Control and Cybernetics

vol. **45** (2016) No. 2

Uses of second order variant Fibonacci universal code in cryptography*

by

Manjusri Basu, Monojit Das

Department of Mathematics,
University of Kalyani,
Kalyani, W.B., 741235, India,
manjusri_basu@yahoo.com
monojitbhu@gmail.com

Abstract: We know from Zeckendorf's theorem that every positive integer n has unique representation of the form $n = \sum_{k=1}^{l} a_k F(k)$, where $a_k \in \{0, 1\}$ and $F(k)$ is a Fibonacci number such that the string $a_1 a_2 a_3 \ldots$ does not contain any consecutive 1's. In this paper we consider second order variant Fibonacci universal code from Gopala-Hemachandra sequence. Thereby, we describe the uses of this code in cryptography with an illustrative example.

Keywords: Fibonacci numbers, Fibonacci coding, Gopala-Hemachandra sequence, Zeckendorf's representation, Gopala-Hemachandra code, GH code straight line, cryptography

1. Introduction

Fibonacci number $F(k)$ $(k = 0, \pm 1, \pm 2, \ldots.)$ is defined by the second order linear recurrence relation

$$F(k) = F(k-1) + F(k-2), \tag{1}$$

where $F(1) = 1$, $F(2) = 2$.
Some Fibonacci numbers are summarized in Table 1.

Table 1. Fibonacci numbers

k	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8
$F(k)$	13	-8	5	-3	2	-1	1	0	1	1	2	3	5	8	13	21	34

Fibonacci universal coding encodes positive integers into binary codewords to obtain Fibonacci universal code by applying Zeckendorf's theorem, namely

*Submitted: December 2015; Accepted: October 2016.

"Every positive integer has a unique representation as the sum of non consecutive Fibonacci numbers" (Zeckendorf, 1972). In other words, this theorem conveys that every positive integer n has unique representation of the form $n = \sum_{k=1}^{l} a_k F(k)$ where $a_k \in \{0, 1\}$ and $F(k)$ is a Fibonacci number such that the string $a_1a_2a_3\ldots$ does not contain any consecutive 1's. This representation is defined as Zeckendorf's representation, Daykin (1960). Therefore, when the recursive nature of Fibonacci numbers allow some integers to have multiple representations using the above process, then Zeckendorf's representation is unique, e.g., 10 can be represented in Fibonacci numbers as $F(2)+F(3)+F(4)$ or $F(2) + F(5)$, and then in Zeckendorf's representation, it is $F(2) + F(5)$. Fibonacci universal codewords end with 11 and have no consecutive 1's before the end. The following steps illustrate a method to encode Fibonacci universal code with the help of Zeckendorf's theorem.

Step 1. By Zeckendorf's Theorem, set $n = F(i_1) + F(i_2) + \ldots + F(i_p)$, where $F(i_1)$ is the largest Fibonacci number less than or equal to n, $F(i_2)$ is the largest Fibonacci number less than or equal to $n - F(i_1)$ and so on. And it is obviously finite.

Step 2. Put 1 in the i_1th, i_2th, $\ldots$, i_pth position, while the remaining positions are all zeros.

Step 3. Put a 1 at the end to encode the positive integer n, so that the codeword ends with 11 and has no consecutive 1 before the end, by Zeckendorf's theorem.

Table 2 represents the Fibonacci universal code of n. Thus, Fibonacci uni-

Table 2. Fibonacci universal code of n

n	Zeckendorf's representation	Fibonacci representation	Fibonacci universal code
1	F(1)	1	11
2	F(2)	01	011
3	F(3)	001	0011
4	F(1) + F(3)	101	1011
5	F(4)	0001	00011
6	F(1) + F(4)	1001	10011
7	F(2) + F(4)	0101	01011
8	F(5)	00001	000011
9	F(1) + F(5)	10001	100011
10	F(2) + F(5)	01001	010011
11	F(3) + F(5)	00101	001011
12	F(1) + F(3) + F(5)	10101	101011
13	F(6)	000001	0000011
14	F(1) + F(6)	100001	1000011
15	F(2) + F(6)	010001	0100011

versal code is a prefix code of variable size. Therefore, it is uniquely decodable binary code. One disadvantage of this representation is that the code size of the integer n is $1 + \lfloor log_2 n \rfloor$. The property of not having adjacent 1 bits restricts the number of binary patterns available for such codes, and so they are longer than the other existing well known codes. Although, it is not asymptotically optimal, it performs well compared to the Elias code (Elias, 1975) as long as the number of source message is not too large. The Fibonacci universal code has the additional attribute of robustness, which manifests itself by the local containment of errors.
Fibonacci universal code has a useful property that sometimes makes it attractive in comparison to other universal codes. It is easier to recover data from a damaged stream. With most of the other universal codes, if a single bit is altered, none of the data that come after it may be correctly read. On the other hand, with Fibonacci universal coding, a changed bit may cause one token to be read as two, or cause two tokens to be read incorrectly as one, but reading a 0 from the stream will stop the errors from propagating further. The total edit distance between a stream damaged by a single bit error and the original stream is at most three, since the only stream that has no 0 in it is a stream of 11 tokens.

2. Gopala-Hemachandra sequence and code

The more general Gopala-Hemachandra (GH) sequence (Kak, 2006) of the Fibonacci sequence is $\{a, b, a+b, a+2b, 2a+3b, \ldots\}$ for any a, $b \in \mathbb{Z}$, the set of integers. The GH sequence represents the Fibonacci sequence for $a = 1$ and $b = 2$. The historical details of these sequences are discussed in Kak (2006, 2008) and Pearce (2002).
For $b = 1-a$, the GH sequence $\{a, 1-a, 1, 2-a, \ldots\}$ is the second order Variant Fibonacci sequence $VF_a(k)$. Also,

$$VF_a(k) = VF_a(k-1) + VF_a(k-2), \ k \geq 3 \tag{2}$$

with the initial terms $VF_a(1) = a$; $VF_a(2) = 1 - a$, where $a \in \mathbb{Z}$, the set of integers.
Some second order Variant Fibonacci numbers are displayed in Table 3.

In 1960, Daykin (1960) proved that only the standard Fibonacci sequence $F(k)$ gives a unique Zeckendorf's representation for all positive integers . Thomas (2007) showed that for the sequence $VF_{-5}(k)$, it is not possible to write Zeckendorf's representation for integers 5 and 12. In 2010, for $-2 \leq a \leq -20$ Basu and Prasad (2010) improved the availability of the GH code up to the positive integer 100, as given in Tables 4 through 7.
The following theorem proves the relation between the Gopala-Hemacandra sequence $VF_a(k)$ and the Fibonacci sequence $F(k)$ for any integer $k \geq 1$ (Basu, Das and Bagchi, 2016).

