USING THE RELATIONSHIP BETWEEN PERIODIC CONTINUED FRACTION AND QUADRATIC IRRATIONALS: ASAB - II CIPHER

Ahmet Şükrü ÖZDEMİR*
Ahmet Bilal YAPRAKDAL**

Abstract

A periodic continued fraction is a continued fraction whose terms eventually repeat from some point onwards. All nontrivial periodic continued fractions represent irrational numbers. In general, an infinite simple fraction (periodic or otherwise) represents a unique irrational number, and each irrational number has a unique infinite continued fraction.

A quadratic irrational is an irrational number which is a root of a quadratic equation with integer coefficients. Quadratic irrationals are exactly the real numbers which have infinite periodic continued fraction expansions. In mathematics, a quadratic irrational, also known as a quadratic irrationality or quadratic surd, is an irrational number that is the solution to some quadratic equation with rational coefficients.

The purpose of this study is to develop a new technique, which we called "ASAB-II" (Initial of the names of authors) cipher, using the relationship between periodic continued fraction and quadratic irrationals. Furthermore, we hope to obtain an algorithm stronger than the structure of ASAB - I.

Keywords: ASAB III Technique, Cryptology, Periodic Continued Fraction, Quadratic Irrational Numbers, Number Theory

---

* *Doç. Dr., Atatürk Eğitim Fakültesi Marmara Universitesi Atatürk Eğitim Fakültesi*
** *Arş.Gör., .Ahmet Bilal Yaprakdal Marmara Universitesi Atatürk Eğitim Fakültesi*

AHMET ŞÜKRÜ ÖZDEMİR
AHMET BİLAL YAPRAKDAL

Periyodik Sürekli Kesir İle Kuadradik İrrasyonel Sayilar Arasindaki İlişki Kullanilarak Asab - Iii Şifrelemesi

Özet

Bir periyodik sürekli kesir belli noktadan itibaren tekrar devam eden bir kısımdır. Tüm aşikar olmayan periyodik sürekli kesirler, irrasyonel sayılar olarak gösterilebilir. Genel olarak, sonsuz bir basit kesir (veya başka şekilde periyodik) ve tek bir irrasyonel sayı gösterir ve her irrasyonel sayı tek bir sonsuz sürekli kesire sahiptir.

Bir kuadratik irrasyonel sayı tam katsayılı ikinci dereceden bir denklemin bir köküdür. Kuadratik irrasyonel sayılar sonsuz periyodik sürekli kesir açılımları olan reel sayılardır. Matematikte, bir kuadratik, irrasyonel sayı bir kuadratik irrasyonel veya ikinci dereceden irrasyonel olarak da bilinen irrasyonel sayılar, rasyonel katsayılı bazı ikinci dereceden denklemin çözüm dür.

Bu çalışmanın amacı, periyodik sürekli kesir ve ikinci dereceden irrasyonel arasındaki ilişki kullanılarak, "ASAB-II" şifrelme (yazarların adları ilk) adı verilen yeni bir tekniği geliştirmektir. Ayrıca, algoritma ASAB –I yapısını daha güçlü kılan bir algoritma yı elde etmeyi ümit ederiz.

Anahtar Kelimeler : ASAB-II Tekniği, Şifreleme, Periyodik Sürekli Kesir, Kuadratik irrasyonel Sayılar,Sayılar Teorisi

INTRODUCTION

Today the usage of electronic media, equipment and devices is becoming widespread and indispensible in communication. In parallel, the prevention of the information that is transferred in electronic media and the secure information sharing become very important. In order to provide a secure data transfer different ciphering methods are developed and used. The ciphering algorithms that are used today can be classified as symmetric, asymmetric and hash algorithms. In symmetric algorithms, such as block ciphering algorithms, the same keyword is used in encoding and decoding [7]. One of the classical ciphering techniques, Vigenere ciphering method makes use of block ciphering

Vigenere ciphering is developed by French cryptologist Blaise de Vegenere. It is more sophisticated and different from Caesar ciphering in terms of using more than one alphabet. Usage of multiple alphabets through keyword instead of mono alphabet decreases the possibility to break the code with frequency analysis. On the other hand, some algorithms developed for determination of the length of the keyword can weaken the strength of the ciphering [12]. Most of the time, choosing a longer keyword in Vigenere ciphering method seems to be a solution to minimize or eliminate the risk. However, this not only increases the time for transmission of the keyword through the safe communication media, but also cannot prevent to decode the coded text easily when third parties get hold of the keyword.

