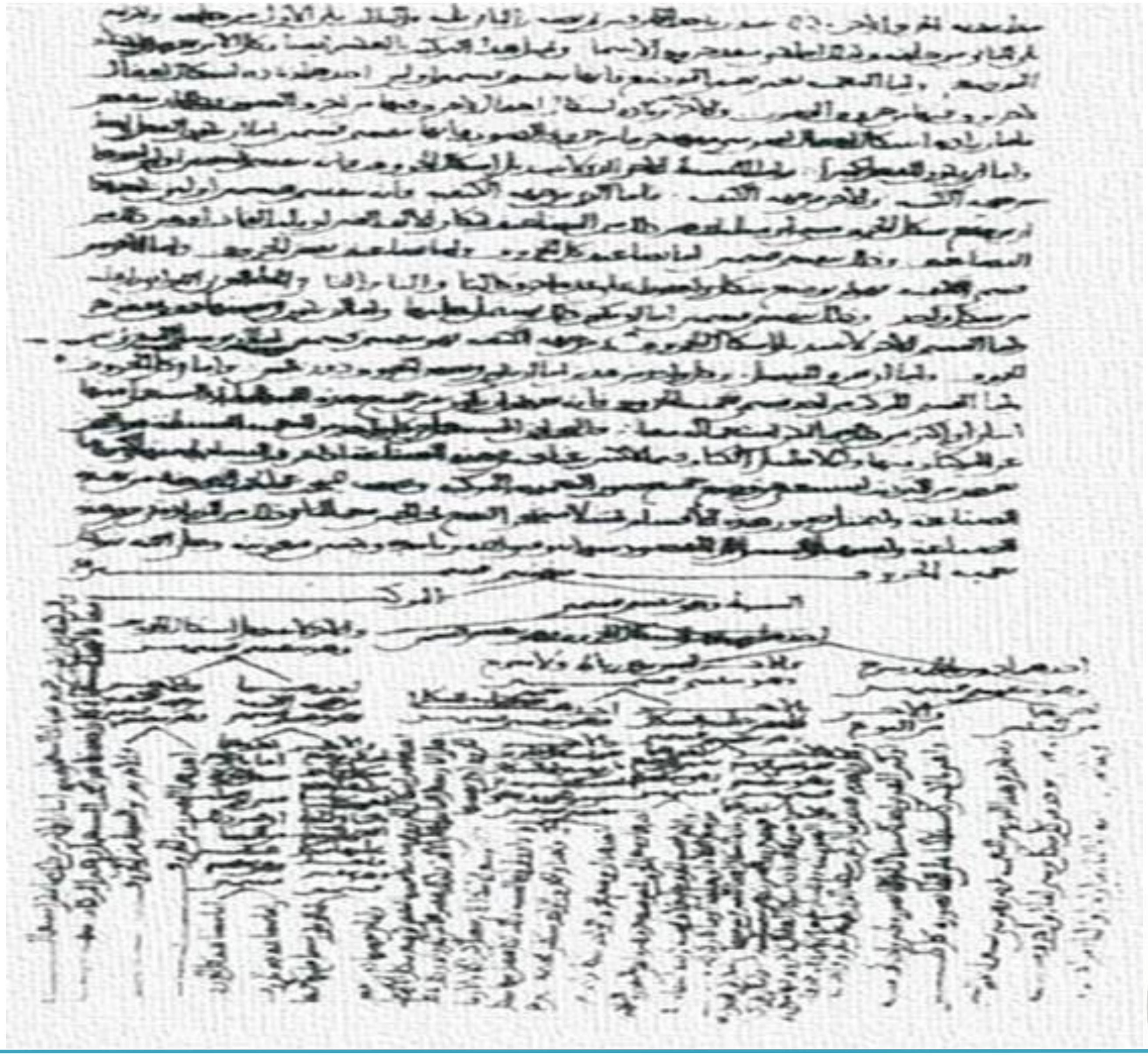


Arabic Origins of Cryptology – Volume One (al-Kindi's Treatise on Cryptanalysis), M. Mrayati et al. KACST and KFCRI *2003*

* *Ibrahim A. Al-Kadi, (2010) ORIGINS OF CRYPTOLOGY: THE ARAB CONTRIBUTIONS, Cryptologia, 16:2, 97-126*