Theorem 2.1 $VF_a(k) = F(k-2) - aF(k-4), \quad k \geq 1.$

Table 3. Second Order Variant Fibonacci Numbers

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$VF_{-2}(k)$	-2	3	1	4	5	9	14	23	37	60	97	157	254	411
$VF_{-3}(k)$	-3	4	1	5	6	11	17	28	45	73	118	191	309	500
$VF_{-4}(k)$	-4	5	1	6	7	13	20	33	53	86	139	225	364	589
$VF_{-5}(k)$	-5	6	1	7	8	15	23	38	61	99	160	259	419	678
$VF_{-6}(k)$	-6	7	1	8	9	17	26	43	69	112	181	293	474	767
$VF_{-7}(k)$	-7	8	1	9	10	19	29	48	77	125	202	327	529	856
$VF_{-8}(k)$	-8	9	1	10	11	21	32	53	85	138	223	361	584	1168
$VF_{-9}(k)$	-9	10	1	11	12	23	35	58	93	151	244	395	639	1034
$VF_{-10}(k)$	-10	11	1	12	13	25	38	63	101	164	265	429	694	1123

Proof We have, from the equation (2)

$$VF_a(k) = \{a, 1-a, 1, 2-a, 3-a, 5-2a, 8-3a, 13-5a, 21-8a, \ldots\}.$$

Therefore, we can write, by using Table 1

$$VF_a(1) = a = 0 - a(-1) = F(-1) - aF(-3) = F(1-2) - aF(1-4)$$

and

$$VF_a(2) = 1 - a(1) = F(0) - aF(-2) = F(2-2) - aF(2-4).$$

Thus, the result is true for $k = 1$ and 2.
Let the result be true for $k = 1, 2, 3, \ldots, m$.
Then, $VF_a(m-1) = F(m-3) - aF(m-5)$ and $VF_a(m) = F(m-2) - aF(m-4)$.

Therefore, $VF_a(m+1) = VF_a(m) + VF_a(m-1) = F(m-3) - aF(m-5) + F(m-2) - aF(m-4) = (F(m-3) + F(m-2)) - a(F(m-5) + F(m-4)) = F(m-1) - aF(m-3) = F(\overline{m+1} - 2) - aF(\overline{m+1} - 4)$.

Hence by the induction, we can write

$$VF_a(k) = F(k-2) - aF(k-4), \quad k \geq 1. \tag{3}$$

□

Basu, Das and Bagchi (2016) describe for what value of a particular positive integer n and for what particular value of $a \in \mathbb{Z}$, the Gopala-Hemachandra codeword exists.

Definition 2.1 *The straight line $y + mx = c$ is called GH code straight line if all the integral points (a, n) for $a \leq -2$, $n \geq 1$ on this straight line have GH codeword. Otherwise it is called Non-GH code straight line.*

3. Properties of GH sequence and GH code for $a \leq -2$

THEOREM 3.1 *The GH codewords for* $n = 1, 2, 3, 4$ *always exist and are* 0011, 10011, 100011, 101011 *respectively for all* a.

PROOF The GH sequence $VF_a(k)$ is $\{a, 1-a, 1, 2-a, 3-a, 5-2a, 8-3a, \ldots\}$
So, $1 = VF_a(3)$. Hence, for $n = 1$, the GH codeword is 0011 for all a.
$2 = VF_a(1) + VF_a(4)$. Hence, for $n = 2$, the GH codeword is 10011 for all a.
$3 = VF_a(1) + VF_a(5)$. Hence, for $n = 3$, the GH codeword is 100011 for all a.
$4 = VF_a(1) + VF_a(3) + VF_a(5)$. Hence, for $n = 4$, the GH codeword is 101011 for all a.
Hence the theorem. □

THEOREM 3.2 *The GH codeword always exists for* $a = -2, -3, -4$ *and* $n \geq 1$.

PROOF We prove the theorem by induction. Tables 3 4 show that the GH codeword exists for $n = 1, 2, 3, \ldots, 100$ and $a = -2, -3, -4$. Let GH codeword exist up to $n = m\,(\geq 100)$ and $a = -2, -3, -4$.
If $m + 1 \in VF_a(k)$ for $a = -2, -3, -4$, then obviously the GH codeword exists for $n = m + 1$.

Let $m + 1 \notin VF_a(k)$ for $a = -2, -3, -4$. Let $m_a = VF_a(i_a)$ be the greatest number, but not greater than $m + 1$, where $i_a \neq 1$ for $a = -2, -3, -4$. Then, it is obvious that $(\overline{m+1} - m_a) < m$ and $(\overline{m+1} - m_a) < VF_a(i_a - 1)$, since $VF_a(k) = VF_a(k-1) + VF_a(k-2)$ for $a = -2, -3, -4$.

Then, the codeword corresponding to $n = m + 1$ exists and it will be the codeword of $(\overline{m+1} - m_a)$, with deleting the last 1 and with i_ath and $(i_a + 1)$th positions equal 1 and the remaining positions all being equal 0.
Hence the theorem. □

PROPERTY 3.1 *For* $a \leq -2$*, we have four straight lines* $y + 0x = 0 + j$*, for* $j = 1, 2, 3, 4$*, such that the four points* $(a, 1-0a)$*,* $(a, 2-0a)$*,* $(a, 3-0a)$*,* $(a, 4-0a)$ *lie on these lines for* $j = 1, 2, 3, 4$*, respectively, which gives the respective GH codewords being* 0011*,* 10011*,* 100011*,* 101011.

PROPERTY 3.2 *For* $a \leq -2$*, we have six straight lines* $y + x = 0 + j$*, for* $j = 1, 2, \ldots 6$*, such that the six points* $(a, 1-a)$*,* $(a, 2-a)$*, …,* $(a, 6-a)$ *lie on these lines for* $j = 1, 2, \ldots, 6$*, respectively, which gives the respective GH codewords* 011*,* 00011*,* 000011*,* 001011*,* 1000011*, and* 1010011.

PROPERTY 3.3 *For* $a \leq -2$*, we have seven straight lines* $y + 2x = 2 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 3-2a)$*,* $(a, 4-2a)$*, …,* $(a, 9-2a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 01011*,* 010011*,* 0000011*,* 0010011*,* 1001011*,* 10000011 *and* 10100011.

Property 3.4 *For* $a \leq -2$*, we have seven straight lines* $y + 3x = 5 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 6 - 3a)$*,* $(a, 7 - 3a)$*, ...,* $(a, 12 - 3a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 0100011*,* 0001011*,* 00000011*,* 00100011*,* 10010011*,* 10001011 *and* 10101011*.*

Property 3.5 *For* $a \leq -2$*, we have seven straight lines* $y + 4x = 7 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 8 - 4a)$*,* $(a, 9 - 4a)$*, ...,* $(a, 14 - 4a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 0101011*,* 01000011*,* 00010011*,* 00001011*,* 00101011*,* 100000011 *and* 101000011*.*

Property 3.6 *For* $a \leq -2$*, we have seven straight lines* $y + 5x = 10 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 11 - 5a)$*,* $(a, 12 - 5a)$*, ...,* $(a, 17 - 5a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 01010011*,* 01001011*,* 000000011*,* 001000011*,* 100100011*,* 100010011 *and* 101010011*.*

Property 3.7 *For* $a \leq -2$*, we have six straight lines* $y + 6x = 13 + j$*, for* $j = 1, 2, \ldots 6$*, such that the six points* $(a, 14 - 6a)$*,* $(a, 15 - 6a)$*, ...,* $(a, 19 - 6a)$ *lie on these lines for* $j = 1, 2, \ldots, 6$*, respectively, which gives the respective GH codewords* 010000011*,* 000100011*,* 000010011*,* 001010011*,* 100001011 *and* 101001011*.*

