International Journal on Emerging Technologies **13**(1): 10-14(2022)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Designing on Secret Password by using Cryptography and M modulo *N* Graceful Labeling

C. Velmurugan[1*] and V. Ramachandran[2]

[1]*Department of Mathematics, Vivekananda College, Madurai, (Tamil Nadu), India.*
[2]*Department of Mathematics, Mannar Thirumalai Naicker College, Madurai, (Tamil Nadu), India.*

(Corresponding author: C. Velmurugan)*
(Received 30 August 2021, Revised 31 October 2021, Accepted 02 December 2021)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cryptography means concealed writing and the essence of a cryptographic application is to ensure that two parties can communicate privately over a channel in which a third party cannot detect what is being communicated. Currently, information security is the paramount challenge in our life on a daily basis. In this paper, we proposed a secret password that helps to protect data and massage in a secure way. We developed a secret password by using cryptography and M modulo *N* graceful labeling on a complete bipartite graph with a secure key known only by the system manager. Further, our proposed secret password improves the security of the message which traverses over the insecure system. This also involves private keys Security is ensured because only the person with the relevant private key can decode the message. Also we illustrated these mathematically.

Keywords: Cryptography, Graceful labeling, M modulo *N* graceful labeling, complete bipartite graph, secret password.

AMS subject classification: 05C78, 05C85, 14G50.

I. INTRODUCTION

At the present time information security is the most significant challenge for sending a message from one source to another source. Graph labeling and cryptography are widely used to generate a password to protect our information's. A function f is called graceful labeling of a graph G = (V , E) if $f : V(G) \to \{0, 1,...,q\}$ is injective and the induced function $f^* : E(G) \to \{1, 2,...,q\}$ defined as $f^*(e) = |f(u) - f(v)|$ is bijective for every edge $e = (u, v) \in E(G)$. A graph G is called graceful graph if it admits a graceful labeling. This definition is originally introduced for proving the Graceful tree conjecture which states that every tree admits graceful labeling [1]. A graph that admits odd graceful labeling is called an odd graceful graph and proved many graphs exist on odd graceful labeling [2]. Avoided any dependence on Schnorr's Geometric Series Assumption with help of Practical lattice based reduction by sampling and it demonstrates that the sampling reduction can significantly reduce the length of the base vectors [3]. The center of a large enough star is identified with any vertex of an arbitrary tree and showed that the resulting tree is graceful and also estimated an upper bound for the size of the star [4]. One modulo three graceful labeling admitted some identifying graphs obtained from star and cycle [5]. Crowns, Armed crowns and chain of even cycles are satisfied One modulo *N* graceful labeling, so that which are known One modulo *N* graceful graph [6]. M modulo *N* graceful labeling technique was initiated and proved that path and star are M modulo *N* graceful graph [7]. Mathematical structures of Elliptic Curves improved the security of the message which traverses over the insecure channels. Further the elliptic curves cryptography involving one public key and private key followed by two public keys and private keys [8]. Difference Modulo Labeling for finite undirected graphs to keep the message or data secured by coding and decoding, because in many industries the communication signals are openly available [9]. The confidentiality is ensured by the methods of cryptography whereas RSA public key cryptosystem is more useful in the digital signatures scheme to ensure integrity and authenticity of data [10]. Graphical Passwords are easy to remember and difficult to guess so a new graphical password authentication technique is generated based on the idea of "topological structure plus number theory" and various labelings for solving network transfer delay. Also defined a new graph labeling, called Module-K super graceful labeling in which some mathematical conjectures are produced. These passwords promise better robustness and memorability [11]. SCAN pattern encryption is generated by the SCAN methodology. The proposed encryption method can achieve two goals. One is to design highly secured image cryptosystem. The other is to reduce the time for encryption and decryption. There are many features of the SCAN methodology such as Lossless encryption of image, increased Security by the use of more several encryption loops [12]. Explicit constructions in External graph theory to give appropriate lower bound for Turan type problems. In the case of prohibited cycles explicit constructions can be used in various problems of Information Security. Described some algorithms of Coding Theory and Cryptography based on algebraic constructions of regular graphs of large girth and graphs with large cycle [13]. The idea used for data encryption and data decryption with the inner magic and inner antimagic graphs making the data transfer highly secure [14].