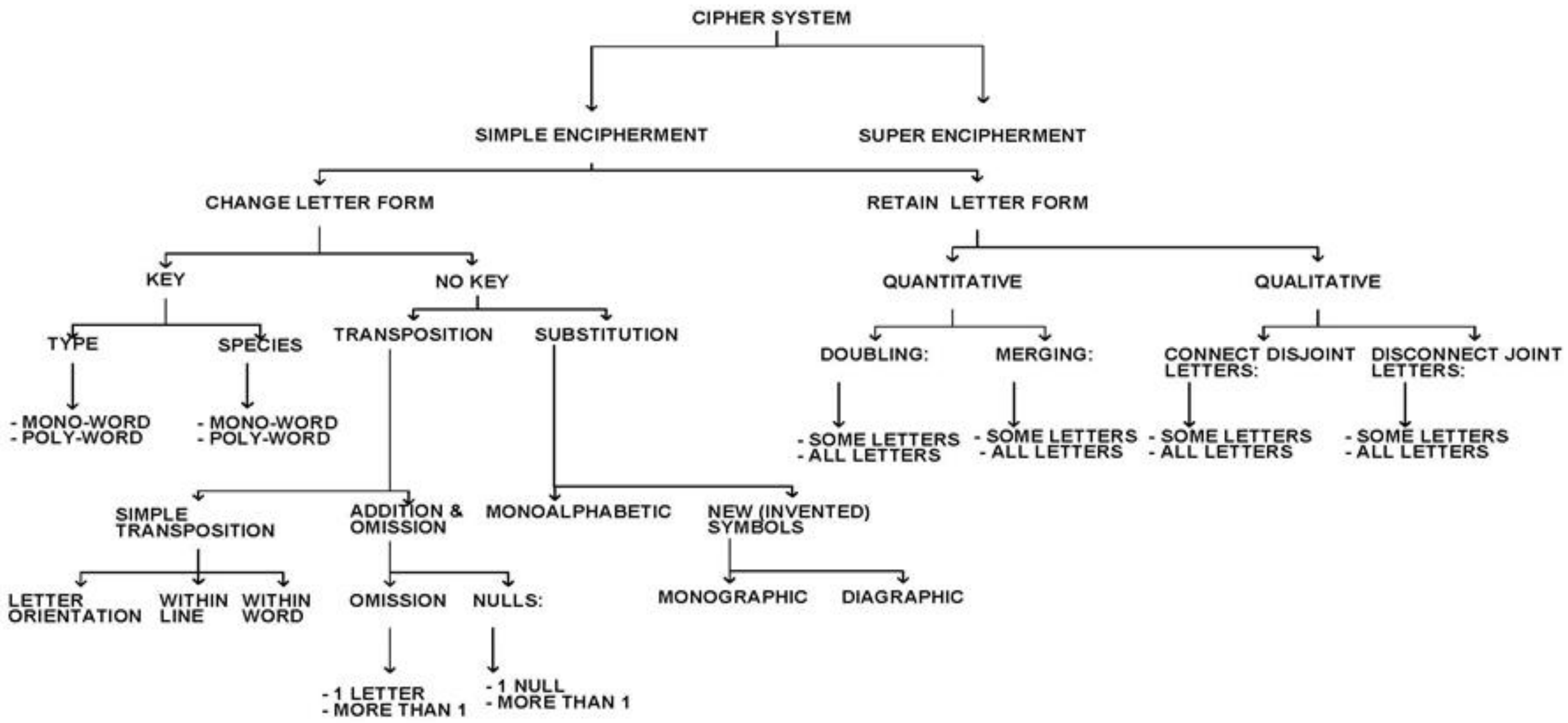
Originality of the Arab Cryptology Works

- al-Kindi's tree diagram classification of cipher types as it appears in his manuscript. He classified cipher systems into categories as transposition, and substitution, seven centuries before G. B. Porta



Originality of the Arab Cryptology Works

- al-Kindi's tree diagram classification of cipher types redrawn and translated



Originality of the Arab Cryptology Works

Concept / Work	Arabic Works	European Works
Manuscript on Cryptanalysis	al-Kindi, (Died 260 AH / 874 AD	L. B. Alberti (1404 -1472 AD) .
Principles of Statistics	al-Kindi, (Died 260 AH / 874 AD	Pierre de Fermat 1607–1665 AD. Blaise Pascal 1623 – 1662 AD
Permutations and Combinations.	al-Farahidi, (100 – 170 AH / 718 - 786 AD)	Pierre de Fermat (1607–1665 AD). Blaise Pascal 1623 – 1662 AD
Solving a mono-alphabetic cipher with no word division.	ibn Adlan, (Died 666AH / 1268 AD)	G. Porta 1535–1615 AD.
A table for encryption.	ibn ad-Durayhim, (Died 762 AH / 1359 AD)	Blaise de Vigenere. (1523 –1596 AD)
A simple grille for encryption.	ibn ad-Durayhim, (Died 762 AH/ 1359 AD)	G. Cardano (1501 – 1576 AD)
Decoding Hieroglyphics	Ibn Wahshiyyah decoded some. (291 AH / 914 AD)	J. F. Champollion decoded all (1790 – 1832 AD)

Originality of the Arab Cryptology Works

- ibn Dunaynir used numbers to encrypt letters. He wrote in his book that “*an example enciphered, (by numbers), for me by **some Maghrebi** in Dar as-Salaam*”