Property 3.8 *For* $a \leq -2$*, we have seven straight lines* $y + 7x = 15 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 16 - 7a)$*,* $(a, 17 - 7a)$*, ...,* $(a, 22 - 7a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 010100011*,* 010010011*,* 000001011*,* 001001011*,* 100101011*,* 1000000011 *and* 1010000011*.*

Property 3.9 *For* $a \leq -2$*, we have seven straight lines* $y + 8x = 18 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 19 - 8a)$*,* $(a, 20 - 8a)$*, ...,* $(a, 25 - 8a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 010001011*,* 000101011*,* 0000000011*,* 0010000011*,* 1001000011*,* 1000100011 *and* 1010100011*.*

Property 3.10 *For* $a \leq -2$*, we have seven straight lines* $y + 9x = 20 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 21 - 9a)$*,* $(a, 22 - 9a)$*, ...,* $(a, 27 - 9a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 010101011*,* 0100000011*,* 0001000011*,* 0000100011*,* 0010100011*,* 1000010011 *and* 1010010011*.*

Property 3.11 *For* $a \leq -2$*, we have seven straight lines* $y + 10x = 23 + j$*, for* $j = 1, 2, \ldots 7$*, such that the seven points* $(a, 24 - 10a)$*,* $(a, 25 - 10a)$*, ...,* $(a, 30 - 10a)$ *lie on these lines for* $j = 1, 2, \ldots, 7$*, respectively, which gives the respective GH codewords* 0101000011*,* 0100100011*,* 0000010011*,* 0010010011*,* 1001010011*,* 1000001011 *and* 1010001011*.*

Property 3.12 *For $a \leq -2$, we have seven straight lines $y + 11x = 26 + j$, for $j = 1, 2, \ldots 7$, such that the seven points $(a, 27 - 11a)$, $(a, 28 - 11a)$, …, $(a, 33 - 11a)$ lie on these lines for $j = 1, 2, \ldots, 7$, respectively, which gives the respective GH codewords* 0100010011*,* 0001010011*,* 0000001011*,* 0010001011*,* 1001001011*,* 1000101011 *and* 1010101011*.*

Property 3.13 *For $a \leq -2$, we have seven straight lines $y + 12x = 28 + j$, for $j = 1, 2, \ldots 7$, such that the seven points $(a, 29 - 12a)$, $(a, 30 - 12a)$, …, $(a, 35 - 12a)$ lie on these lines for $j = 1, 2, \ldots, 7$, respectively, which gives the respective GH codewords* 0101010011*,* 0100001011*,* 0001001011*,* 0000101011*,* 0010101011*,* 10000000011 *and* 10100000011*.*

Property 3.14 *For $a \leq -2$, we have seven straight lines $y + 13x = 31 + j$, for $j = 1, 2, \ldots 7$, such that the seven points $(a, 32 - 13a)$, $(a, 33 - 13a)$, …, $(a, 38 - 13a)$ lie on these lines for $j = 1, 2, \ldots, 7$, respectively, which gives the respective GH codewords* 0101001011*,* 0100101011*,* 00000000011*,* 00100000011*,* 10010000011*,* 10001000011 *and* 10101000011*.*

Also, Basu, Das and Bagchi (2016) stated that the GH codeword exists for (a, n) if and only if (a, n) satisfies at least one of the straight lines $y + mx = c + j$, where m, c, j are non-negative integers and
Case 1: $m = 0$,
$c = 0$ and $j = 1, 2, 3, 4$.
Case 2: $m = 1$,
$c = 0$ and $j = 1, 2, 3, 4, 5, 6$.
Case 3: $m > 1$,
if the coefficient of $F(1)$ in the Zeckendorf's representation of $m - 2$ is 0 then $c = \sum_{k=1}^{l} a_k F(k + 2) + 2$
where $\sum_{k=1}^{l} a_k F(k)$ is the Zeckendorf's representation of $m - 2$, otherwise

$$c = \sum_{k=1}^{l} a_k F(k + 2)$$

where $\sum_{k=1}^{l} a_k F(k)$ is the Zeckendorf's representation of $m - 1$ and for $m = F(4) + F(1)$, $F(6) + F(1)$, $F(6) + F(4) + F(1)$, $F(7) + F(4) + F(1)$, $F(8) + F(1)$, $F(8) + F(4) + F(1)$, $F(8) + F(6) + F(1)$, $F(8) + F(6) + F(4) + F(1)$, $F(9) + F(4) + F(1)$, $F(9) + F(6) + F(1)$, $F(9) + F(6) + F(4) + F(1)$, $F(9) + F(7) + F(4) + F(1)$, $F(10) + F(1) \ldots$, $j = 1, 2, 3, 4, 5, 6$
otherwise $j = 1, 2, 3, 4, 5, 6, 7$.
The GH codewords corresponding to the different values of j, depending on the values of m up to 14, are given in Table 8.

The GH code straight lines for $m = 0, 1, 2, 3, 4, 5, 6, 7, 8$ are given in Fig. 1.

Corollary 3.1 *The GH codeword of (a, n) is the code corresponding to the associated code of the straight line $y + mx = c + j$, which is satisfied by (a, n).*

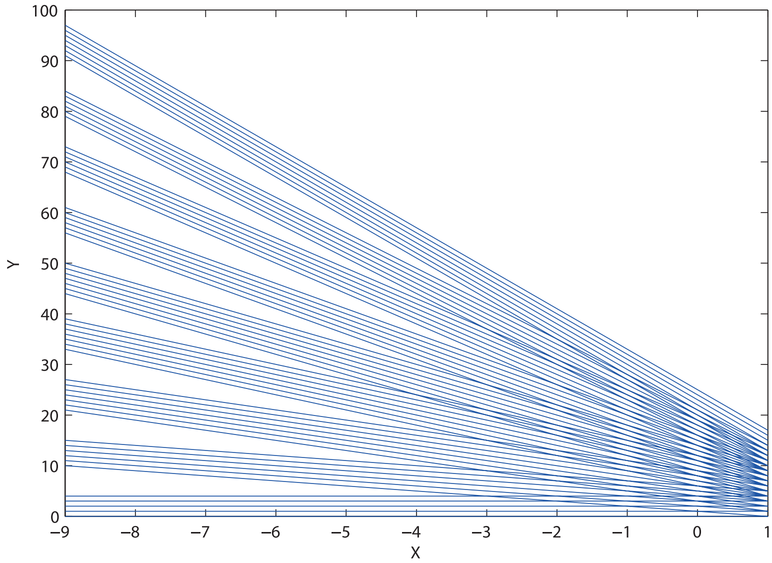

Figure 1. GH code straight lines

Corollary 3.2 *The GH codeword of* (a, n) *is not unique if* (a, n) *satisfies more than one straight line.*

Corollary 3.3 *More than one GH codeword of* (a, n) *exists for* $-4 \leq a \leq -2$.

Corollary 3.4 *Any point* (a, n) *lies on at most two GH code straight lines.*

Corollary 3.5 *The maximum GH codeword representation of any point* (a, n)*, if it exists, is two.*

Note 3.1 *In Tables 4 and 5 the point* (a, n) *whose codeword is represented by bold fonts has two representations of codeword.*

As example, we consider the point $(-3, 9)$. *This point has two codewords:* 1010011 *and* 01011.