This study provides a new insight about minimizing the above explained risks. Moreover, this study is continuation and a different interpretation of ASAB technique which is first introduced in "Proceedings of the Third International Conference on Modeling, Simulation and Applied Optimization (2009)" [6]. ASAB technique uses one of the mathematical definitions of finite continuous fractions, whereas ASAB – II technique, which will be introduced in this study, utilizes representation of irrational numbers as infinite continuous fractions.

1.PRELIMINARIES AND LITERATURE SURVEY

1.1. Relationship Between Irrational Numbers and Periodic Continuous Fractions

Definition: An infinite continuous fraction is periodic continuous fraction with period k, if there exist k and L positive numbers such that for all, $a_l = a_{l+k}$ is hold [4]. It is represented by

$$[a_0, a_1, \ldots\ldots, a_{L-1}, \overline{a_L, a_{L+1}, \ldots\ldots a_{L+k-1}}] \quad (1)$$

There exists a continuous fraction for every real number which is unique. The continuous fraction is finite for rational numbers and infinite for irrational numbers. Every infinite continuous fraction corresponds to an irrational number. In other words, irrational numbers can be represented as continuous fractions [3].

Theorem: Let $\alpha = \alpha_0$ be an irrational number and let the sequence $a_0, a_1, a_2, \ldots$ is defined as,

$$a_k = [\![\alpha_k]\!], \quad \alpha_{k+1} = \frac{1}{(\alpha_k - a_k)} \quad (2)$$

Then, $\alpha\ [a_0, a_1, a_2, \ldots]$ is the value of infinite ordinary continuous fraction [8]. As an example, for irrational number $\sqrt{6}$, one can write the following equalities:

$$k = 0 \quad \Rightarrow \quad a_0 = [\![\alpha_0]\!] = 2$$

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{6} - 2} = \frac{\sqrt{6}+2}{2}$$

$$k = 1 \quad \Rightarrow \quad a_1 = [\![\alpha_1]\!] = \left[\!\!\left[\frac{\sqrt{6}+2}{2}\right]\!\!\right] = 2$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \sqrt{6} + 2$$

$$k = 2 \quad \Rightarrow \quad a_2 = [\![\alpha_2]\!] = [\![\sqrt{6}+2]\!] = 4$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{\sqrt{6}+2}{2}$$

Since $\alpha_1 = \alpha_3$, we conclude

$$\sqrt{6} = [2 : 2, 4, 2, 4, \ldots] = [2 : \overline{2, 4}]$$

A graph that shows the relationship between the number of digits in periodic part (N) and the irrational number can be obtained when irrational numbers are represented as periodic fractions. The below figure shows as the

irrational number gets larger, it is more possible to have more digits in periodic part of the fraction.

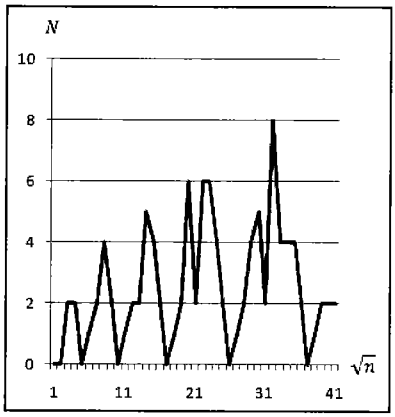

Figure 01. *Irrational Numbers and Number of Periodic Digits*

The above graph is obtained by representing the irrational numbers generated by taking the square root of the numbers from 1 to 40, as periodic continuous fractions. The corresponding calculations are given below [10]:

$\sqrt{n}$	$\alpha_{\sqrt{n}}$	$\sqrt{n}$	$\alpha_{\sqrt{n}}$
2	$[1:\overline{2}]$	3	$[1:\overline{1,2}]$
5	$[2:\overline{4}]$	6	$[2:\overline{2,4}]$
7	$[2:\overline{1,1,1,4}]$	8	$[2:\overline{1,4}]$
10	$[3:\overline{6}]$	11	$[3:\overline{3,6}]$
12	$[3:\overline{2,6}]$	13	$[3:\overline{1,1,1,1,6}]$
14	$[3:\overline{1,2,1,6}]$	15	$[3:\overline{1,6}]$
17	$[4:\overline{8}]$	18	$[4:\overline{4,8}]$
19	$[4:\overline{2,1,3,1,2,8}]$	20	$[4:\overline{2,8}]$

21	$[4:\overline{1,1,2,1,1,8}]$	22	$[4:\overline{1,2,4,2,1,8}]$
23	$[4:\overline{1,3,1,8}]$	24	$[4:\overline{1,8}]$
26	$[5:\overline{10}]$	27	$[5:\overline{5,10}]$
28	$[5:\overline{3,2,3,10}]$	29	$[5:\overline{2,1,1,2,10}]$
30	$[5:\overline{2,10}]$	31	$[5:\overline{1,1,3,5,3,1,1,10}]$
32	$[5:\overline{1,1,1,10}]$	33	$[5:\overline{1,2,1,10}]$
34	$[5:\overline{1,4,1,10}]$	35	$[5:\overline{1,10}]$
37	$[6:\overline{12}]$	38	$[6:\overline{6,12}]$
39	$[6:\overline{4,12}]$	40	$[6:\overline{3,12}]$

Table 01. *Representation of Irrational Numbers as Periodic Fractions*

1.2. Vigenere (Mono Alphabet) Cryptography

2.2.1. Encoding and Decoding Algorithm

Vigenere ciphering technique was developed by a French Royalty member Blaise de Vigenere in 16th century. The below Vegenere Table can be used in this technique to determine the substituting characters. For English alphabet, the table is a square with 26 rows. Ciphering is done with a keyword and the characters of the keyword are searched in the heading row. On the contrary, the characters of the text are searched in the heading column. The text is encoded through replacing the characters of the text with the ones that are found by intersecting the corresponding row and column. Decoding is done by interchanging the rows and the columns [2].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 02. *Vigenere Table*

As an example, the plain text "STAY BEHIND THE HILL" can be encoded to "TEUCCPBMOONLFSCPM" with the above Vigenere Table using the keyword "BLUE".

Keyword: BLUEBLUEBLUEBLUEB
Plain Text: STAYBEHINDTHEHILL
Encoded Text: TEUCCPBMOONLFSCPM

2.2.2. Breaking Vigenere (Mono Alphabet) Ciphering Method

In Vigenere ciphering method, the length of the keyword can be determined by calculating the distance among the repeating patterns of the encoded text. If the length of the keyword is found as x, then it will be clear that the ciphering method is replacing with x-many, if the characters of the keyword are distinct, mono alphabets. At this point, for each mono alphabet encoded text, an attack that utilizes the frequencies of the characters of the plain text can be realized [2]. Below, frequency values of the characters of the English alphabet, i.e. the usage percentages of the characters in vernacular, are given [11].

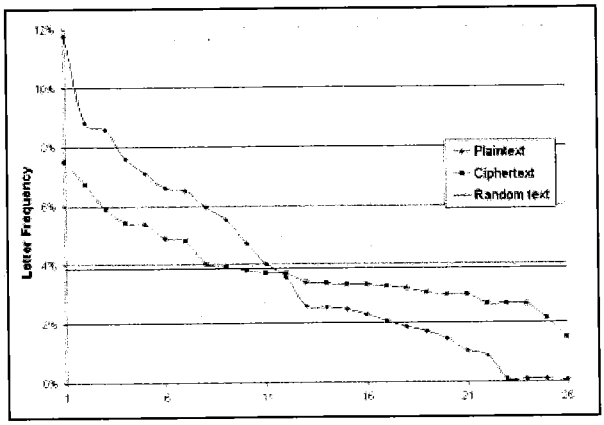

Figure 02. *Usage Freq. of the Characters of the English Alphabet*

Kasiski examination and Friedman test are two cryptanalysis methods to break the Vigenere (mono alphabet) ciphering. Kasiski examination makes use of the repeating character groups to find the length of the keyword. Friedman test can reveal the keyword, whose length was determined through Kasiski examination, with the help of the frequencies of the characters. As the encoded text gets longer, repeating character groups increase most of the time which increases the accuracy of these two methods. With these two methods, finding the shorter keyword is easier than breaking the longer one [1]. Kasiski examination works as follows [11]:

Step 1: Find the repeating character groups in the encoded text and count the number of characters among these.