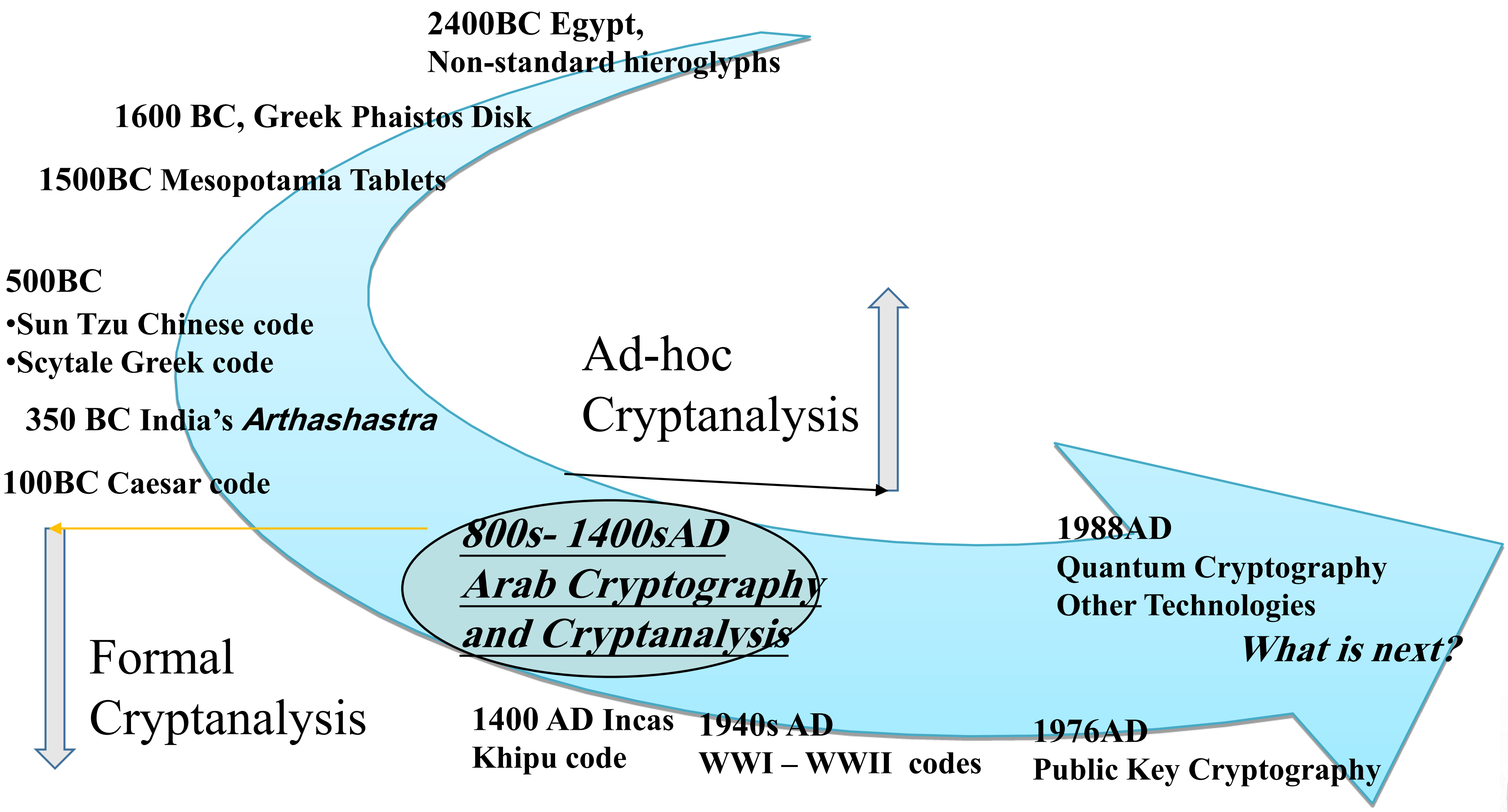
- al-Gurhumi calculated the frequencies of bigrams and trigrams. He also mentioned that complex encryption techniques may lead to problems for the legitimate decryptor during wars, and that encryption errors may help the attacker

- al-Gurhumi noted that when the ciphertext is short it may be impossible to cryptanalyze.

- al-Gurhumi and the author of the two essays explained how to use more than one character to substitute for a high frequency letter, so that frequency analysis attacks are rendered useless.

- ibn Wahab explained using complex encryption by substitution and transposition at the same time.

Historical Milestones in Cryptology After the Discovery of the Manuscripts



2400BC Egypt,
Non-standard hieroglyphs

1600 BC, Greek Phaistos Disk

1500BC Mesopotamia Tablets

500BC
- **Sun Tzu Chinese code**
- **Scytale Greek code**

350 BC India's *Arthashastra*

100BC Caesar code

Ad-hoc Cryptanalysis

800s- 1400sAD
Arab Cryptography
and Cryptanalysis

Formal Cryptanalysis

1400 AD Incas
Khipu code

1940s AD
WWI – WWII codes

1976AD
Public Key Cryptography

1988AD
Quantum Cryptography
Other Technologies

What is next?

Final Remarks for Further Investigation

- Arab Cryptologists do not mention “unbreakable” ciphers*! Why?

- The Arabs did not expand on their work on Statistical and Combinatorial Analyses. Why?

- The Umayyads, who fled the Abbasid power in the East, formed their own Caliphate in Maghreb and Andalusia, and used Cryptology. ** Did they copy from the East or develop their own or both?

- Did the Arabs develop signatures? The Arabs of Maghreb and Andalusia used some form of numerical signature. **

- Ibn Wahshiyyah’s book was translated into English by J. Hammer in 1806. The translation was known to A. Kircher, and to Silvestre de Sacy, the professor of Jean Francois Champollion who decoded the Hieroglyphs in 1820. **ibn Wahshaiyyah’s work certainly aided in decoding the Hieroglyphics***.**