Corollary 3.6 *If the GH codeword exists for* $a \leq -5$ *and* $n \geq 1$*, then it is unique.*

Now we describe the uses of GH code in cryptography. In cryptography, we consider the ordered pair $(m, c + j)$ in place of the GH code straight line $y + mx = c + j$, which represents a unique GH codeword.

4. Uses of second order variant Fibonacci universal code (Gopala-Hemachandra code) in cryptography

We work over binary alphabets, $\{0,1\}$, since the GH code is binary.

DEFINITION 4.1 *A synchronous stream cipher is a tuple* (P, C, K, L, E, D), *together with a function* g, *such that the following conditions are satisfied:*

1. P *is a finite set of possible plaintexts*
2. C *is a finite set of possible cipher texts*
3. K *is the keyspace in a finite set of possible keys*
4. L *is a finite set called the keystream alphabet*
5. g *is the keystream generator.* g *takes a key* K *as input, and generates an infinite string* $z_1 z_2 \ldots$ *called the keystream, where* $z_i \in L$ *for all* $i \geq 1$.
6. *For each* $z \in L$, *there is an encryption rule* $e_z \in E$ *and a corresponding decryption rule* $d_z \in D$. $e_z : P \to C$ *and* $d_z : C \to P$ *are functions such that* $d_z(e_z(x)) = x$ *for every plaintext element* $x \in P$ *(Stinson, 2006).*

In this paper, we consider $P = C = L = \mathbb{Z}_2$. We set the key as a binary t-tuple $(k_1, k_2, \ldots, k_t)$ and define the keystream as follows

$$z_i = \begin{cases} k_i & \text{if} \quad 1 \leq i \leq t \\ z_{i-t} & \text{if} \quad i \geq t+1 \end{cases}. \tag{4}$$

This generates the keystream

$$k_1 k_2 \ldots k_t k_1 k_2 \ldots k_t k_1 k_2 \ldots$$

We define the encryption rule as:

$$e_z(x) = (z + x) \; mod \; 2, \quad \text{for all } x \in P \tag{5}$$

and the decryption rule as:

$$d_z(y) = (y + z) \; mod \; 2, \quad \text{for all } y \in C. \tag{6}$$

First, we associate an ordered pair $(m, c + j)$ to every alphabet, space, number, special character etc. which we need for sending the text message. These associations are one-to-one and are known to both the sender and to the receiver.

The following algorithm states the procedure of using the GH code in cryptography.

ALGORITHM 4.1

Step 1. Arrange message to $(m, c + j)$ chronologically.
Step 2. Write the corresponding GH codeword of $(m, c + j)$ accordingly.
Step 3. Write the plaintext and obtain its length l.
Step 4. Set the key and send it to the receiver via a secure channel.
Step 5. Obtain the keystream z of length l by using equation (4).
Step 6. To obtain ciphertext, encrypt plaintext by using equation (5).

Step 7. To obtain plaintext, the receiver decrypts ciphertext by using equation (6).
Step 8. Break the plaintext into a number of parts so that each part ends with 11, meaning so that each part represents a GH codeword.
Step 9. Convert GH codeword to $(m, c+j)$.
Step 10. Write $(m, c+j)$ to message chronologically.

Figure 2 presents the flowchart of this procedure.

Example 4.1 *We consider the text message*

$$A\_williams2014@edu.com$$

and the relations between the ordered pair $(m, c+j)$ *and each character of the message are displayed in Table 9.*

Step 1. *From Table 9, we have*

A	*_*	*w*	*i*	*l*	*l*
(2,2+1)	*(10,23+1)*	*(9,20+1)*	*(7,15+1)*	*(7,15+4)*	*(7,15+4)*
i	*a*	*m*	*s*	*2*	*0*
(7,15+1)	*(5,10+6)*	*(7,15+5)*	*(8,18+4)*	*(0,0+2)*	*(1,0+6)*
1	*4*	*@*	*e*	*d*	*u*
(0,0+1)	*(0,0+4)*	*(9,20+7)*	*(6,13+3)*	*(6,13+2)*	*(8,18+6)*
.	*c*	*o*	*m*		
(9,20+6)	*(6,13+1)*	*(7,15+7)*	*(7,15+5)*		

Step 2. *From Table 8, we have the respective GH codewords, which are*

(2,2+1)	*(10,23+1)*	*(9,20+1)*	*(7,15+1)*	*(7,15+4)*	*(7,15+4)*
01011	*0101000011*	*010101011*	*010100011*	*001001011*	*001001011*
(7,15+1)	*(5,10+6)*	*(7,15+5)*	*(8,18+4)*	*(0,0+2)*	*(1,0+6)*
010100011	*100010011*	*100101011*	*0010000011*	*10011*	*1010011*
(0,0+1)	*(0,0+4)*	*(9,20+7)*	*(6,13+3)*	*(6,13+2)*	*(8,18+6)*
0011	*101011*	*1010010011*	*000010011*	*000100011*	*10001000011*
(9,20+6)	*(6,13+1)*	*(7,15+7)*	*(7,15+5)*		
1000010011	*010000011*	*1010000011*	*100101011*		

Step 3. *Thus, the plaintext is*

$$01011010100001101010101101010001100100101100100101101010001110$$

$$001001110010101100100000011100111010011001110101110100100110000$$

$$1001100010001110001000011100001001101000001110100000011100101011$$

The length of plaintext is 186.

Step 4. *Set* $(1, 0, 0, 1)$ *as the key so that* $t = 4$ *and send it to the receiver via a secure channel.*

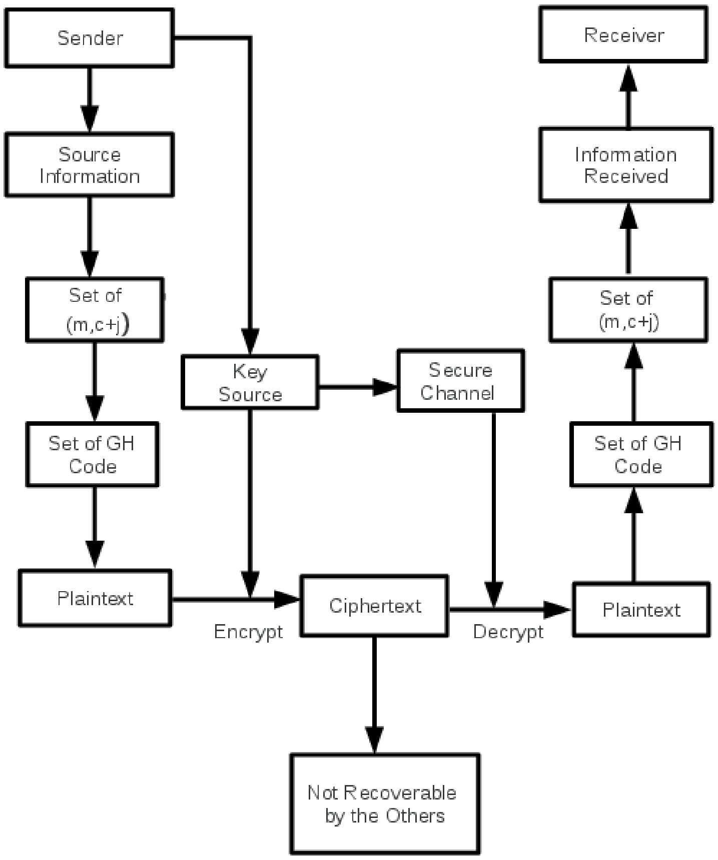

Figure 2. Flowchart of the procedure for using GH code in cryptography

Step 5. *The keystream of length* 186 *is*

100110011001100110011001100110011001100110011001100110011001100110

011001100110011001100110011001100110011001100110011001100110011001

100110011001100110011001100110011001100110011001100110011001100110

Step 6. *After encryption the ciphertext is:*

110000110001111100110010110010000000101101010000111100111010000

010000001010011010100011010000000100101010100011011100001010101001

000000010001011110111010000111010100100111101101100001010011101

Step 7. *After decryption the plaintext is:*

010110101000011010101011010100011001001011001001011010100011100

001001110010101100100000111001110100110011101011101001001100000

100110001000111000100001110000100110100000111010000011100101011

Step 8. *The receiver breaks the plaintext into a number of parts so that each part ends with* 11 *to obtain GH codewords.*