Example:

Encoded text: YDUXRMHTVDVNQDQNWDYDUXRMHARTJGWNQD

Repeating Character Group 1: DYDUXRMH, repeats two times
Number of characters among groups: 18 characters

Repeating Character Group 2: NQD, repeats two times

Number of characters among groups: 20 characters

Step 2: Find the multipliers of the distance among the character groups.

Example:

Number of characters among groups: 18 characters
Multipliers: 18, 9, 6, 3, 2

Number of characters among groups: 20 characters
Multipliers: 20, 10, 5, 4, 2

Step 3: Determine the common multipliers of the distances. The common multiplier(s) is the possible character number of the keyword.

Example:

Common multiplier(s): 2
Possible character number of keyword: 2

After determination of the length of the keyword, making use of Friedman test and some statistical formulas see reference [5], the keyword can be found with the usage frequencies of the characters in the corresponding language.

2.INCREASING THE STRENGTH OF THE KEYWORD WITH ASAB – II TECHNIQUE

1.3. ASAB – II Technique

ASAB – II technique increases the number of characters of the keyword which is selected in Vigenere (mono alphabet) ciphering method without using any other key parameter by utilizing the property that the irrational numbers can be represented as periodic continuous fractions. It is more difficult or sometimes impossible to reach a keyword that has more characters. In ASAB – II technique, there is no change in byte requirement of the keyword in the communication media. Therefore, there is no increase in the transferring time of

the keyword in a secure electronic communication media. Moreover, if the keyword in the secure communication media is reached by third parties, it is not possible to decode the encrypted text since they get only the raw version of the keyword and without knowing the ASAB – II technique it is unable to find the processed keyword. The difference between the Vigenere (mono alphabet) ciphering and strengthen Vigenere (mono alphabet) with ASAB – II technique can be summarized with below figures.

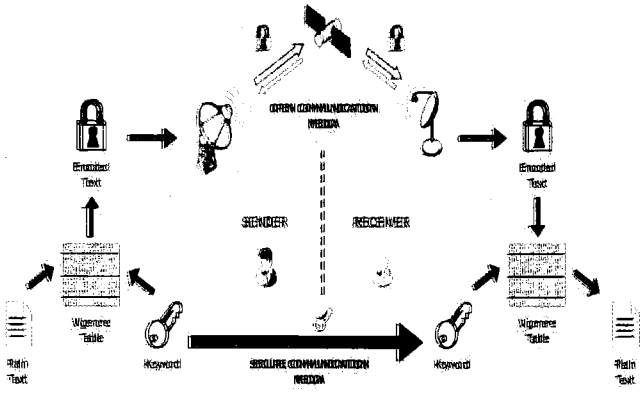

Figure 03. *Vigenere (Mono Alphabet) Ciphering*

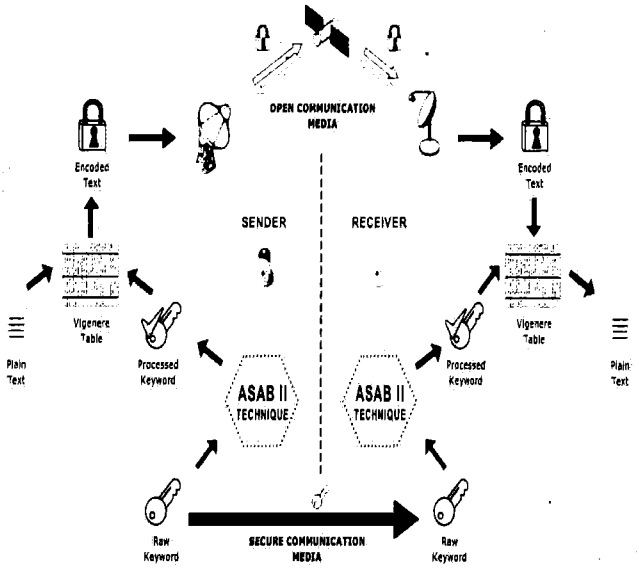

Figure 04. *Vigenere (Mono Alphabet) Ciphering strengthen with ASAB - II Technique*

