JOURNAL OF
NATURAL SCIENCES
AND
MATHEMATICS RESEARCH

Available online at http://journal.walisongo.ac.id/index.php/jnsmr

Classical Cryptography of Wind's Eye Cell Circles

Razis Aji Saputro[1], Risti Sokawati[2], Mudrikah[3], Nikken Prima Puspita[4]
Departement of Mathematics Fakultas Sains dan Matematika Universitas Diponegoro, Jl. Prof.Soedarto, Kampus UNDIP Tembalang, 50275, Central Java, Indonesia

Abstracts

Corresponding author: razisaji25@gmail.com
Recived: 06 November 2016, Revised : 10 December 2016 Accepted: 27 December 2016.

This classic cryptographic algorithms was designed from the concept of cardinal directions and the S-box. circles Concept given 16 directions winds and 8 circles lined with each cells according to ASCII table. The process of encryption algorithm using two kinds of key symbol that are (k_1) form 16 symbols of the wind, and (k_2) is a 7-bit binary number. plaintext encryption process become chiperteks1 with forming angle against north wind and k1 roomates are from plaintext rotating accordance angle formed. Chipertext 1 to chipertext 2 using binary numbers divided become r_1 as directions displacement away from the center circle and r_2 move with rotating around the center circle. Spinning process followed directions clockwise circle if even if odd and vice versa. Decryption process is done by doing a backward on the algorithm by using the key k_2 (r_2 then r_1) and then r_1. Spins counter-encryption process. ©2016 JNSMR UIN Walisongo. All rights reserved.

Keywords: Cryptographic; Cardinal Direction; S-Box; Encryption; Decryption.

1. Introduction

Delivery of messages before the computer, so the message is not known to its meaning by the recipient of the unauthorized, then used the art in writing a message known as classical cryptography. Cryptography is a mathematical science that deals with data transformations aimed at making messages unintelligible, preventing them from unauthorized changes, or preventing them from unauthorized use. Cryptography can also be interpreted as a process of converting back from encrypted data into understandable form, meaning that cryptography can be interpreted as a process to protect data in a broad sense [1].

The more sophisticated the technology, cryptography developed from classical cryptography to modern cryptography. The cryptography discussed in this paper is the development of a classical algorithm designed from the S-box concept [2], added with the concept of 16 wind direction [3], and eight circles that all components will be associated with the circle name of the wind cell.

2. Cryptography

The basic concepts and terms used in cryptography that cryptography is a secret technique in writing, with special characters, using letters and characters outside of their original form, or by other methods that can only be understood by the parties who process the key , Also all things written down. So, in general can be interpreted as the art of writing or solving cipher [4].

Cryptography is one technique that can provide several services to improve the security of information such as authentication, non-repudiation, and confidentiality. Authentication is a service that relates to the identification of the message source's source. The encryption message is to convert the original message (plaintext) into a message in encrypted form (chiphertext). The encryption process will generate encrypted data and can only be opened or read by the recipient who has the key while the description process is returning the encoded data to the original form. The encryption process and the description performed by using the same key are known by the cryptographic cryptography of the symmetry algorithm.

In this type of algorithm, the key is confidential and should be known only to the sender and recipient only. In addition to cryptographic algorithms the key symmetry has been developed as well as cryptographic algorithms asymmetry keys, namely the encryption process and descriptions performed by using different keys. There is a key pair of public keys that are used for the encryption process and the private key (private key) is used for the description process. The public key is not confidential and should be known to the sender when it encrypts the data. Conversely for private key is confidential and only known by data recipient.

3. Results and Discussion

In this study, we transformed the characters in the ASCII table into a repeating loop forming several cells, as in the Figure 1.

The reference angle used in the circle of the eye cell is the northern axis, the northern axis moves clockwise to rotate 360 degrees. The picture of the circle is divided into 16 parts based on the number of 16 wind direction, the distance for each angle between the direction of the wind is 22.5 degrees. Each wind direction is symbolized by number 0 by 15 in a clockwise order which will then be used as key 1 (k1). Generate the Table 1.

In the circle of the cell of the eye of the wind in a square condition there is up to. As the first odd circle, and as the first even circle as well as so forth to arrive. Which one shifts clockwise, while it shifts counter-clockwise. And then the cell shifts from the pivot circle to the outer circle. So when the main axis split will produce the Figure 2.