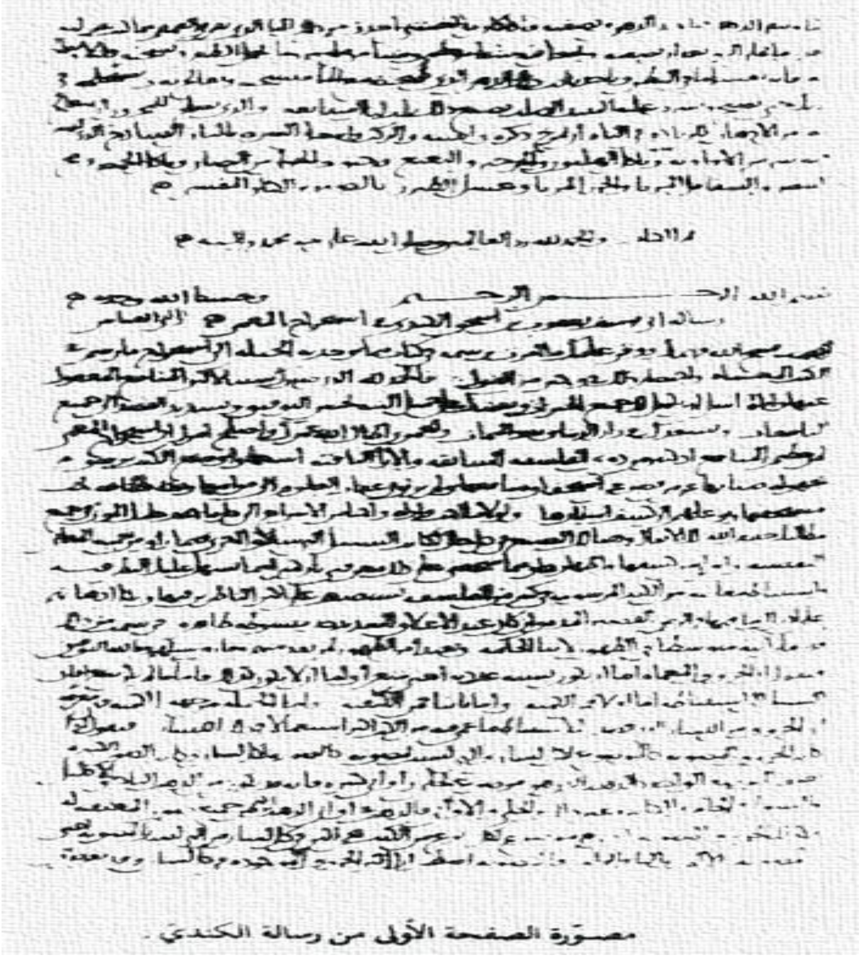
**Ibrahim A. Al-Kadi, (2010) ORIGINS OF CRYPTOLOGY: THE ARAB CONTRIBUTIONS, Cryptologia, 16:2, 97-126*

***Abdelmamlik Aziz & Mostafa Aziz, Cryptologia; Pages 47-57 | Published online: 22 Dec 2010*

**** An article by Dr. Okaskah El Daly, at http://www.muslimheritage.com/article/deciphering-egyptian-hieroglyphs-muslim-heritage*

Originality of the Arab Cryptology Works

Photocopies of some pages



[illegible]

[illegible]

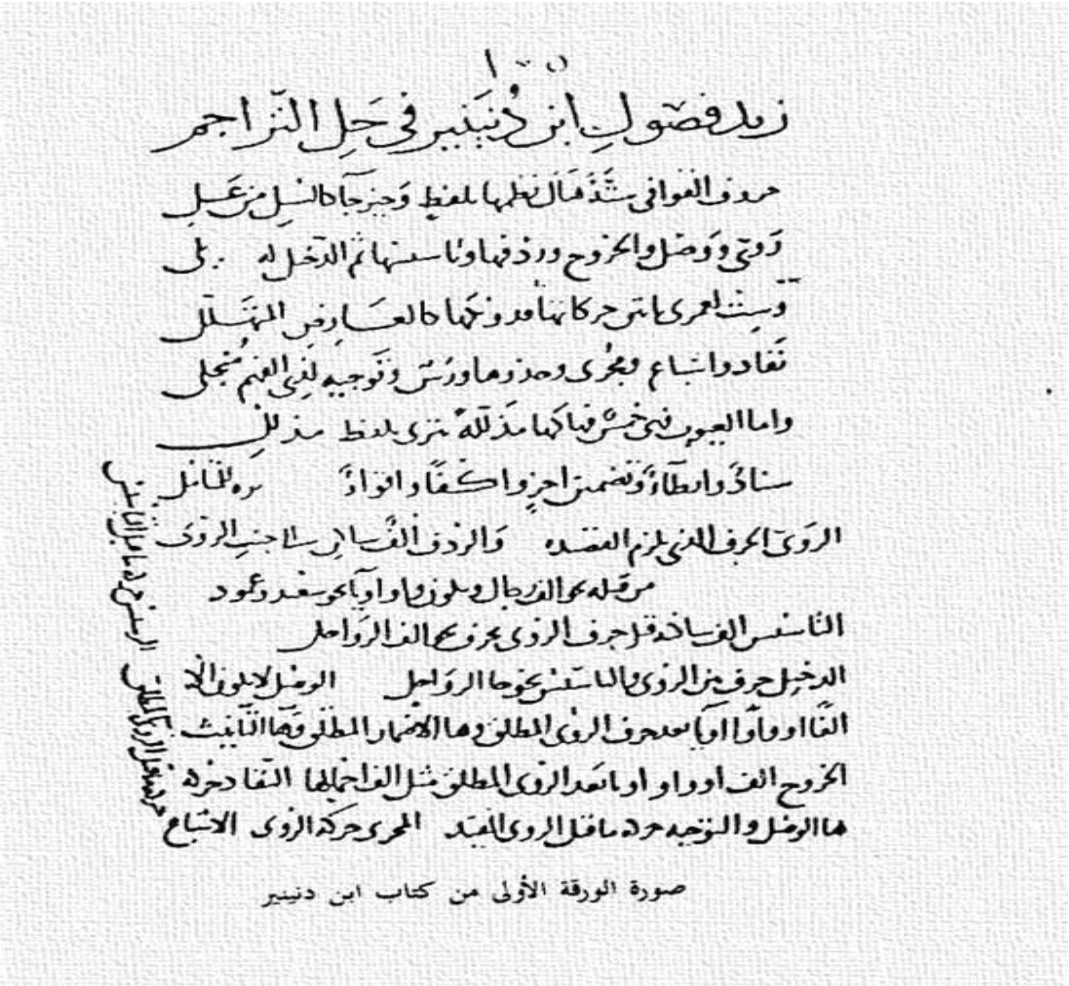
بسم الله الرحمن الرحيم وحسبنا الله وحده

رسالة ابي يوسف يعقوب ... في استخراج المعمى [illegible]