01011	0101000011	010101011	010100011	001001011	001001011
010100011	100010011	100101011	0010000011	10011	1010011
0011	101011	1010010011	000010011	000100011	10001000011
1000010011	010000011	1010000011	100101011		

Step 9. Convert each GH codeword to $(m, c + j)$:

(2,2+1)	(10,23+1)	(9,20+1)	(7,15+1)	(7,15+4)	(7,15+4)
(7,15+1)	(5,10+6)	(7,15+5)	(8,18+4)	(0,0+2)	(1,0+6)
(0,0+1)	(0,0+4)	(9,20+7)	(6,13+3)	(6,13+2)	(8,18+6)
(9,20+6)	(6,13+1)	(7,15+7)	(7,15+5)		

Step 10. Write $(m, c + j)$ chronologically:

$$A\_williams2014@edu.com$$

The receiver receives the message.

Note 4.1 *Construction of Table 9 depends on the users' decision.*

References

Basu, M. and Prasad, B. (2010) Long range variations on the Fibonacci universal code. *Journal of Number Theory* **130**, 1925-1931.

Das, M., Basu, M. and Bagchi, S. (2016) The Gopala-Hemachandra universal code. Communicated to Professor Gerhard Hiss, Lehrstuhl D für Mathematik, RWTH Aachen; Editor, *Journal of Algebra*.

Daykin, D.E. (1960) Representation of natural numbers as sums of generalized Fibonacci numbers. *J. Lond. Math. Soc.* **35**, 143-160.

Elias, P. (1975) Universal codeword sets and representations of the integers. *IEEE Trans. Inform. Theory IT* **21**(2), 194-203.

Kak, S. (2008)*Aristotle and Gautama on logic and physics.* arxiv:physics/0505172.

Kak, S. (2005) Greek and Indian cosmology: Review of early history. In: G.C. Pande (ed.), *The Golden Chain.* CSC, New Delhi, (2005), arxiv: physics/0303001.

Kak, S. (2006) The golden mean and the physics of aesthetics. *Foarm Magazine* **5**, 7381, arxiv:physics/0411195.

Pearce, I.G. (2002) *Indian mathematics: Redressing the balance.* http://www.history.mcs.st-andrews.ac.uk/history/projects/pearce/index.html.

Stinson, Douglas R. (2006) *Cryptography Theory and Practice, Third Edition.* Chapman & Hall/CRC.

Thomas, J. H. (2007) *Variation on the Fibonacci universal code.* arXiv: cs/0701085v2.

Zeckendorf, E. (1972) Representation des nombres naturels par une somme des nombres de Fibonacci ou de nombres de Lucas. *Bull. Soc. Roy. Sci. Liège* **41**, 179-182.

Table 4. GH Code

n	GH_{-2}	GH_{-3}	GH_{-4}	GH_{-5}	GH_{-6}	GH_{-7}	GH_{-8}	GH_{-9}	GH_{-10}	GH_{-11}
1	0011	0011	0011	0011	0011	0011	0011	0011	0011	0011
2	10011	10011	10011	10011	10011	10011	10011	10011	10011	10011
3	**011**	**100011**	100011	100011	100011	100011	100011	100011	100011	100011
4	**00011**	011	101011	101011	101011	101011	101011	101011	101011	101011
5	000011	00011	011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	001011	000011	00011	011	N/A	N/A	N/A	N/A	N/A	N/A
7	**01011**	001011	000011	00011	011	N/A	N/A	N/A	N/A	N/A
8	**1010011**	1000011	001011	000011	00011	011	N/A	N/A	N/A	N/A
9	0000011	**1010011**	1000011	001011	000011	00011	011	N/A	N/A	N/A
10	0010011	010011	1010011	1000011	001011	000011	00011	011	N/A	N/A
11	1001011	0000011	01011	1010011	1000011	001011	000011	00011	011	N/A
12	**0100011**	0010011	010011	N/A	1010011	1000011	001011	000011	00011	011
13	**10100011**	1001011	0000011	01011	N/A	1010011	1000011	001011	000011	00011
14	00000011	10000011	0010011	010011	N/A	N/A	1010011	1000011	001011	000011
15	00100011	**10100011**	1001011	0000011	01011	N/A	N/A	1010011	1000011	001011
16	**10010011**	0001011	10000011	0010011	010011	N/A	N/A	N/A	1010011	1000011
17	**01000011**	00000011	10100011	1001011	0000011	01011	N/A	N/A	N/A	1010011
18	**10101011**	00100011	0100011	10000011	0010011	010011	N/A	N/A	N/A	N/A
19	00001011	10010011	0001011	10100011	1001011	1000011	01011	N/A	N/A	N/A
20	00101011	**0101011**	00000011	N/A	10000011	0010011	010011	N/A	N/A	N/A
21	**01010011**	**10101011**	00100011	0100011	10100011	1001011	0000011	01011	N/A	N/A
22	**101000011**	00010011	10010011	0001011	N/A	10000011	0010011	010011	N/A	N/A
23	000000011	00001011	10001011	00000011	N/A	10100011	1001011	0000011	01011	N/A
24	001000011	00101011	**0101011**	00100011	0100011	N/A	10000011	0010011	010011	N/A
25	100100011	100000011	01000011	10010011	0001011	N/A	10100011	1001011	0000011	01011
26	**100010011**	**01010011**	00010011	10001011	00000011	N/A	N/A	10000011	0010011	010011
27	**101010011**	01001011	00001011	10101011	00100011	0100011	N/A	10100011	1001011	0000011
28	000010011	000000011	00101011	0101011	10010011	0001011	N/A	N/A	10000011	0010011
29	001010011	001000011	100000011	01000011	10001011	00000011	N/A	N/A	10100011	1001011
30	**010100011**	100100011	101000011	00010011	10101011	00100011	0100011	N/A	N/A	10000011
31	**101001011**	100010011	01010011	00001011	N/A	10010011	0001011	N/A	N/A	10100011
32	000001011	**101010011**	01001011	00101011	0101011	10001011	00000011	N/A	N/A	N/A
33	001001011	000100011	000000011	100000011	01000011	10101011	00100011	0100011	N/A	N/A
34	100101011	000010011	001000011	101000011	00010011	N/A	10010011	0001011	N/A	N/A
35	**010001011**	001010011	100100011	N/A	00001011	N/A	10001011	00000011	N/A	N/A
36	**1010000011**	100001011	100010011	01010011	00101011	0101011	10101011	00100011	0100011	N/A
37	0000000011	**101001011**	101010011	01001011	100000011	01000011	N/A	10010011	0001011	N/A
38	0010000011	010010011	010000011	000000011	101000011	00010011	N/A	10001011	00000011	N/A
39	**1001000011**	000001011	000100011	001000011	N/A	00001011	N/A	10101011	00100011	0100011
40	**1000100011**	001001011	000010011	100100011	N/A	00101011	0101011	N/A	10010011	0001011
41	**1010100011**	100101011	001010011	100010011	01010011	100000011	01000011	N/A	10001011	00000011
42	0000100011	1000000011	100001011	101010011	01001011	101000011	00010011	N/A	10101011	00100011
43	0010100011	**010001011**	101001011	N/A	000000011	N/A	00001011	N/A	N/A	10010011
44	**0101000011**	000101011	010100011	010000011	001000011	N/A	00101011	0101011	N/A	10001011
45	**1010010011**	0000000011	010010011	000100011	100100011	N/A	100000011	01000011	N/A	10101011
46	0000010011	0010000011	000001011	000010011	100010011	01010011	101000011	00010011	N/A	N/A
47	0010010011	1001000011	001001011	001010011	101010011	01001011	N/A	00001011	N/A	N/A
48	1001010011	**010101011**	100101011	100001011	N/A	000000011	N/A	00101011	0101011	N/A
49	**1000001011**	**1010100011**	1000000011	101001011	N/A	001000011	N/A	100000011	01000011	N/A
50	**1010001011**	0001000011	1010000011	N/A	010000011	100100011	N/A	101000011	00010011	N/A