Table 1. Provisions of Angular Axis

AMA	Large Angle (∠)	k_1	AMA	Large Angle (∠)	k_1
U	0^0	0	S	170^0	8
UTL	22.5^0	1	SBD	202.5^0	9
TL	45^0	2	BD	225^0	10
TTL	67.5^0	3	BBD	247.5^0	11
T	90^0	4	B	270^0	12
TTG	112.5^0	5	BBL	292.5^0	13
TG	125^0	6	BL	315^0	14
STG	157.5^0	7	UBL	337.5^0	15

Note: The angle is calculated from the northern axis.

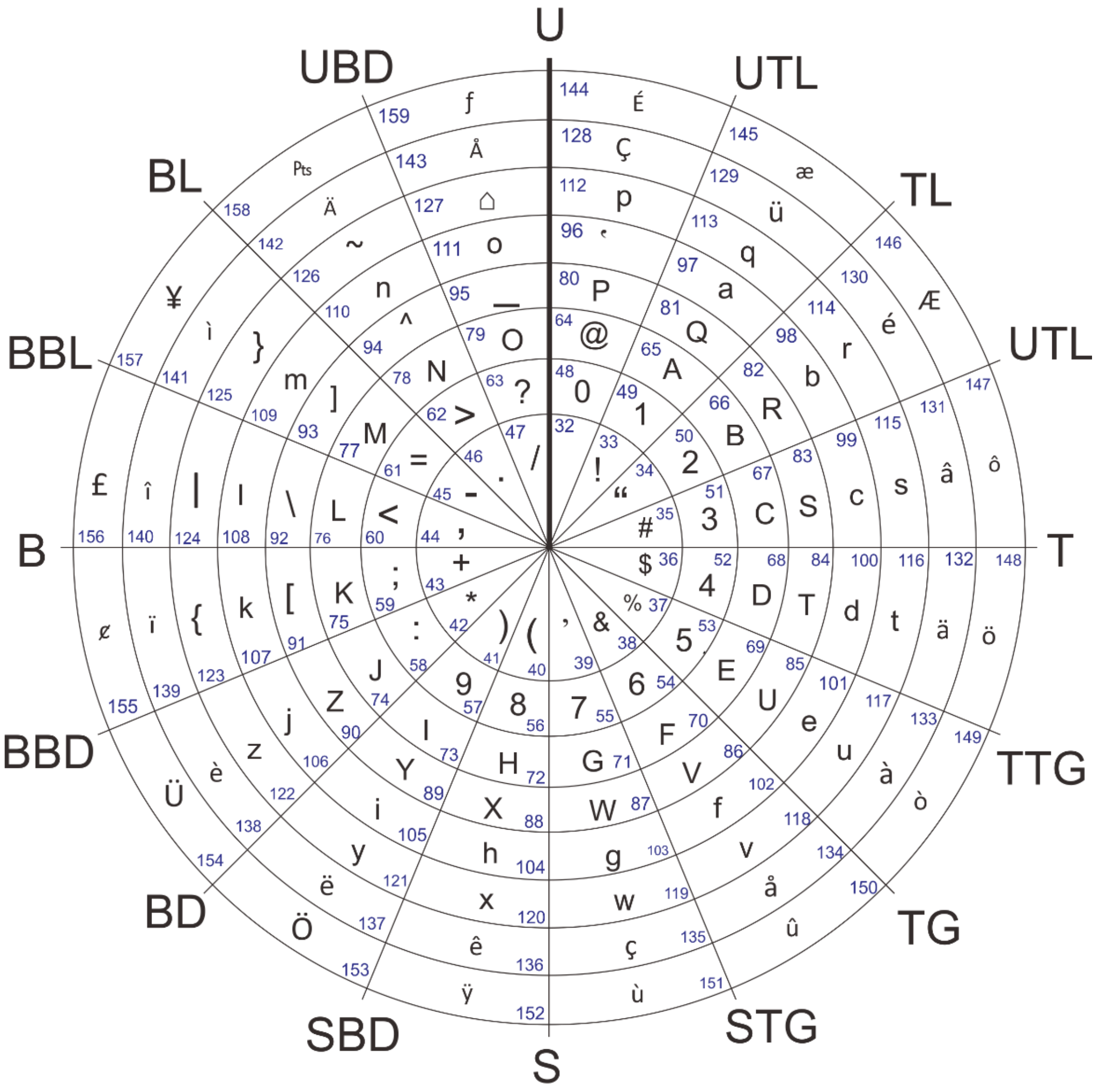
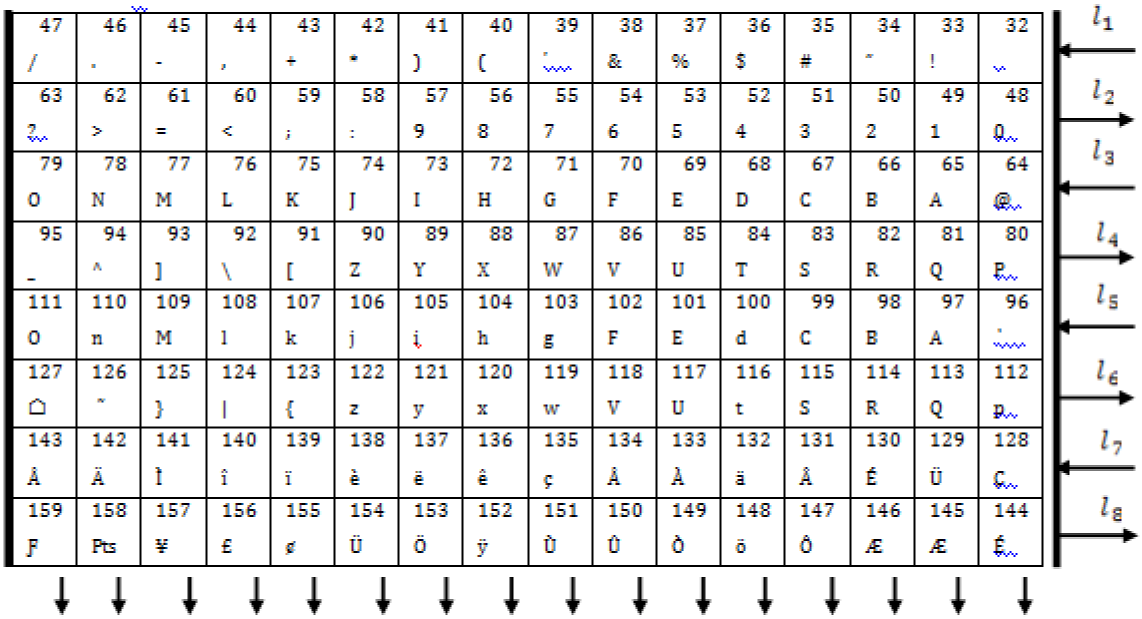