[illegible]

مصورة الصفحة الأولى من رسالة الكندي

The first page of Al-Kindi’s Manuscript



١٠٥

زبد فصول ابن دنينير في حل التراجم

حروف القوافي ستة فمال نظمها بلفظ وجيز جاء كالسيل من عل
روي ووصل والخروج وردفها وتاسيسها ثم الدخيل له بلي
وست لعمري بالتي حركاتها فعدو خمها كالعارض المتهلل
نفاذ واشباع ومجرى وحذوها ورس وتوجيه لذي الفهم منجلي
واما العيوب فهي خمس فنا كها مذ لله تري بلفظ مذلل
سناد وايطاء وتضمين اجزوا كفاء واقواء ره للقائل

الروي الحرف الذي يلزم القصيدة والردف الف ساكن قبل الروي
من قبله نحو الرجال وسلوى واو ياء نحو سعيد وعود
التاسيس الف بينها وبين حرف الروي حرف نحو الف الرواحل
الدخيل حرف بين الروي والتاسيس نحو حا الرواحل الوصل الاطلاق الا
الف او واو او ياء بعد حرف الروي المطلق وها الاضمار المطلق وها التانيث
الخروج الف او واو او ياء بعد الروي المطلق مثل الف الجمل لها النفاذ حركة
ها الوصل والتوجيه حركة ما قبل الروي المقيد المجرى حركة الروي الاشباع

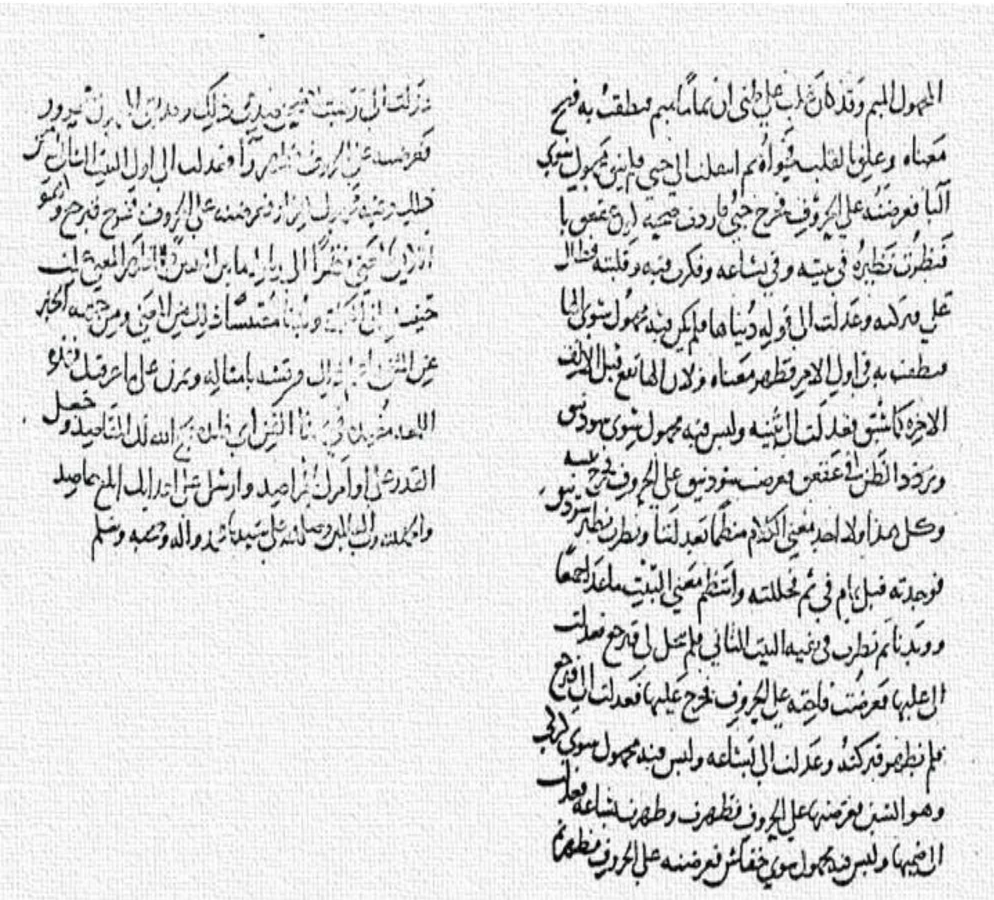
[illegible]