1.4. Vigenere (Mono) Encoding with ASAB - II Technique

Step 1: Encoding with ASAB –II technique

1.1 Determine the plain text and the keyword.

Example:

Plain Text: VIGENEREPOWEREDBYASAB
Raw keyword: ASK

1.2 Calculate the sum (*T*) of the numerical values of the characters of the raw keyword.

Example:

Raw keyword: ASK

Numerical values: A = 0, S = 18, K = 10
Sum of the numerical values: $T = 0 + 18 + 10 = 28$

1.3 Calculate the periodic continuous fraction equivalent of the irrational number $\sqrt{T}$. If $\sqrt{T}$ is an integer, than use $\sqrt{T+1}$.

Example:

Irrational number: $\sqrt{28}$

$$k = 0 \quad \Rightarrow \quad a_0 = [\![\alpha_0]\!] = \mathbf{5}$$

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{28} - 5} = \frac{2\sqrt{7} + 5}{3}$$

$$k = 1 \quad \Rightarrow \quad a_1 = [\![\alpha_1]\!] = \left[\!\!\left[\frac{2\sqrt{7} + 5}{3}\right]\!\!\right] = \mathbf{3}$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{\sqrt{7} + 2}{2}$$

$$k = 2 \quad \Rightarrow \quad a_2 = [\![\alpha_2]\!] = \left[\!\!\left[\frac{\sqrt{7} + 2}{2}\right]\!\!\right] = \mathbf{2}$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{2\sqrt{7} + 4}{3}$$

$$k = 3 \quad \Rightarrow \quad a_3 = [\![\alpha_3]\!] = \left[\!\!\left[\frac{2\sqrt{7} + 4}{3}\right]\!\!\right] = \mathbf{3}$$

$$\alpha_4 = \frac{1}{\alpha_3 - a_3} = 2\sqrt{7} + 5$$

$$k = 4 \quad \Rightarrow \quad a_4 = [\![\alpha_4]\!] = [\![2\sqrt{7} + 5]\!] = \mathbf{10}$$

$$\alpha_5 = \frac{1}{\alpha_4 - a_4} = \frac{2\sqrt{7}+5}{3}$$

Since $\alpha_1 = \alpha_5$ we conclude that

$$\sqrt{28} = [5 : 3, 2, 3, 10, \ldots] = [2 : \overline{3, 2, 3, 10}]$$

1.4 Write the character equivalent of the numbers in the periodic part of the periodic continuous fraction.

Example:
Numbers in the periodic part of the fraction: 3, 2, 3, 10
Character equivalents of the numbers: D, C, D, K

1.5 Let n be the number of characters in raw keyword, and characters are represented with the sequence $a_1, a_2, \ldots, a_n$. Let m be the number of the character equivalents of the periodic part of the periodic continuous fraction, and the characters are represented with the sequence $p_1, p_2, \ldots, p_m$. Then, the processed keyword can be obtained as follows:

i. If $n > m$, the processed keyword is the sequence $a_1, p_1, a_2, p_2, \ldots, a_m, p_m, a_{m+1}, p_1, a_{m+2}, p_2, \ldots, a_n, p_{n-m}$.
ii. If $n = m$, the processed keyword is the sequence $a_1, p_1, a_2, p_2, \ldots, a_{n-1}, p_{m-1}, a_n, p_m$.
iii. If $n < m$, the processed keyword is the sequence $a_1, p_1, a_2, p_2, \ldots, a_n, p_n, p_{n+1}, p_{n+2}, \ldots, p_m$.