n	GH_{-2}	GH_{-3}	GH_{-4}	GH_{-5}	GH_{-6}	GH_{-7}	GH_{-8}	GH_{-9}	GH_{-10}	GH_{-11}
51	000001011	000100011	10001011	10100011	00100011	00010011	1010011	N/A	0001011	N/A
52	010001011	010100011	00101011	10010011	00010011	01010011	1001011	N/A	0101011	101011
53	**101010011**	000010011	000000011	00001011	01010011	N/A	00000011	N/A	00000011	1000011
54	**100001011**	**010010011**	010000011	01001011	00001011	N/A	01000011	N/A	01000011	0010011
55	**001001011**	100100011	001000011	00101011	01001011	N/A	00100011	N/A	N/A	0001011
56	000101011	000010011	000100011	000000011	N/A	10000011	00010011	1010011	N/A	0101011
57	010101011	010010011	**10101011**	010000011	N/A	00100011	01010011	1001011	N/A	00000011
58	**0000000011**	001010011	100000011	N/A	10100011	00010011	N/A	00000011	N/A	01000011
59	**100101011**	000001011	001000011	10001011	10010011	01010011	N/A	01000011	N/A	N/A
60	0000000011	**100010011**	000100011	00101011	00001011	00001011	N/A	00100011	N/A	N/A
61	0100000011	001010011	010100011	000000011	01001011	01001011	N/A	00010011	1010011	N/A
62	**0010000011**	000001011	000010011	010000011	00101011	N/A	10000011	01010011	1001011	N/A
63	**1000000011**	010001011	010010011	001000011	000000011	N/A	00100011	N/A	00000011	N/A
64	**0101000011**	001001011	101000011	000100011	010000011	N/A	00010011	N/A	01000011	N/A
65	0001000011	**000101011**	100100011	010100011	N/A	10100011	01010011	N/A	00100011	N/A
66	0101000011	**010101011**	000010011	10101011	N/A	10010011	00001011	N/A	00010011	1010011
67	**0000100011**	001001011	010010011	100000011	10001011	00001011	01001011	N/A	01010011	1001011
68	0100100011	000101011	001010011	001000011	00101011	01001011	N/A	10000011	N/A	00000011
69	0000100011	010101011	000001011	000100011	000000011	00101011	N/A	00100011	N/A	01000011
70	0100100011	0000000011	010001011	010100011	010000011	000000011	N/A	00010011	N/A	00100011
71	**0010100011**	**101001011**	100010011	000010011	001000011	010000011	N/A	01010011	N/A	00010011
72	**1000100011**	100101011	001010011	010010011	000100011	N/A	10100011	00001011	N/A	01010011
73	**0100010011**	0000000011	000001011	N/A	010100011	N/A	10010011	01001011	N/A	N/A
74	0000010011	0100000011	010001011	101000011	N/A	N/A	00001011	N/A	10000011	N/A
75	**0100010011**	0010000011	001001011	100100011	10101011	10001011	01001011	N/A	00100011	N/A
76	**0010010011**	**0001000011**	000101011	000010011	100000011	00101011	00101011	N/A	00010011	N/A
77	**1000010011**	**0101000011**	**101010011**	010010011	001000011	000000011	000000011	N/A	01010011	N/A
78	0101010011	0010000011	100001011	001010011	000100011	010000011	010000011	N/A	00001011	N/A
79	0001010011	0001000011	001001011	000001011	010100011	001000011	N/A	10100011	01001011	N/A
80	**0101010011**	0101000011	000101011	010001011	000010011	000100011	N/A	10010011	N/A	10000011
81	**1010010011**	0000100011	010101011	N/A	010010011	010100011	N/A	00001011	N/A	00100011
82	1001010011	0100100011	10000000011	100010011	N/A	N/A	N/A	01001011	N/A	00010011
83	0000001011	01001000011	10100000011	001010011	N/A	N/A	10001011	00101011	N/A	01010011
84	0100001011	0000100011	101001011	000001011	101000011	10101011	00101011	000000011	N/A	00001011
85	**0010001011**	0100100011	100101011	010001011	100100011	100000011	000000011	010000011	N/A	01001011
86	**0001001011**	0010100011	0000000011	001001011	000010011	001000011	010000011	N/A	10100011	N/A
87	0101001011	**0000010011**	0100000011	000101011	010010011	000100011	001000011	N/A	10010011	N/A
88	0001001011	**0100010011**	0010000011	010101011	001010011	010100011	000100011	N/A	00001011	N/A
89	**0101001011**	0010100011	0001000011	101010011	000001011	000010011	010100011	N/A	01001011	N/A
90	**1010001011**	0000010011	**0101000011**	100001011	010001011	010010011	N/A	N/A	00101011	N/A
91	0100101011	0100010011	1000000011	001001011	N/A	N/A	N/A	10001011	000000011	N/A
92	0000101011	**0010010011**	0010000011	000101011	N/A	N/A	N/A	00101011	010000011	N/A
93	0100101011	**1010100011**	0001000011	010101011	100010011	N/A	10101011	000000011	N/A	10100011
94	**0010101011**	0101010011	0101000011	0000000011	001010011	101000011	100000011	010000011	N/A	10010011
95	**1000101011**	0010010011	0000100011	0100000011	000001011	100100011	001000011	001000011	N/A	00001011
96	0010101011	0001010011	0100100011	N/A	010001011	000010011	000100011	000100011	N/A	01001011
97	00000000011	**0101010011**	1010000011	101001011	001001011	010010011	010100011	010100011	N/A	00101011
98	01000000011	0000001011	1001000011	100101011	000101011	001010011	000010011	N/A	N/A	000000011
99	**1010101011**	1010010011	0000100011	0000000011	010101011	000001011	010010011	N/A	10001011	010000011
100	**00010000011**	1001010011	0100100011	0100000011	N/A	010001011	N/A	N/A	00101011	N/A