صورة الورقة الأولى من كتاب ابن دنينير

The first page of Ibn Dunaynir’s Treatise

Originality of the Arab Cryptology Works

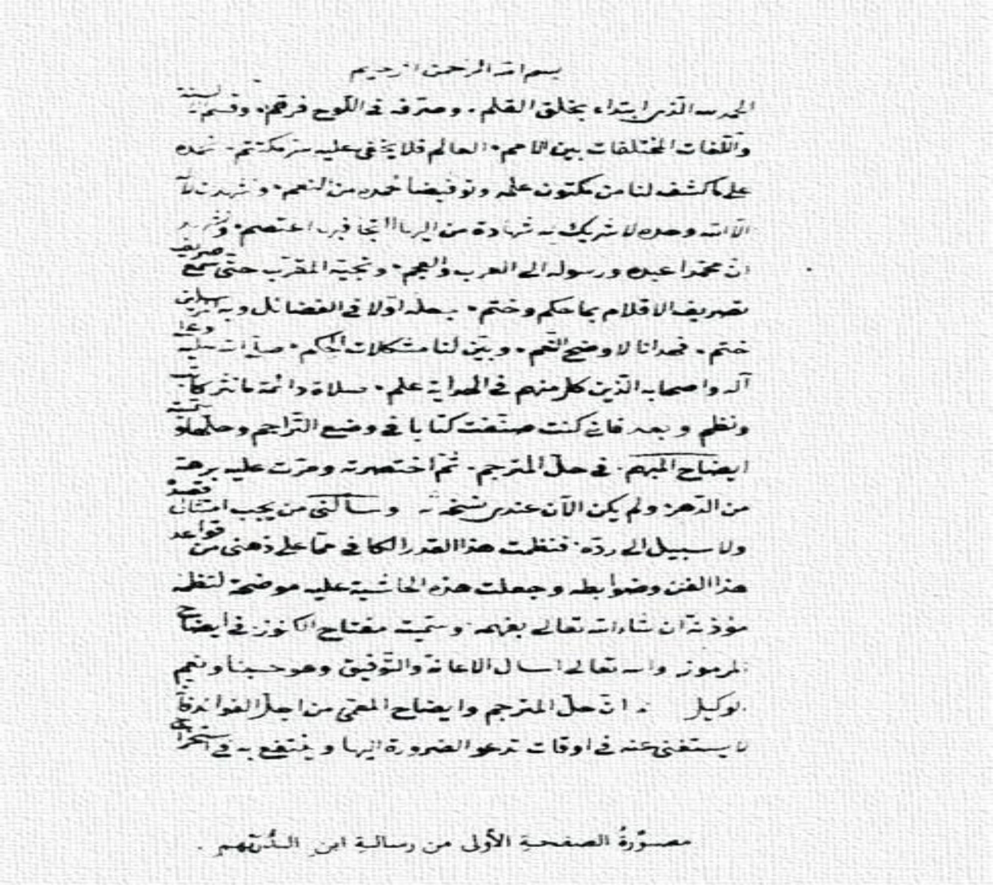
Photocopies of some pages



المجهول المبهم وقد ذكرت غلب على ظني ان بها ما ابهم منطبق به في
معناه وعلقوا بالقلب فتوا ثم اسلنا الى حتى فاين مجهول سوى
الباء فعرضته على الحروف فخرج حتى فاردف صحبه اربع ممعن با
فنظرت نظيره في بيته وفي تساعه وفكرت فيه وقلبته فخالف
على ما ذكرته وعدلت الى اوله دنيا ها فلم يكن فيه مجهول سوى الباء
منطبق به في اول الامر فظهر معناه ولان الهاء تقع قبل الالف
الاخره كا شئ فعدلت الى ثنيه وليس فيه مجهول سوى سودنى
وبرددا النظر في عنقتى فعرضت سودنى على الحروف فخرج بيسه
وكل هذا ولا احد معنى الكلام منتظما فعدلنا ونظرت نظيره سودنى
فوجدته قبل ام في ثم فحللته واستظم معنى البيت ملعدلجها
ووجدنا ثم نظرت في نفيه البيت الثاني فلم يحل لي فرح فعدلت
الى عليها فعرضت ملحته على الحروف فخرج عليها فعدلت الى فرحع
فلم نظهر فتركته وعدلت الى تساعه وليس فيه مجهول سوى دجب
وهو النشر فعرضته على الحروف فظهر وظهر تساعة فعدلت
الى ضيها وليس فيه مجهول سوى خفاش فعرضته على الحروف فظهر

فعدلت الى [illegible] [illegible] ذلك [illegible] [illegible] يرود
فعرضته على الحروف [illegible] وعدلت الى اول البيت الثاني
خلي [illegible] [illegible] فعرضته على الحروف فخرج فرحي وانحو
[illegible] [illegible] الى [illegible] ما بين [illegible] المعنى له
خيف [illegible] [illegible] متنسقا الى المعنى ومن جهة الخبر
عن [illegible] [illegible] بامثاله ويزن على ما عرفتك فتفهمه
[illegible] [illegible] [illegible] ذلك [illegible] الله لك التاييد وجعل
القدرة [illegible] [illegible] وارشد [illegible] الى ما يحمد
والحمد لله رب العالمين وصلى الله على سيدنا محمد واله وصحبه وسلم