This paper shows that the complete bipartite graph is M modulo *N* graceful labeling. Also, we applied this technique in cryptography to protect the information's in a secure way with encryption and decryption.

II. MAIN DEFINITION

Definition: 2.1 A **graceful labeling** of a graph G of size q is an injective assignment of labels from the set {0,1,...,q} to the vertices of G such that when each edge of G has been assigned a label defined by the absolute difference of its end-vertices, the resulting edge labels are distinct.

Definition: 2.2 A graph G is said to be **one modulo *N* graceful labeling**(where *N* is a positive integer) if there is a function *f* from the vertex set of G to $\{0, 1, N, (N + 1), 2N, (2N + 1), \ldots, N(q - 1), N(q - 1) + 1\}$ in such a way that (i) *f* is 1 – 1 (ii) *f* induces a bijection *f** from the edge set of G to $\{1, N+1, 2N+1, \ldots, N(q-1) + 1\}$ where $f^*(uv) = | f(u) - f(v)|$ for all $u, v \in V(G)$.

Definition: 2.3 A graph G (V(G),E(G)) with p vertices and q edges is said to be **M modulo *N* graceful labeling** (where *N* is positive integer and M= 1 to *N*) if there is a function *f* from the vertex set of G to $\{0, M, N, N + M, 2N, \ldots, N(q-1), N(q-1) + M\}$ in such a way that (i) *f* is 1-1 ,(ii) *f* induces a bijection *f** from edge set of G to $\{M, N + M, 2N + M, \ldots, N(q-1) + M\}$ where $f^*(u, v) = |f(u) - f(v)|$ for all $u, v \in V(G)$. A graph G satisfied M modulo *N* graceful labeling is known as M modulo *N* graceful graph.

Definition: 2.4 A **bipartite** graph is a graph in which the vertices can be partitioned into two disjoint sets V_1 and V_2 such that every edge connects a vertex in V_1 to a vertex in V_2.

Definition: 2.5 A **complete bipartite** graph is a simple graph in which the vertices can be partitioned into two disjoint sets V_1 and V_2 such that each vertex in V_1 is adjacent to each and every vertex in V_2. Take $| V_1 | = m$ and $| V_2 | = n$, the complete bipartite graph is denoted by $K_{m, n}$

Definition: 2.6 Encryption is a process of converting a plain text into an encrypted or cipher text which is not human readable. **Decryption** is reverse of encryption and is a process of converting the encrypted or cipher text into plain text which is human readable. **Plain text** is the message or information in a form that is easily readable by humans. **Cipher text** is data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.

III. RESULTS AND DISCUSSION

Theorem: 3.1 Any Complete bipartite graph $K_{m, n}$ is M modulo *N* graceful labeling, *N* is any positive integer and M = 1 to *N*.

Proof:

Let $K_{m, n}$ be complete bipartite graph and vertex set of $K_{m, n}$ can be partition into two non empty sets, say X and Y. Let $X = \{x_1, x_2, \ldots, x_m\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$.

Labeling of Vertices are defined as:

$f(x_i) = [mn - 1]N - n[i - 1]N + M$

$= [n(m - i + 1) -1]N + M$ for for $i = 1$ to m.

$f(y_i) = [i-1]N$ for $i = 1$ to n.

The vertices have labeling as $\{f(x_i)$, for $i = 1$ to m$\} \cup \{f(y_i)$, for $i = 1$ to n $\} = \{[mn - 1]N + M, [n(m - 1) - 1]N + M, \ldots, [n - 1]N + M\} \cup \{0, N, 2N, \ldots, [n - 1]N\} = \{0, N, 2N, \ldots, [n - 1]N, [n - 1]N + M, \ldots, [n(m - 1) - 1]N + M, [mn - 1]N + M\} \subseteq \{0, M, N, N + M, 2N, \ldots, N[q - 1], N[q - 1] + M\}$. Hence each vertex labeling is distinct.

Labeling of edges are defined as:

Let i = 1 to m and j = 1 to n

$f^*(e_{m(i-1)+j}) = | f(x_i) - f(y_j) |$

$= |[n(m - i + 1) -1]N + M - (j - 1)N |$

$= |[n(m - i + 1) - j]N + M]|$.