Table 5. GH Code

n	GH_{-12}	GH_{-13}	GH_{-14}	GH_{-15}	GH_{-16}	GH_{-17}	GH_{-18}	GH_{-19}	GH_{-20}
1	0011	0011	0011	0011	0011	0011	0011	0011	0011
2	10011	10011	10011	10011	10011	10011	10011	10011	10011
3	100011	100011	100011	100011	100011	100011	100011	100011	100011
4	101011	101011	101011	101011	101011	101011	101011	101011	101011
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	00011	011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	000011	00011	011	N/A	N/A	N/A	N/A	N/A	N/A
16	001011	000011	00011	011	N/A	N/A	N/A	N/A	N/A
17	1000011	001011	000011	00011	011	N/A	N/A	N/A	N/A
18	1010011	1000011	001011	000011	00011	011	N/A	N/A	N/A
19	N/A	1010011	1000011	001011	000011	00011	011	N/A	N/A
20	N/A	N/A	1010011	1000011	001011	000011	00011	011	N/A
21	N/A	N/A	N/A	1010011	1000011	001011	000011	00011	011
22	N/A	N/A	N/A	N/A	1010011	1000011	001011	000011	00011
23	N/A	N/A	N/A	N/A	N/A	1010011	1000011	001011	000011
24	N/A	N/A	N/A	N/A	N/A	N/A	1010011	1000011	001011
25	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1010011	1000011
26	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1010011
27	01011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
28	010011	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
29	0000011	01011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
30	0010011	010011	N/A	N/A	N/A	N/A	N/A	N/A	N/A
31	1001011	0000011	01011	N/A	N/A	N/A	N/A	N/A	N/A
32	10000011	0010011	010011	N/A	N/A	N/A	N/A	N/A	N/A
33	10100011	1001011	0000011	01011	N/A	N/A	N/A	N/A	N/A
34	N/A	10000011	0010011	010011	N/A	N/A	N/A	N/A	N/A
35	N/A	10100011	1001011	0000011	01011	N/A	N/A	N/A	N/A
36	N/A	N/A	10000011	0010011	010011	N/A	N/A	N/A	N/A
37	N/A	N/A	10100011	1001011	0000011	01011	N/A	N/A	N/A
38	N/A	N/A	N/A	10000011	0010011	010011	N/A	N/A	N/A
39	N/A	N/A	N/A	10100011	1001011	0000011	01011	N/A	N/A
40	N/A	N/A	N/A	N/A	10000011	0010011	010011	N/A	N/A
41	N/A	N/A	N/A	N/A	10100011	1001011	0000011	01011	N/A
42	0100011	N/A	N/A	N/A	N/A	10000011	0010011	010011	N/A
43	0001011	N/A	N/A	N/A	N/A	10100011	1001011	0000011	01011
44	00000011	N/A	N/A	N/A	N/A	N/A	10000011	0010011	010011
45	00100011	0100011	N/A	N/A	N/A	N/A	10100011	1001011	0000011
46	10010011	0001011	N/A	N/A	N/A	N/A	N/A	10000011	0010011
47	10001011	00000011	N/A	N/A	N/A	N/A	N/A	10100011	1001011
48	10101011	00100011	0100011	N/A	N/A	N/A	N/A	N/A	10000011
49	N/A	10010011	0001011	N/A	N/A	N/A	N/A	N/A	10100011
50	N/A	10001011	00000011	N/A	N/A	N/A	N/A	N/A	N/A

Table 6. GH Code

Table 7. GH Code

n	GH_{-12}	GH_{-13}	GH_{-14}	GH_{-15}	GH_{-16}	GH_{-17}	GH_{-18}	GH_{-19}	GH_{-20}
51	N/A	10101011	00100011	0100011	N/A	N/A	N/A	N/A	N/A
52	N/A	N/A	10010011	0001011	N/A	N/A	N/A	N/A	N/A
53	N/A	N/A	10001011	00000011	N/A	N/A	N/A	N/A	N/A
54	N/A	N/A	10101011	00100011	0100011	N/A	N/A	N/A	N/A
55	N/A	N/A	N/A	10010011	0001011	N/A	N/A	N/A	N/A
56	0101011	N/A	N/A	10001011	00000011	N/A	N/A	N/A	N/A
57	01000011	N/A	N/A	10101011	00100011	0100011	N/A	N/A	N/A
58	00010011	N/A	N/A	N/A	10010011	0001011	N/A	N/A	N/A
59	00001011	N/A	N/A	N/A	10001011	00000011	N/A	N/A	N/A
60	00101011	0101011	N/A	N/A	10101011	00100011	0100011	N/A	N/A
61	100000011	01000011	N/A	N/A	N/A	10010011	0001011	N/A	N/A
62	101000011	00010011	N/A	N/A	N/A	10001011	00000011	N/A	N/A
63	N/A	00001011	N/A	N/A	N/A	10101011	00100011	0100011	N/A
64	N/A	00101011	0101011	N/A	N/A	N/A	10010011	0001011	N/A
65	N/A	100000011	01000011	N/A	N/A	N/A	10001011	00000011	N/A
66	N/A	101000011	00010011	N/A	N/A	N/A	10101011	00100011	0100011
67	N/A	N/A	00001011	N/A	N/A	N/A	N/A	10010011	0001011
68	N/A	N/A	00101011	0101011	N/A	N/A	N/A	10001011	00000011
69	N/A	N/A	100000011	01000011	N/A	N/A	N/A	10101011	00100011
70	N/A	N/A	101000011	00010011	N/A	N/A	N/A	N/A	10010011
71	01010011	N/A	N/A	00001011	N/A	N/A	N/A	N/A	10001011
72	01001011	N/A	N/A	00101011	0101011	N/A	N/A	N/A	10101011
73	000000011	N/A	N/A	100000011	01000011	N/A	N/A	N/A	N/A
74	001000011	N/A	N/A	101000011	00010011	N/A	N/A	N/A	N/A
75	100100011	N/A	N/A	N/A	00001011	N/A	N/A	N/A	N/A
76	100010011	01010011	N/A	N/A	00101011	0101011	N/A	N/A	N/A
77	101010011	01001011	N/A	N/A	100000011	01000011	N/A	N/A	N/A
78	N/A	000000011	N/A	N/A	101000011	00010011	N/A	N/A	N/A
79	N/A	001000011	N/A	N/A	N/A	00001011	N/A	N/A	N/A
80	N/A	100100011	N/A	N/A	N/A	00101011	0101011	N/A	N/A
81	N/A	100010011	01010011	N/A	N/A	100000011	01000011	N/A	N/A
82	N/A	101010011	01001011	N/A	N/A	101000011	00010011	N/A	N/A
83	N/A	N/A	000000011	N/A	N/A	N/A	00001011	N/A	N/A
84	N/A	N/A	001000011	N/A	N/A	N/A	00101011	0101011	N/A
85	N/A	N/A	100100011	N/A	N/A	N/A	100000011	01000011	N/A
86	010000011	N/A	100010011	01010011	N/A	N/A	101000011	00010011	N/A
87	000100011	N/A	101010011	01001011	N/A	N/A	N/A	00001011	N/A
88	000010011	N/A	N/A	000000011	N/A	N/A	N/A	00101011	0101011
89	001010011	N/A	N/A	001000011	N/A	N/A	N/A	100000011	01000011
90	100001011	N/A	N/A	100100011	N/A	N/A	N/A	101000011	00010011
91	101001011	N/A	N/A	100010011	01010011	N/A	N/A	N/A	00001011
92	N/A	010000011	N/A	101010011	01001011	N/A	N/A	N/A	00101011
93	N/A	000100011	N/A	N/A	000000011	N/A	N/A	N/A	100000011
94	N/A	000010011	N/A	N/A	001000011	N/A	N/A	N/A	101000011
95	N/A	001010011	N/A	N/A	100100011	N/A	N/A	N/A	N/A
96	N/A	100001011	N/A	N/A	100010011	01010011	N/A	N/A	N/A
97	N/A	101001011	N/A	N/A	101010011	01001011	N/A	N/A	N/A
98	N/A	N/A	010000011	N/A	N/A	000000011	N/A	N/A	N/A
99	N/A	N/A	000100011	N/A	N/A	001000011	N/A	N/A	N/A
100	010100011	N/A	000010011	N/A	N/A	100100011	N/A	N/A	N/A