The last two pages of ibn Adlan’s Treatise



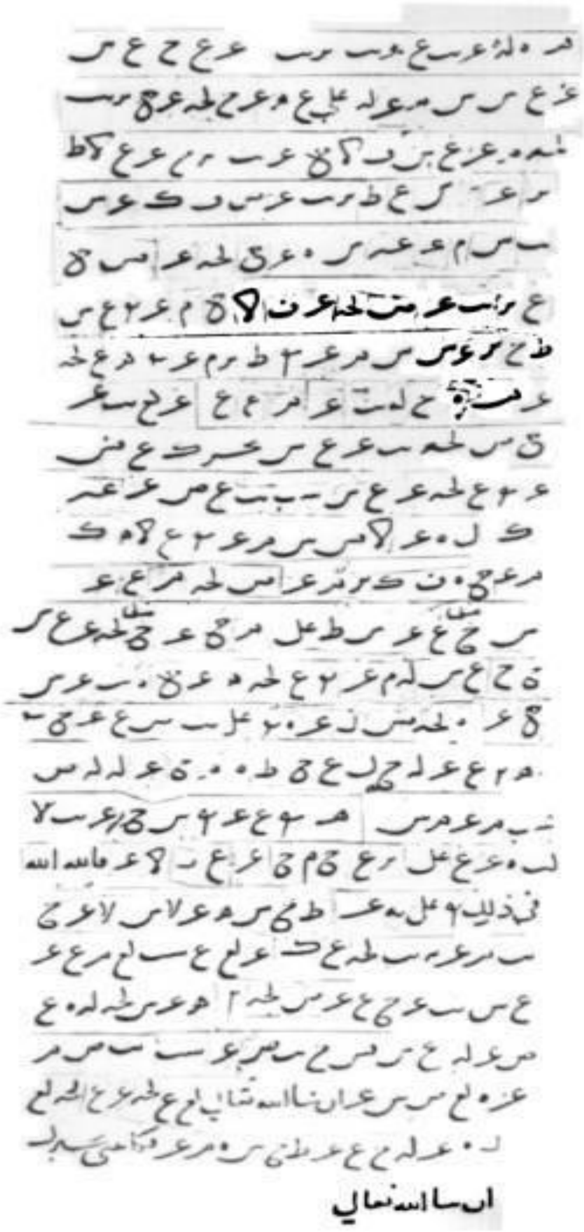
بسم الله الرحمن الرحيم

الحمد لله الذي ابتدأ بخلق القلم . وصرفه في اللوح فرقم . وقسم الألسنة
واللغات المختلفات بين الأمم . العالم فلا يخفى عليه سر مكتتم . نحمده
على ما كشف لنا من مكنون علمه وتوفيقنا خير من النعم . ونشهد أن لا
إله إلا الله وحده لا شريك له شهادة من إليها التجأ فبها اعتصم . ونشهد
أن محمدا عبده ورسوله إلى العرب والعجم . ونجيه المقرب حتى سمع صريف
تصريف الأقلام بما حكم وختم . بعله أولا في الفضائل وبه
ختم . فهدانا لأوضح اللقم . وبين لنا مشكلات الحكم . صلى الله عليه وعلى
آله وأصحابه الذين كل منهم في الهداية علم . صلاة دائمة ما نثر كلام
ونظم وبعد فإني كنت صنفت كتابا في وضع التراجم وحلها سميته
إيضاح المبهم في حل المترجم . ثم اختصرته ومرت عليه برهة
من الدهر ولم يكن الآن عندي نسخة . وسألني من يجب امتثال قصده
ولا سبيل إلى رده . فنظمت هذا القدر الكافي مما على ذهني من قواعد
هذا الفن وضوابطه وجعلت هذه الحاشية عليه موضحة لنظمه
مؤذنة إن شاء الله تعالى بفهمه . وسميته مفتاح الكنوز في إيضاح
المرموز والله تعالى أسأل الإعانة والتوفيق وهو حسبنا ونعم
الوكيل . إن حل المترجم وإيضاح المعمى من أجل الفوائد التي
لا يستغنى عنه في أوقات تدعو الضرورة إليها وينتفع به في استخراج

مصوّرةُ الصفحةِ الأولى من رسالةِ ابن الدُّرَيهم .

The first page of Ibn Ad-Durayhim’s Treatise

Cryptanalysis Example by the author of the two essays



ان شا الله تعالى

Four basic principles for cryptanalysis used by the Arab scholars

Four basic principles for cryptanalysis, commonly used by the Arabs with surprising efficiency. They are the following principles:

1) Making use of the number of letters in a cryptogram to identify the language of the text.

2) Statistical Cryptanalysis: Making use of the frequency of letter occurrences in the text, and comparing it with the frequencies of the language in question.

3) Statistical Cryptanalysis: Making use of the frequency of the occurrence of bigrams and trigrams and other particularities, or what they called the "combination and non-combination of letters".

4) Probable Words: Making use of the traditional opening statements or honorary titles, to guess useful information about the cryptogram.

What Made The Arab Advancement In Cryptology Possible?

Advances in the following fields made the Arab development of Cryptology possible:

1. **Translation:** The need to translate encrypted books; and scripts in dead languages.
2. **Administrative Studies:** The need of the emerging Islamic state for administrative organization and communicating over large distances.
3. **Mathematical Studies:** Major contributions in mathematics.
4. **Linguistic Studies:** All aspects of linguistic studies were pre- requisites for the advancement of cryptography and cryptanalysis.
5. **Paper technology**
6. **Widespread Literacy.**