The edges have labeling as $\{ f^*(e_i)$, for $i = 1$ to mn$\} = \{[mn - 1]N + M, [mn - 2]N + M, \ldots, n[m - 1]N + M, \ldots, N + M, M \} = \{M, N + M, 2N + M, \ldots, [mn - 1] N + M \}$. Hence each edge has distinct labeling.

From the definition of *f* and *f** Complete bipartite graph $K_{m, n}$ is M modulo *N* graceful labeling, *N* is any positive integer and M = 1 to *N*.

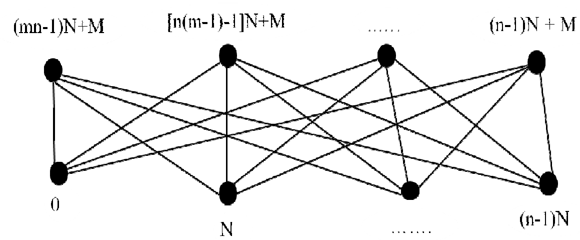
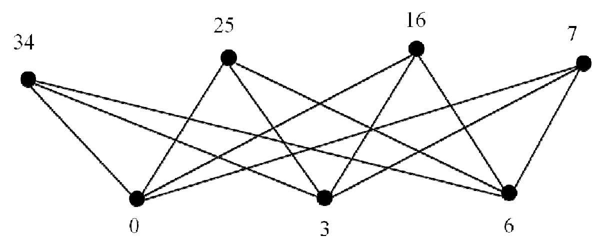
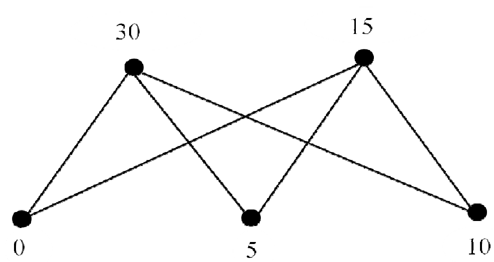


Fig. 1. M modulo *N* graceful graph of $K_{m, n}$.

Example: 3.2 1 modulo 3 graceful graph of $K_{4, 3}$.



Example: 3.3 5 modulo 5 graceful graph of $K_{2, 3}$.



Algorithm: 3.4 Algorithm for M modulo *N* graceful labeling of $K_{m, n}$ for any positive integer *N* and M = 1 to *N*

```
#include<iostream.h>
#include<conio.h>
void main()
{
clrscr();
int i, j, n,N, M, Y, m;
cout<<"Enter m value for Km,n:";
 cin>>m;
 cout<<"Enter n value for Km,n:";
 cin>>n;
 cout<<"Enter N Value:";
 cin>>N;
 cout<<"m = "<<m<<" n = "<<n<<"N = "<<N;
 cout<<endl<<" Want to find particular Value of M and N:";
 cout<<endl<<"Say Yes=1 or No = 0: Y =";
 cin>>Y;
if(Y==1)
{
cout<<endl<<"Enter M Value: M = ";
cin>>M;
goto G;
}
for(M=1;M<=N;M++)
{
G:
cout<<endl<<M<<" modulo "<<N<<" gracful labeling of
          vertex K"<<m<<","<<n<<":";
for(i=1;i<=m;i++)
{
cout<<" X"<<i<<"="<<(n*(m-i+1)-1)*N+M;
}
for(i=1;i<=n;i++)
{
cout<<" Y"<<i<<"="<<(i-1)*N;
}
cout<<endl<<M<<" modulo "<<N<<" gracful labeling of edge K"<<m<<","<<n<<":";
for(i=1;i<=m;i++)
{
for(j=1;j<=n;j++)
{
cout<<" e"<<m*(i-1)+j<<"="<< (n*(m-i+1)-j)*N+M;
}}
if(Y==1)
{
goto g;
}}
g:
if(Y==1)
{
cout<<endl<<"Hence K"<<m<<","<<n<<" is "<<M<<"
         modulo "<<N<<"graceful labeling";
}
else
{
cout<<endl<<"Hence K"<<m<<","<<n<<" is "<<" M
          modulo N graceful labeling";
}
getch();
}
```

IV. DESIGNING SECRET PASSWORD WITH CRYPTOGRAPHY AND M MODULO *N* GRACEFUL LABELING

A. Procedure for generating Secret key:

Step 1: Let any complete bipartite graph.