Table 8. The values of j for different values of m and the corresponding GH codewords

m	c(m)	j	(m,c+j)	GH codeword	m	c(m)	j	(m,c+j)	GH codeword
0	0	1	(0,0+1)	0011	8	18	1	(8,18+1)	010001011
		2	(0,0+2)	10011			2	(8,18+2)	000101011
		3	(0,0+3)	100011			3	(8,18+3)	0000000011
		4	(0,0+4)	101011			4	(8,18+4)	0010000011
1	0	1	(1,0+1)	011			5	(8,18+5)	1001000011
		2	(1,0+2)	00011			6	(8,18+6)	1000100011
		3	(1,0+3)	000011			7	(8,18+7)	1010100011
		4	(1,0+4)	001011	9	20	1	(9,20+1)	010101011
		5	(1,0+5)	1000011			2	(9,20+2)	010000011
		6	(1,0+6)	1010011			3	(9,20+3)	0001000011
2	2	1	(2,2+1)	01011			4	(9,20+4)	0000100011
		2	(2,2+2)	010011			5	(9,20+5)	0010100011
		3	(2,2+3)	0000011			6	(9,20+6)	1000010011
		4	(2,2+4)	0010011			7	(9,20+7)	1010010011
		5	(2,2+5)	1001011	10	23	1	(10,23+1)	0101000011
		6	(2,2+6)	10000011			2	(10,23+2)	0100100011
		7	(2,2+7)	10100011			3	(10,23+3)	0000010011
3	5	1	(3,5+1)	0100011			4	(10,23+4)	0010010011
		2	(3,5+2)	0001011			5	(10,23+5)	1001010011
		3	(3,5+3)	00000011			6	(10,23+6)	1000001011
		4	(3,5+4)	00100011			7	(10,23+7)	1010001011
		5	(3,5+5)	10010011	11	26	1	(11,26+1)	0100010011
		6	(3,5+6)	10001011			2	(11,26+2)	0001010011
		7	(3,5+7)	10101011			3	(11,26+3)	0000001011
4	7	1	(4,7+1)	0101011			4	(11,26+4)	0010001011
		2	(4,7+2)	01000011			5	(11,26+5)	1001001011
		3	(4,7+3)	00010011			6	(11,26+6)	1000101011
		4	(4,7+4)	00001011			7	(11,26+7)	1010101011
		5	(4,7+5)	00101011	12	28	1	(12,28+1)	0101010011
		6	(4,7+6)	100000011			2	(12,28+2)	0100001011
		7	(4,7+7)	101000011			3	(12,28+3)	0001001011
5	10	1	(5,10+1)	01010011			4	(12,28+4)	0000101011
		2	(5,10+2)	01001011			5	(12,28+5)	0010101011
		3	(5,10+3)	000000011			6	(12,28+6)	10000000011
		4	(5,10+4)	00100011			7	(12,28+7)	10100000011
		5	(5,10+5)	100100011	13	31	1	(13,31+1)	0101001011
		6	(5,10+6)	100010011			2	(13,31+2)	0100101011
		7	(5,10+7)	101010011			3	(13,31+3)	00000000011
6	13	1	(6,13+1)	010000011			4	(13,31+4)	00100000011
		2	(6,13+2)	000100011			5	(13,31+5)	10010000011
		3	(6,13+3)	000010011			6	(13,31+6)	10001000011
		4	(6,13+4)	001010011			7	(13,31+7)	10101000011
		5	(6,13+5)	100001011	14	34	1	(14,34+1)	01000000011
		6	(6,13+6)	101001011			2	(14,34+2)	00011000011
7	15	1	(7,15+1)	010100011			3	(14,34+3)	00001000011
		2	(7,15+2)	010010011			4	(14,34+4)	00101000011
		3	(7,15+3)	000001011			5	(14,34+5)	100001000011
		4	(7,15+4)	001001011			6	(14,34+6)	10100100011
		5	(7,15+5)	100101011					
		6	(7,15+6)	1000000011					
		7	(7,15+7)	1010000011					

Table 9. Relation between the ordered pair (m,c+j) and the message character

Character	(m,c+j)	Character	(m,c+j)
1	(0,0+1)	a	(5,10+6)
2	(0,0+2)	b	(5,10+7)
3	(0,0+3)	c	(6,13+1)
4	(0,0+4)	d	(6,13+2)
5	(1,0+1)	e	(6,13+3)
6	(1,0+2)	f	(6,0+4)
7	(1,0+3)	g	(6,13+5)
8	(1,0+4)	h	(6,13+6)
9	(1,0+5)	i	(7,15+1)
0	(1,0+6)	j	(7,15+2)
A	(2,2+1)	k	(7,15+3)
B	(2,2+2)	l	(7,15+4)
C	(2,2+3)	m	(7,15+5)
D	(2,2+4)	n	(7,15+6)
E	(2,2+5)	o	(7,15+7)
F	(2,2+6)	p	(8,18+1)
G	(2,2+7)	q	(8,18+2)
H	(3,5+1)	r	(8,18+3)
I	(3,5+2)	s	(8,18+4)
J	(3,5+3)	t	(8,18+5)
K	(3,5+4)	u	(8,18+6)
L	(3,5+5)	v	(8,18+7)
M	(3,5+6)	w	(9,20+1)
N	(3,5+7)	x	(9,20+2)
O	(4,7+1)	y	(9,20+3)
P	(4,7+2)	z	(9,20+4)
Q	(4,7+3)	space	(9,20+5)
R	(4,7+4)	.	(9,20+6)
S	(4,7+5)	@	(9,20+7)
T	(4,7+6)	_	(10,23+1)
U	(4,7+7)	%	(10,23+2)
V	(5,10+1)	&	(10,23+3)
W	(5,10+2)	$	(10,23+4)
X	(5,10+3)	α	(10,23+5)
Y	(5,10+4)	β	(10,23+6)
Z	(5,10+5)	γ	(10,23+7)
			...