
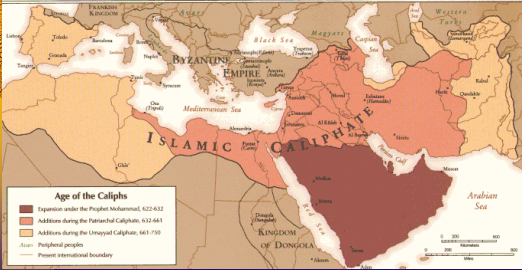


Arabic Cryptography



The Rise of Islam





The Rise of Cryptography

Administration




Mathematics



Translation






Modern Beginnings

600 AD Widespread use of monoalphabetic substitution ciphers for administrative use

700 AD Al-Khalil (philologist): use of a crib ('In the name of God')




Al-Kindi (801-873)

“A Manuscript on Deciphering Cryptographic Messages”

- cryptanalytic methods
 - cribs
 - vowel-consonant combinations
 - frequency analysis
- classification of ciphers
- linguistic analysis (letter frequencies)

Taken from Al-Kadi, *Origins of Cryptology-The Arab Contribution*, Cryptologia, 2, 2010



Al-Kindi and Frequency Analysis

One way to solve an encrypted message if we know its language, is to find a text of the same language long enough ... and then count each letter of it. We call the most frequently occurring letter the “first”, ... and so on. Then we look at the cryptogram we want to solve and we also classify its symbols. We find the most occurring symbol and change it to the form of the “first” letter.


Taken from Al-Kadi, *Origins of Cryptology-The Arab Contribution*, Cryptologia, 2, 2010



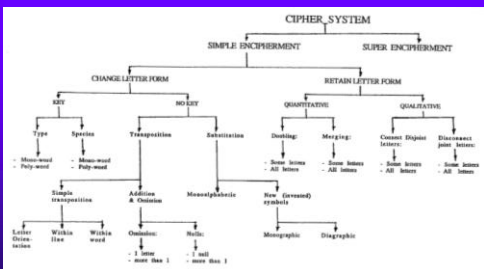
Al-Kindi's Classification




Taken from Al-Kadi, *Origins of Cryptology-The Arab Contribution*, Cryptologia, 2, 2010



Al-Kindi's Classification




Taken from Al-Kadi, *Origins of Cryptology-The Arab Contribution*, Cryptologia, 2, 2010



Cipher systems

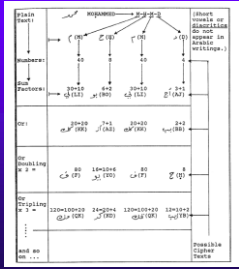
Ciphersystems suggested by Ibn ad-Duraihim (1312-1361), according to al-Qalqashandi 14 volume encyclopedia (published in 1412):

- (1) One letter may replace another
- (2) A word may be written backwards.
- (3) Swap alternate letters of a word.
- (4) Replace letters by numbers.
- (5) Replace letters by two other letters the sum of whose numeric values is the same.
- (6) "Substitute for each letter the name of a man or something like that."
- (7) Use lunar mansions, fruits, trees, countries, etc. as substitutes.




Ad-Duraihim

ad-Duraihim's book survives and contains more detail n al-Qalqashandi



Taken from Al-Kadi, *Origins of Cryptology- The Arab Contribution*, Cryptologia, 2, 2010




Frequency Analysis

1412 AD Al-Qalqashandi based on earlier writings by Ibn ad-Duraihim (1300 AD)

“When you want to solve a message which you have received in code, begin first of all by counting the letters, and then count how many times each symbol is repeated and set down the totals individually.” ...

“When you see that one letter occurs in the message more often than the rest, then assume that it is alif; then assume that the next most frequent is lām.”



Modern Frequency Analysis I


Frequency orderings:

eaoidhnrstuyfcglmwbkpxz E.A. Poe, 1843

etaonirshdlucmpfywgbvjkqxx Kahn, 1967

Frequency counts:


a	8.04%	
b	1.54%	
c	3.06%	(Meyer-Matyas)
d	3.99%	
e	12.51%	
...		



Modern Frequency Analysis II

Frequency cliques:

{e}	{t}	{aoin}	{srh}	(high)
{ld}	{cumf}	{pgwyb}		(medium)
{vk}	{xjqz}			(low)



Modern Frequency Analysis III

Frequent words:


the of and to a in that it is I for as with was his he be ...

Frequent bigrams:

th he an in er re on es ti at st en or nd to nt ed is ar

Frequent trigrams:

the ing and ion tio ent ere her ate ver ter tha ati for




Modern Frequency Analysis IV

Other helpful information:

- a, i, and o avoid contact with the exception of io
- n tends to be preceded by a vowel
- h occurs often before e, but rarely after it
- vowels have more contact with other letters than consonants

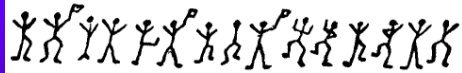
For cryptograms with word divisions:

- t, o, s are frequent both as first and last letters
- a, i, h are frequent as first, but not last letters
- e, n, r are frequent as last, but not first letters



Dancing Men and Golden Bugs

In "Sherlock Holmes and the Dancing Men" Holmes is confronted with a graphical substitution cipher,



53 3 3 3 3 3 0 5) 6 * ; 4 8 2 6) 4 3 ; .) 4 3 ; : 8 0 6 * ; 4 8 7 8 ¶
 6 0)) 8 5 ;] 8 * ; 3 * 8 7 8 3 (8 8) 5 * 7 ; 4 6 (; 8 8 * 9 6 *
 ? ; 8) * 3 ; (; 4 8 5) ; 5 * 7 2 : * 3 ; (; 4 9 5 6 * 2 (5 * - 4) 8 ¶
 8 * ; 4 0 6 9 2 8 5) ;) 6 7 8) 4 3 ; ; 1 (3 ; 9 ; 4 8 0 8 1 ; 8 ; 8 3
 1 ; 4 8 7 8 5 ; 4) 4 8 5 7 5 2 8 8 0 6 * 8 1 (3 ; 9 ; 4 8 ; (8 8 ; 4 (;
 3 4 ; 4 8) 4 3 ; ; 1 6 1 ; ; 1 8 8 ; 3 ; ? ;

Cryptogram from
Poe's "The Gold
Bug".