Example: Since $n < m$, the processed keyword can be obtained as

Raw keyword:	A		S		K		
Character equivalents of the periodic part of the fraction:		D		C		D	K
Processed keyword:	A	D	S	C	K	D	K

1.6 Encode the plain text with the processed keyword and the Vigenere Table.

Example:

Processed Keyword:	A	D	S	C	K	D	K	A	D	S	C
Plain Text:	V	I	G	E	N	E	R	E	P	O	W
Encoded Text:	V	L	Y	G	X	H	B	E	S	G	Y
Processed Keyword:	K	D	K	A	D	S	C	K	D	K	
Plain Text:	E	R	E	D	B	Y	A	S	A	B	
Encoded Text:	O	U	O	D	E	Q	C	C	D	L	

If the same plain text was encoded with the raw keyword, the following encoded text would be obtained:

Processed Keyword:	A	S	K	A	S	K	A	S	K	A	S
Plain Text:	V	I	G	E	N	E	R	E	P	O	W
Encoded Text:	V	A	Q	E	F	O	R	W	Z	O	O
Processed Keyword:	K	A	S	K	A	S	K	A	S	K	
Plain Text:	E	R	E	D	B	Y	A	S	A	B	
Encoded Text:	O	R	W	N	B	Q	K	S	S	L	

Therefore, we get the following encoded texts by two methods:

(1) Encoded text obtained by ASAB II Technique	VLYGXHBESGYOUODEQCCDL
(2) Encoded text obtained by Classical Vigenere Method	VAQEF**ORW**ZOO**ORW**NBQKSSL

As it can be seen above, there is no repeating character group in encoded text (1), whereas the character group "ORW" repeats and the distance among the groups is 6. According to Kasiski examination, one of the multipliers of 6, i.e. 6, 3 or 2, will be the possible length of the keyword. In our case, the keyword is "ASK" with three characters. Therefore, applying Kasiski examination to encoded text (2), one can possibly reach the keyword. On the other hand, in encoded text (1), there is no repeating character group which means Kasiski examination will not work for this case. From this result, it can be argued that the text (1) is encoded more effectively than the text (2). The performance comparison of Classical Vegenere Ciphering and Vegenere Ciphering strengthen with ASAB – II is tabulated in section 3.4 which supports our conclusion about ASAB – II technique here.

3.3. Vigenere (Mono Alphabet) Decoding with ASAB - II Technique

Step 2: Decoding with ASAB – II technique

2.1 Determine the processed keyword from the raw keyword that is obtained from the secure communication media by applying sub steps (1.2) – (1.5) in section 3.2.

2.2 The encoded text that is obtained from open communication media is decoded with the processed keyword that is found in previous step and the Vigenere Table.

Example:

Processed Keyword:	V	L	Y	G	X	H	B	E	S	G	Y
Plain Text:	A	D	S	C	K	D	K	A	D	S	C
Encoded Text:	V	I	G	E	N	E	R	E	P	O	W
Processed Keyword:	O	U	O	D	E	Q	C	C	D	L	
Plain Text:	K	D	K	A	D	S	C	K	D	K	
Encoded Text:	E	R	E	D	B	Y	A	S	A	B	

3.4. Performance Evaluation with Vigenere Cipher Cryptanalysis Program

Vigenere Cipher Cryptanalysis program, developed by Computer Sciences Department of Rhode Island University, includes an efficient web-based code breaking algorithm. The algorithm is capable to calculate the possible keyword length from the frequency values of the characters in the encrypted text, subdivides the encrypted text into length of the keyword many parts and finally reaches the keyword from the usage frequencies of the characters in English alphabet in vernacular [9].

Performance comparison of Classical Vigenere Ciphering (Technique I) and Vigenere Ciphering strengthen with ASAB – II technique (Technique II) is done via this program and the below figure and table are obtained. A random text in English of about 1000 characters is used as the plain text. Meaningful or meaningless keywords are selected of length varying from 2 to 10. For each keyword length, different encoded texts are generated using 100 different keywords and some tests are conducted with Vigenere Cipher Cryptanalysis program.