Step 2: Find the M modulo *N* graceful labeling.

Step 3: **Construct problem:** System manager wants to protect the system with secret password. He encrypts the password by using M modulo *N* graceful labeling and φ are the keys which known only the system manager.

Step 4: Constructing password by use of selecting edges [Like path or cycle]:

> Select any one edge from the given graph say e_i.
> Select second edge from which is incident to e_i, say e_j, $i \neq j$. Now we get $e_i \to e_j$.
> Select Third edge from which is incident to e_j, say e_k, $i \neq j \neq k$.Now we get $e_i \to e_j \to e_k$.
> Repeat the process until we get a require pattern [Like path or cycle].

Step 5: **Plain text:** The alphabetical letters are assigned for selecting edges as follows,

Mapping each labeling value into the alphabetic letters, like 0»A, 1»B, 2»C …, 25»Z , 26»A, 27»B, ..., etc,. by using modulo 26.

Step 6: **Encryption:**

i. Cipher message is defined as: (Visible to third persons)

$C_M^N(e_{[n(i-1)+j]}) = |f(x_i) - f(y_j)| \pmod N + \varphi = M + \varphi$, j = 1 to n and i = 1 to m. Where M, *N* and φ are known the system manager. Suppose if he wants to restrict two keys then he assume $\varphi = 0$, we get

ii. Encrypt letters are arranged by a sequence based on edges in the selected pattern [Like path or cycle].

Step 7: **Decryption:** Cipher password converted to plain password by using the following relation two cases:

Case i. If $N = M$

$D_M^N\,[C_M^N(e_i)] = N(q - i) + C_M^N(e_i) - \varphi$, i = 1 to q = mn .

Case ii. If $N \neq M$

$D_M^N\,(C_M^N(e_i)) = N(q + 1 - i) - \varphi$, i = 1 to q = mn .

Decrypt letters are arranged by a sequence based on edges in the selected pattern [Like path or cycle].

Only selected edges in the pattern are encrypted and decrypted others are vanished.

By using the above process the enter password is encrypted by using M modulo N graceful labeling and the private key φ. The encryption text was constructed based on M and φ. Then we decrypt the encryption by using only the same value of M and φ**.** The following examples 4.2 and 4.3 are describing the above process clearly and briefly with respect to $N \neq M$ and $N = M$.

Example: 4.2 Let the complete bipartite graph $K_{4,\,3}$, here m = 4 and n = 3 and Let the Keys are M = 1 and $N = 3$, $\varphi = 2$, Hence 1 modulo 3 graceful labeling on $K_{4,\,3}$ and password pattern are shown in the Fig. 2.

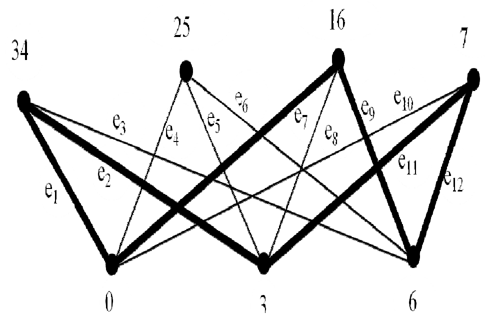


Fig. 2. 1 modulo 3 graceful graph of $K_{4,3}$.

From the Password pattern we get an edge sequence as follows[cycle: $e_1 \rightarrow e_7 \rightarrow e_9 \rightarrow e_{12} \rightarrow e_{11} \rightarrow e_2$]

We assign the letters By using Table 1 as follows

Table 1: Mapping between labeling and alphabetical letters.

x_i/y_j	y_1	y_2	y_3
x_1	e_1	e_2	-
x_2	-	-	-
x_3	e_7	-	e_9
x_4	-	e_{11}	e_{12}

x_i/y_j	0	3	6
34	34	31	-
25	-	-	-
16	16	-	10
7	-	4	1

	I	F	.
	.	.	.
	Q	.	K
	.	E	B

Suppose if choose e_1, then M modulo *N* graceful labeling of e_1 as 34 then which is processed by using modulo property and assign the corresponding letter as I. ie. 34 = 8(mod 26), 8 assign by a letter I(8>>I). Similarly we find the entire letter as required.