Figure 1. Wind Cell End Circle



47 /	46 .	45 -	44 ,	43 +	42 *	41)	40 (	39 '	38 &	37 %	36 $	35 #	34 "	33 !	32	l_1 ←
63 ?	62 >	61 =	60 <	59 ;	58 :	57 9	56 8	55 7	54 6	53 5	52 4	51 3	50 2	49 1	48 0	l_2 →
79 O	78 N	77 M	76 L	75 K	74 J	73 I	72 H	71 G	70 F	69 E	68 D	67 C	66 B	65 A	64 @	l_3 ←
95 _	94 ^	93]	92 \	91 [	90 Z	89 Y	88 X	87 W	86 V	85 U	84 T	83 S	82 R	81 Q	80 P	l_4 →
111 O	110 n	109 M	108 l	107 k	106 j	105 i	104 h	103 g	102 F	101 E	100 d	99 C	98 B	97 A	96 `	l_5 ←
127 ⌂	126 ~	125 }	124 |	123 {	122 z	121 y	120 x	119 w	118 V	117 U	116 t	115 S	114 R	113 Q	112 p	l_6 →
143 Å	142 Ä	141 Ì	140 î	139 ï	138 è	137 ë	136 ê	135 ç	134 å	133 à	132 ä	131 â	130 é	129 ü	128 Ç	l_7 ←
159 ƒ	158 Pts	157 ¥	156 £	155 ¢	154 Ü	153 Ö	152 ÿ	151 ù	150 û	149 ò	148 ö	147 ô	146 Æ	145 æ	144 É	l_8 →
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	

Figure 2. Windspace Cell Circle in square condition

The decimal on ASCII contained in each interval in the windblow cell image with N is the original number.