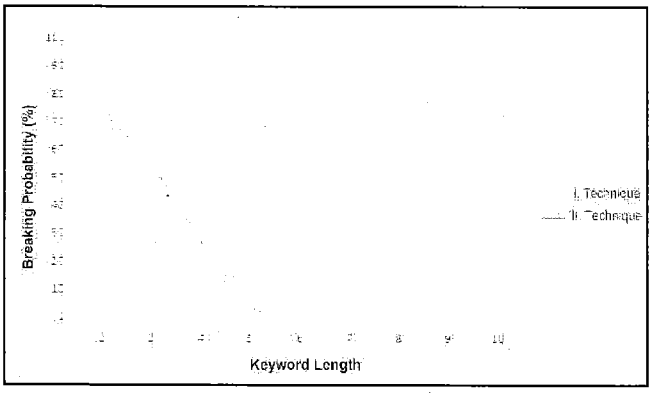

Figure 05. *Comparison of the Breaking Probabilities of the Techniques I and II According to Keyword Length*

Length of Keyword (n)	2	3	4	5	6	7	8	9	10
Ciphering Technique	Breaking Probability								
Technique I	%98	%95	%88	%76	%60	%39	%12	%1	%0
Technique II	%74	%55	%26	%3	%0	%0	%0	%0	%0

Table 03. *Comparison of the Breaking Probabilities of Two Techniques with the Vigenere Cipher Cryptanalysis Program*

3.CONCLUSION

This study aims to improve the keyword efficiency and reliability in Vigenere Ciphering Method, and it is observed that the proposed method works as desired. Kasiski algorithm, which is developed to break Vigenere encryption, tries to find the keyword. ASAB – II method strengthens the existing raw keyword by processing. Figure 05 show there is a significant shift among the lines that represent the affectivity of the keywords. For technique I, there is a positive probability to break the raw keyword of length less than or equal to 9, whereas for technique II it is 5. In other words, average of the breaking percentages is 47% for technique I, which drops to 16% for technique II.

This study also exhibits the close relationship among Mathematics and Cryptology. In particular, it points that existing classical and modern ciphering techniques can be upgraded or new ciphering techniques can be developed with the help of number theory and its sub topics. Becoming an outstanding cryptologist requires being an outstanding mathematician.

REFERENCES

Bauer, F.L., "*Decrypted Secrets: Methods and Maxims of Cryptology*", Third Edition, Springer-Verlag, Berlin, Heidelberg, Germany, 2002.

Dalgınç, G. & Akın, O. "*Anahtar Tabanlı Gelişmiş Rotor Makinesi*", Akademik Bilişim Konferansı, Gaziantep Üniversitesi, Gaziantep, 2-4 Şubat 2005.

Khinchin, A. Y., "*Continued Fractions*", Dover Publications, N.Y., U.S.A., 1997. (URL: http://books.google.co.uk/books ?id=R7Fp8vytgeAC, Last Visited: 09.10.2009)

Mutlu, Z., "*Cebirsel Sayılar Teorisinden Bazı Algoritmalar*", Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı, Yüksek Lisans Tezi, Danışman: Prof. Dr. Ali Bülent Ekin, Ankara, 2005.

Neuenschwander, D., "*Probabilistic and Statistical Methods in Cryptology*", Springer-Verlag, Berlin, Heidelberg, Germany, 2004.

Özdemir A. Ş. & Yaprakdal A. B.. "*A New Cryptology Technique (Asab) Using Finite Continued Fractions*", Proceedings of the Third International Conference on Modeling, Simulation and Applied Optimization, Sharjah, U.A.E January 20-22, 2009.

Sakallı, M. T. & Buluş, E. & Şahin, A. & Büyüksaraçoğlu, F. "*Bir Blok Şifreleme Algoritmasına Karşı Square Saldırısı*", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu ve Sergisi, İstanbul, 2005.

Rosen, K. H., "*Elementary Number Theory and its Applications*", Third Edition, Addison - Wesley Publishing Company, N.Y., U.S.A., 1992.

University of Rhode Island, "*Vigenere Cipher Cryptanalysis Interactive Demo Program*",
URL:http://www.cs.uri.edu/cryptography/classicalvigenerecryptdemo.htm, Last Visited: 05.12.2009.

Weisstein, Eric W. "*Periodic Continued Fraction*", MathWorld
URL: http://mathworld.wolfram.com/Periodic ContinuedFraction.html, Last Visited: 09.10.2009.

Wikipedia, "*Vigenère Cipher*"
URL: http://en.wikipedia.org/ wiki/Vigen%C3%A8re_ cipher, Last Visited: 10.10.2009.

Wikipedia, "*Vigenere Tablosu*"
URL: http://tr.wikipedia.org /wiki/Vigenere_tablosu, Last Visited: 11.10.2009.