Plain text: IQKBEF

Encryption:

Cipher password is defined as:(Visible to third persons)
$C_M^N(e_{[n(i-1)+j]}) = |f(x_i)-f(y_j)| \pmod N + \varphi = M + \varphi$, j=1 to n and i = 1 to m. Where M, *N* and φ are known sender and receiver.

Let choose e_1, then M modulo *N* graceful labeling of e_1 as 34 then which is processed by using modulo property and $\varphi=2$, now assign the corresponding letter as D. ie. 34 = 1(mod 3), assign by a letter D(1+2 = 3>>D). Similarly we find the others as follows.

$C_1^3(e_1) = |f(x_1) - f(y_1)| \pmod 3 + 2 = 34 \pmod 3 + 2 = 1 + 2 = 3$ » D

$C_1^3(e_2) = |f(x_1) - f(y_2)| \pmod 3 + 2 = 31 \pmod 3 + 2 = 1 + 2 = 3$ » D

$C_1^3(e_7) = |f(x_3) - f(y_1)| \pmod 3 + 2 = 16 \pmod 3 + 2 = 1 + 2 = 3$ » D

$C_1^3(e_9) = |f(x_3) - f(y_3)| \pmod 3 + 2 = 10 \pmod 3 + 2 = 1 + 2 = 3$ » D

$C_1^3(e_{11}) = |f(x_4) - f(y_{11})| \pmod 3 + 2 = 4 \pmod 3 + 2 = 1 + 2 = 3$ » D

$C_1^3(e_{12}) = |f(x_4) - f(y_{12})| \pmod 3 + 2 = 1 \pmod 3 + 2 = 1 + 2 = 3$ » D

$C_1^3(e_3), C_1^3(e_4), C_1^3(e_5), C_1^3(e_6), C_1^3(e_8), C_1^3(e_{10})$ are vanished.
Arrange According to Pattern [cycle: $e_1 \rightarrow e_7 \rightarrow e_9 \rightarrow e_{12} \rightarrow e_{11} \rightarrow e_2$]

Cipher text: DDDDDD

Decryption:

Cipher password converted to Plain password:
$D_M^N(C_M^N(e_i)) = N(mn-i) + C_M^N(e_i) - \varphi$, i = 1 to mn .
$D_1^3(C_1^3(e_i)) = 3(12-i) + C_1^3(e_i) - 2$, i = 1 to 12.

Let choose e_1 and encryption Value of e_1 as 3 ($C_1^3(e_1) = 3$), then which is Decrypted by using a model $D_M^N(C_M^N(e_i)) = N(mn-i) + C_M^N(e_i) - \varphi$, i = 1 to mn, and assign the corresponding letter as I. ie. $D_1^3(C_1^3(e_1)) = 3(12-1)+3-2 = 34$ » I, ie. 34 = 8(mod 26), 8 assign by a letter I(8>>I). Similarly we find the others as follows.

$D_1^3(C_1^3(e_1)) = 3(12-1)+3-2 = 34$ » I
$D_1^3(C_1^3(e_2)) = 3(12-2)+3-2 = 31$ » F
$D_1^3(C_1^3(e_7)) = 3(12-7)+3-2 = 16$ » Q
$D_1^3(C_1^3(e_9)) = 3(12-9)+3-2 = 10$ » K
$D_1^3(C_1^3(e_{11})) = 3(12-11)+3-2 = 4$ » E
$D_1^3(C_1^3(e_{12})) = 3(12-12)+3-2 = 1$ » B
$D_1^3(e_3), D_1^3(e_4), D_1^3(e_5), D_1^3(e_6), D_1^3(e_8), D_1^3(e_{10})$ are vanished
Arrange According to Pattern [cycle: $e_1 \rightarrow e_7 \rightarrow e_9 \rightarrow e_{12} \rightarrow e_{11} \rightarrow e_2$].

Decryption Text : IQKBEF

Example: 4.3 Let complete bipartite graph $K_{2,3}$, here m =2 and n = 3.Using 5 modulo 5 graceful Labeling on $K_{2,3}$ and M= 5, N = 5 and $\varphi = 0$ are the keys.