$l_1 = [32,47] \in N$	$l_5 = [96,111] \in N$
$l_2 = [48,63] \in N$	$l_6 = [112,127] \in N$
$l_3 = [64,79] \in N$	$l_7 = [128,143] \in N$
$l_4 = [80,95] \in N$	$l_8 = [144,159] \in N$

The encryption and decryption algorithms are organized as follows:

A. Encryption of Algorithm

1. Select $\boxed{k_1}$ k_2 as the sender of the message.
2. Each character on plaintext will be encrypted into C_1 by k_1 and then encrypted again into C_2 by k_2. C_1 is a 16-way wind symbol (T, TTG, TG, STG, S, SBD, BD, BBD, B, BBL, BL, UBL, U, TL, TTL) and k_2 is a 7 bit binary number.
3. Plaintext (P) will be encrypted from P_1 to P_n, where $P=P_i=P_1P_2P_3 \ldots P_n$, i=1,2,3,...,n.
4. Changing P to C_1 using $\boxed{k_1}$, where $C_1=C_{1i}=C_{11}C_{12}C_{13} \ldots C_{1n}$, i=1,2,3,...,n.

$$C_{1i} \begin{cases} \text{if } P_i \in l_{ganjil} \begin{cases} C_{1i}' = P_i + k_1 & , C_{1i}' \in l_{ganjil} \\ C_{1i}' - 16 & , C_{1i}' \notin l_{ganjil} \end{cases} \\ \text{if } P_i \in l_{genap} \begin{cases} C_{1i}' = P_i + (16- k_1) & , C_{1i}' \in l_{genap} \\ C_{1i}' - 16 & , C_{1i}' \notin l_{genap} \end{cases} \end{cases}$$

Note: even odd circles follow the origin of the circle from P_i

5. Changing C_1 to C_2 using k_2 . where $C_2=C_{2i}=C_{21}C_{22}C_{23} \ldots C_{2n}$ i=1,2,3,...,n.
   a). k_2 is a 7-bit binary number so obtained $b_1b_2b_3b_4b_5b_6b_7$.
   b).Define, b1b4b7 as r_1 and $b_2b_3b_5b_6$ as r_2.
   c). C_1 will be converted first into S by using r1, where $S=S_i=S_1S_2S_3 \ldots S_n$.
   Define $S_i' = 16\ r_1+C_{1i}$

$$S_i \begin{cases} S_i' & , 32 \leq S_i' \leq 159 \\ (S_i' \bmod 159) + 31 & , S_i' > 159 \end{cases} \qquad [5]$$

d).Then change from S to C_2 using r_2, that is:

$$C_2 \begin{cases} \text{if } S_i \in l_{ganjil} & \begin{cases} C_{2i}' = S_i + r_2 & , C_{2i}' \in l_{ganjil} \\ C_{2i}' - 16 & , C_{2i}' \notin l_{ganjil} \end{cases} \\ \text{if } S_i \in l_{genap} & \begin{cases} C_{2i}' = S_i + (16 - r_2) & , C_{2i}' \in l_{genap} \\ C_{2i}' - 16 & , C_{2i}' \notin l_{genap} \end{cases} \end{cases}$$

Note: even odd circles follow the origin of C_2 circle

B. Decryption of Algorithm

The process of describing the message with the wind circle cell algorithm, namely:

First step

1. Changing C_2 to C_1 using k_2. where $C_1 = C_{1i} = C_{11}C_{12}C_{13} \ldots C_{1n}$ $i = 1,2,3,\ldots,n$.
   a) K2 is a 7-bit binary number so obtained $b_1b_2b_3b_4b_5b_6b_7$.
   b) Define, $b_1b_4b_7$ as r_1 and $b_2b_3b_5b_6$ as r_2.
   c) For odd and odd circular directions even in opposite directions with encryption.
   d) Then change from C_2 to S using r_2, with $S = S_i = S_1S_2S_3 \ldots S_n$ that is:

$$S \begin{cases} \text{if } S_i \in l_{ganjil} & \begin{cases} S_i' = C_{2i} - r_2 & , S_i' \in l_{ganjil} \\ S_i' - 16 & , S_i' \notin l_{ganjil} \end{cases} \\ \text{If } S_i \in l_{genap} & \begin{cases} S_i' = C_{2i} - (16 - r_2) & , S_i' \in l_{genap} \\ S_i' - 16 & , S_i' \notin l_{genap} \end{cases} \end{cases}$$

   e) S will be converted to C_1 by using r1,
   Define S - 16 r_1

$$C_{1i} \begin{cases} S - 16r_1 \\ (159 + (S - 31)) - (16r_1) \end{cases}$$

At this stage it produces 2 different C_1 possibilities, then in the process all so it will get the right plaintext results.