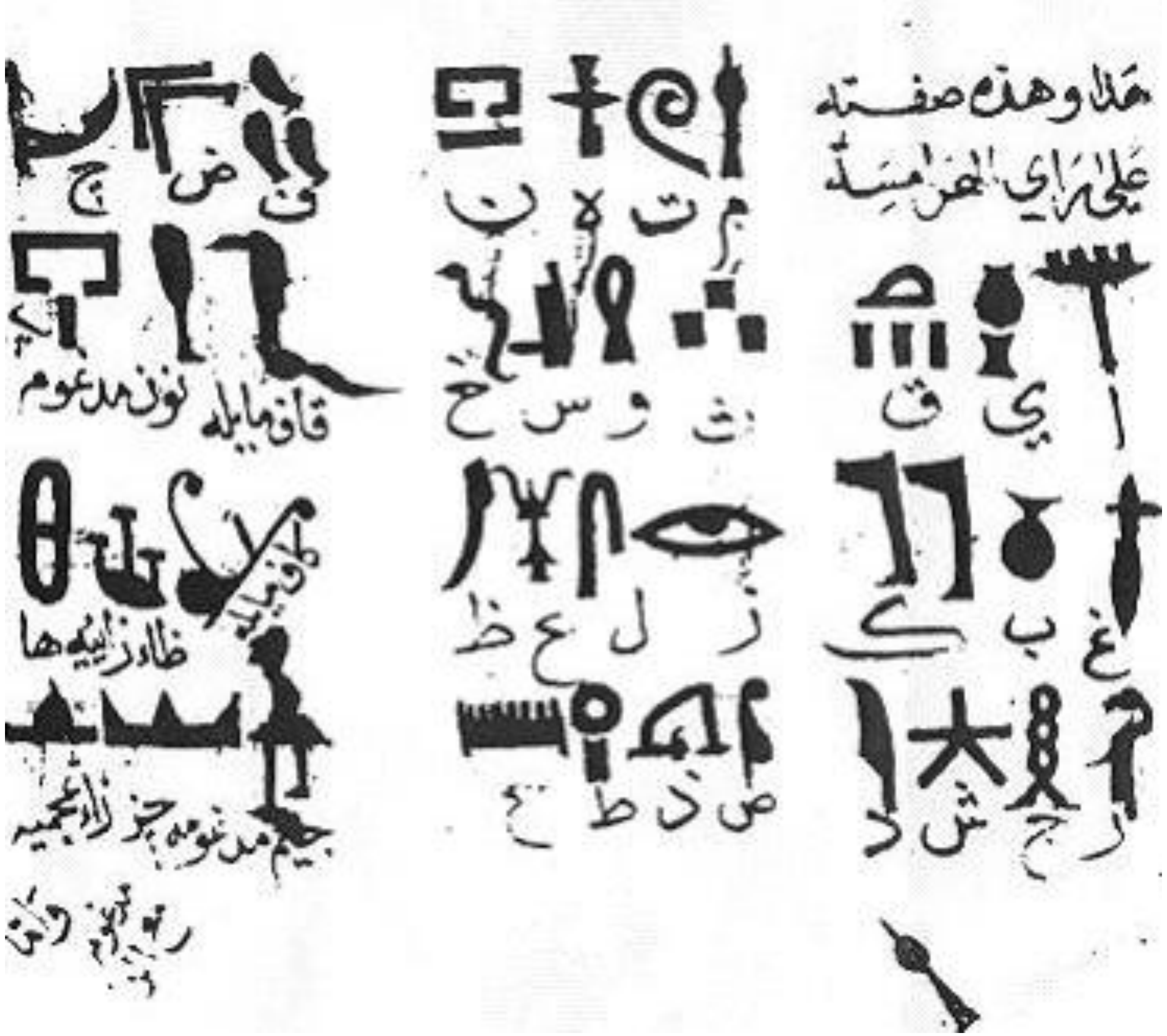
Books that have not been found yet.

The analysis of the discovered manuscripts and other references brought to light other works by Arab scholars on Cryptology which have not been found yet. Some of those works include:

Scholar	Life Span	Works
Al-Khalil ibn Ahmad al-Farahidi	AH 100 - 170 AD 718 - 786	A Book on Cryptology not found yet, but referenced by az-Zubaidi and ibn Nubata. ibn Nubata considered al-Farahidi as the founder of Cryptology.
Jaber ibn Hayyan	AH … - 200 AD ... - 815	A book titled “Hall ar-rumuz wa mafatih al kunuz”, *(Solving Symbols and the keys toTreasures),* not found yet, but referenced by Ahmad ibn Wahshiyya.
Ahmad Abu al-Qasim al-Iraqi	Unknown	A Book on “ Hall ar-rumuz wa fath aqfal al-kunuz”, *(Solving Symbols and opening the keys to Treasures),* not found yet, but referenced by the author of “Kashf az-zunun” ‘

Lyle D. Broemeling (2011) An Account of Early Statistical Inference in Arab Cryptology, The American Statistician, 65:4, 255-257, DOI: 0.1198/tas.2011.10191

Beginning in the seventh and eighth centuries, an early use of statistical inference appeared as a tool to decipher encrypted Arabic messages. Cryptology was pioneered by the Arabs and as one of the methods used to decipher the cryptograms is relative frequency analysis. Following al-Kindi, cryptology was advanced by the Arabs for the next 400 years and the advancement included frequency analysis and other statistical techniques. One of the earliest references to statistical inference is found in the Pascal and Fermat (1654) correspondence. It is interesting, however, to observe that the standard texts on the history of statistics do not mention Arab contributions. For example, Stigler (1986, 1999), David (1962), and Hald (1990, 1998) do not cite Arab works in statistics; in fact, the first reference I found is by al-Kadi (1992). It would be interesting to find if additional contributions to statistics were made by Arab cryptologists.


هذا وهذه صفته
علمه اي الهرامسة
ا ي ق
غ ب ك
ر ج ش د
م ت ه ن
ث و س خ
ز ل ع ظ
ص ذ ط ع
ج ض ي
نون مدغوم
قاف مايله
كاف مايله
ظاء زايه ها
جيم مدغومه جزاء العجميه