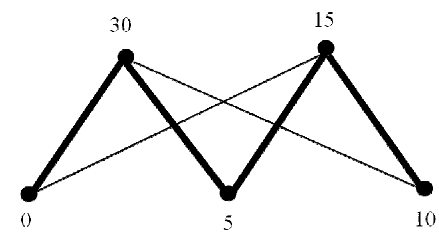


Fig. 3. 5 modulo 5 graceful graph of $K_{2,3}$.

Password pattern is selecting by bold line as follows [Path: $e_1 \rightarrow e_2 \rightarrow e_5 \rightarrow e_6$]

Plain text : EZKF

Encryption: AAAA (Cipher text)

Decryption Text : EZKF

Conclusion

In this paper, we proved Complete bipartite graph is M modulo *N* graceful labeling and develops C++ algorithm to finding M modulo *N* graceful labeling on the complete bipartite graph when vertices and edges are large. Further we design a secret password by using Encryption and Decryption methodology with the help of M modulo *N* graceful labeling on the complete bipartite graph. This password protects our messages or data in a secure way and no one couldn't steal the data without knowing the exact password. In our proposal, all the letters are the same in the encryption so it is not easy to Decrypt. In future we apply M modulo *N* graceful labeling techniques on image scrambling for protecting visual massages.

REFERENCES

[1]. Rosa, A. (1967). On certain valuations of the vertices of a graph. *Theory of Graphs (International Symposium, Rome, July 1966), Gordon and Breach, New York and Dunod Paris*, 349-355.

[2]. Gnanajothi, R. B. (1991). Topics in Graph theory. *Ph.D. Thesis, Madurai Kamaraj University, Tamilnadu, India*.
[3]. Lal, S., Yadav, S. K. and Bhardwaj, K. (2010). On lattice based cryptographic sampling: An algorithmic approach. *International Journal on Emerging Technologies*, *1*(1): 67-70.
[4]. Chan, T. L., Cheung, W. S. and Ng, T. W. (2014). Graceful labeling for mushroom trees. *Aequationes Mathematicae,* DOI 10.1007/s00010-014-0259-5.
[5]. Sekar, C. (2002). Studies in Graph theory. *Ph.D. Thesis, Madurai Kamaraj University, Tamilnadu, India*.
[6]. Ramachandran, V. and Sekar, C. (2018). One modulo *N* gracefulness of Crowns, Armed crowns and chain of even cycles. *Ars Combinatoria*, *138*: 143 - 159.
[7]. Velmurugan, C. and Ramachandran, V. (2019). M Modulo *N* Graceful Labeling of Path and Star. *Journal of Information and Computational Science*, *9*(12): 1212-1221.
[8]. Sharma, A. K. and Badoga, N. K. (2020). Elliptic Curve Cryptography Involving two Private Keys and Public Keys. *International Journal of Electrical, Electronics and Computer Engineering*, *9*(1&2): 12-19.
[9]. Rekha, S. and Maheswari, V. (2019). Difference Modulo Labeling. *International Conference on Physics and Photonics Processes in Nano Sciences*, *1362*: 1 - 10.
[10]. Sharma, A. K. and Badoga, N. K. (2020). Digital Signatures using RSA Public Key Cryptosystem Scheme. *International Journal of Theoretical & Applied Sciences,* 12(1): 37- 42.
[11]. ZHANG, X., SUN, H., YAO, B. and LIU, X. (2018)**.** A technique based on the module-K Super graceful labeling for designing new-type graphical Passwords. *2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference*, 1495-1499.
[12]. Pandey, S. and Shrivastava, A. (2018). A Image Encryption Scheme is Based on Scan Pattern for Colour Image. *International Journal of Electrical, Electronics and Computer Engineering*, *7*(1): 01-05.
[13]. Polak, M., Romańczuk, U., Ustimenko, V. and Wróblewska, A. (2013). On the applications of Extremal Graph Theory to Coding Theory and Cryptography. *Electronic Notes in Discrete Mathematics*, *43*: 329 – 342.
[14]. Krishnaa. A. (2019). Inner magic and inner antimagic graphs in cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*: 1-10.

How to cite this article: Velmurugan, C. and Ramachandran, V. (2022). Designing On Secret Password by Using Cryptography and M modulo *N* Graceful Labeling. *International Journal on Emerging Technologies, 13*(1): 10–14.