2. Converting C1 to P using $\boxed{k_1,}$

$$P_i \begin{cases} \text{if } C_{1i} \in l_{ganjil} & \begin{cases} P_i' = C_{1i} - k_1 & , P_i' \in l_{ganjil} \\ P_i' + 16 & , P_i' \notin l_{ganjil} \end{cases} \\ \text{if } C_{1i} \in l_{genap} & \begin{cases} P_i' = C_{1i} - (16 - k_1) & , P_i' \in l_{genap} \\ P_i' + 16 & , P_i' \notin l_{genap} \end{cases} \end{cases}$$

Step Algorithm

Encryption

Plaintext to Cipherteks 1 (Figure 3)

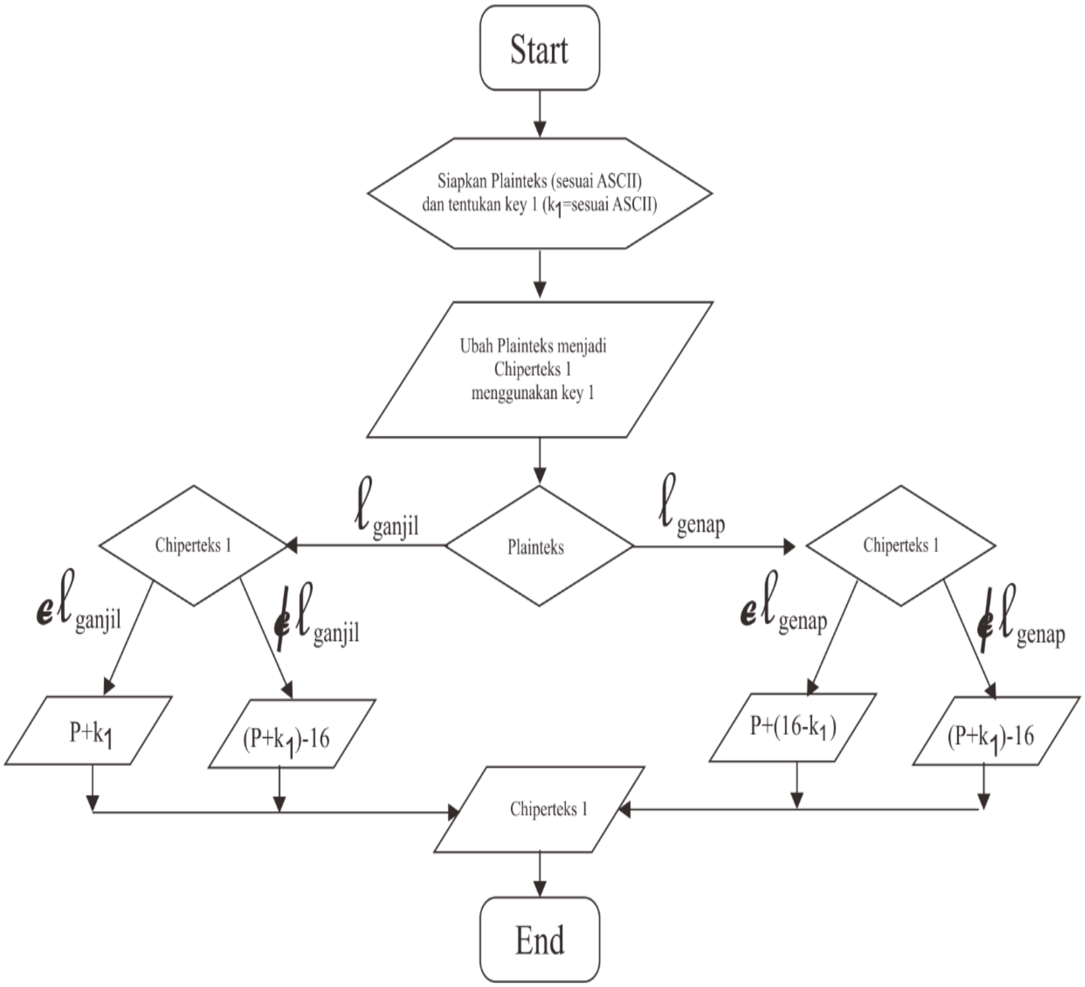


Figure 3. Plaintext to Cipherteks 1

Chipertext 1 to Cipherteks 2:

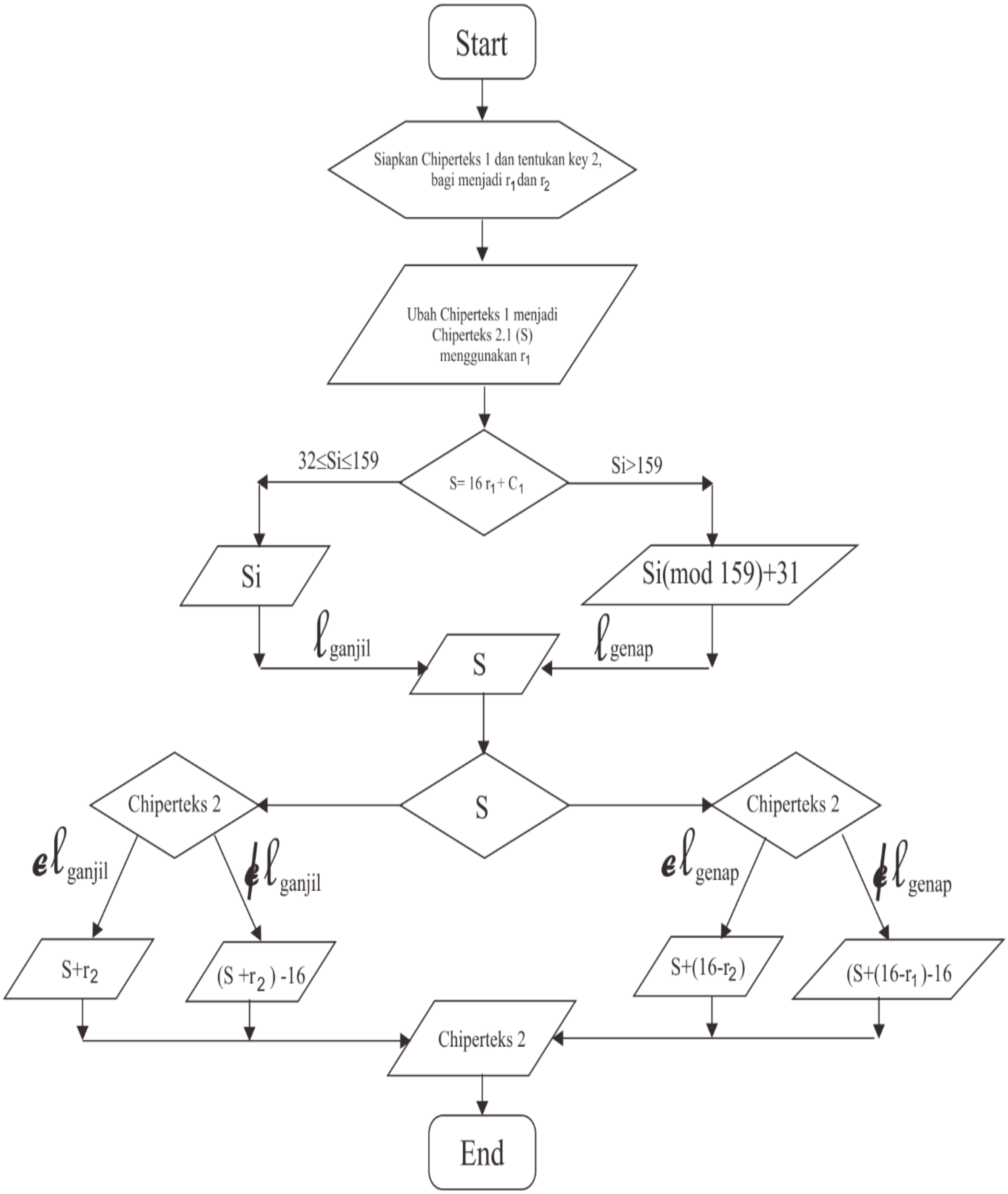


Figure 4, Chipertext 1 to Cipherteks 2

Decryption

Chipertext 2 to Cipherteks 1:

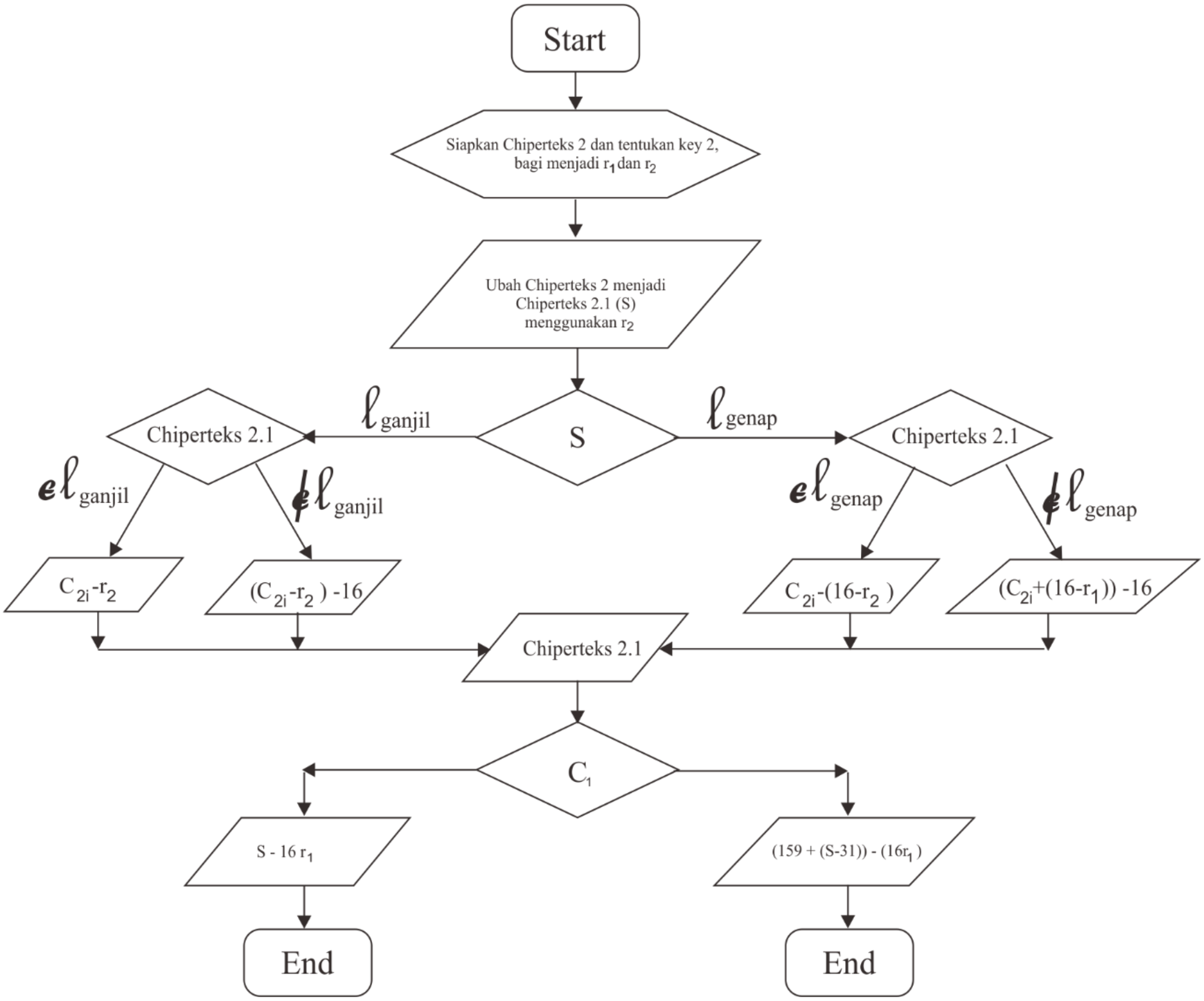


Figure 5. Chipertext 2 to Cipherteks 1

It should be noted that the search is appropriate so that at the end of the plaintext can be a clear sentence.

Cipherteks 1 to Plainteks:

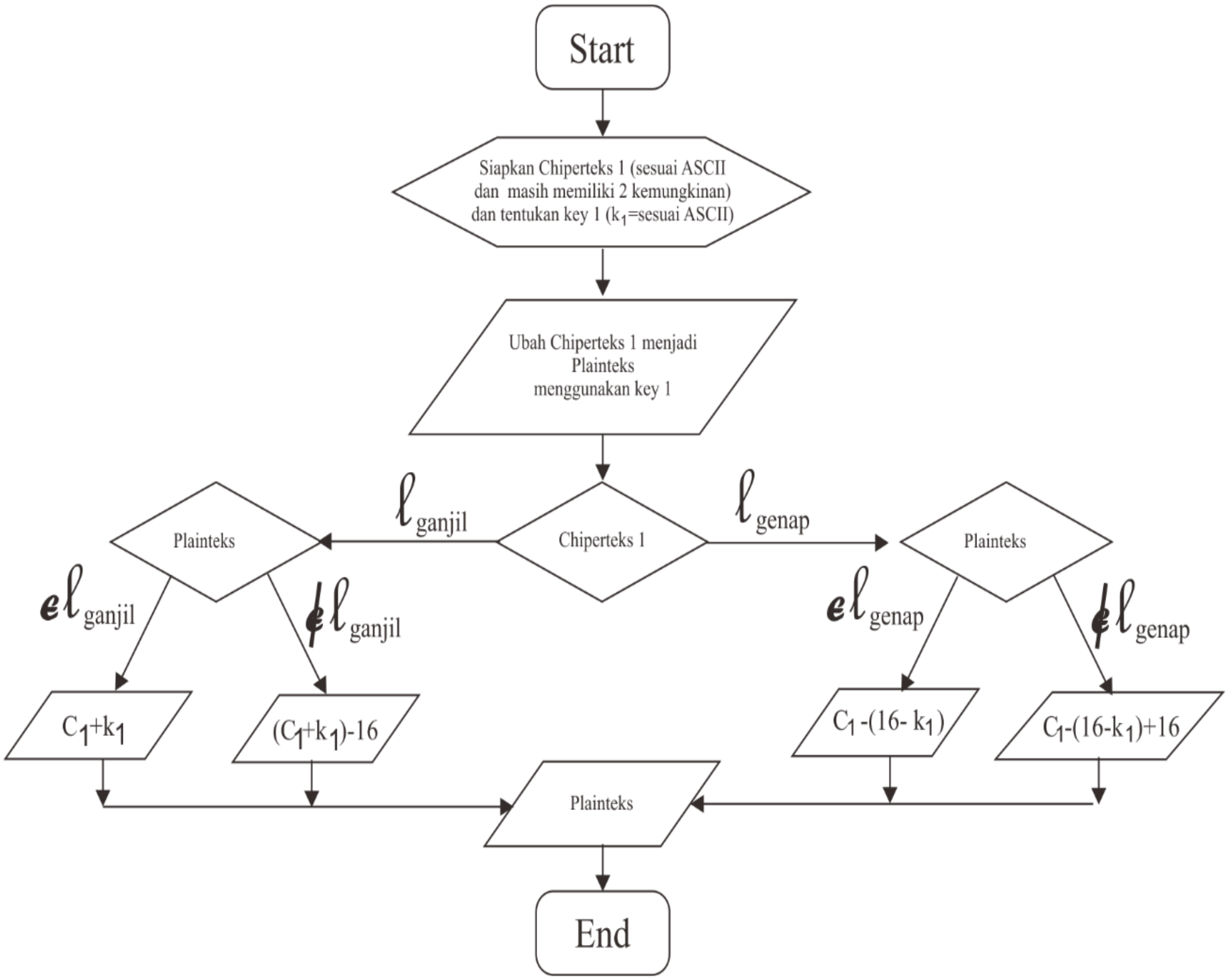


Figure 6. Cipherteks 1 to Plainteks

4. Conclusion

Wind blow cell circles are simple examples of cryptography by utilizing ASCII codes from 32 to 159, cells in circles, and binary number operations. From the concept of S-Box that usually only use a square shape can be transformed in the form of a circle. Encryption and decryption process can be done by the sender of the message manually and computer. If the text is sent long enough, it will be difficult for users of this algorithm to perform calculations manually. Thus to speed up the process, can use the computer program with the algorithm that has been given in the previous section.

Acknowledgment

Departement of Mathematics Fakultas Sains dan Matematika Universitas Diponegoro for supporting this work.

References

[1] R. Oppliger, *Contemporary Cryptography*. Artech House, Inc : Bandung : 2005.
[2] S. Kromodimoeljo, *Teori dan Aplikasi Kriptografi*. SPK IT Consulting. 2009.
[3] J.Talbot, and D. Welsh. *Complexity and Cryptography*. USA : Cambridge University Press. 2006.
[4] R. Munir, *Matematika Diskrit*. Bandung : Informatika. 2012.
[5] Wikipedia Bahasa Indonesia. *Boxing the compass*. https://id.wikipedia.org/wiki/Boxing_the_compass , 27 September 2016.
[6] Documents.tips.*16 Arah Mata Angin dan Besar Derajatnya.*. http://documents.tips/documents/16-arah-mata-angin-dan-besar-derajatnya, 6 Desember 2016.