

A Scheme to Passcode Generation

Ahmad Yusairi Bani Hashim*

* Faculty of Manufacturing Engineering, Universiti Teknikal Malaysia Melaka, 76100 Durian Tunggal, Malaysia

e-mail: yusairi@utem.edu.my

Abstract- A passcode is a password usually used to receive permission to access a system. It is a combination of 4 or 6 digits or alphanumerics. Generating a passcode may be done by merely guessing the mixture using, for instance, a birthdate, street address, pet's name. The said approach is straightforward and easy to memorize. This study uses the procedures for generating a passcode by gene encoding. Gene encoding is a framework of a synthetic community that they mingle around, get married, and have children. The data of who is who and whose offspring it is are the critical data that lead to a passcode creation. We use a set of information in the form of thumbprints belong to ten participants. There was a balanced ratio between male and female participants whose age range from 20 to 26 years old. All participants have had no thumbprint trauma. The data was gene encoded. It has created a new community of families of two parents and a child. The child's personality becomes the basis for the passcode generation. The developed passcodes relate the owner's biographic and biometric data. The results suggest that the outcomes of the algorithm able to produce the strongest to the weakest passcodes. The method has its strength in giving solutions from particular procedures. It is the artist's total control on how the algorithm would run the processes. Therefore, the steps in constructing the codes discussed in this work are mere guidelines for generating passcodes.

Keywords- Passcode; genetic information; biometric; access system.

1. Introduction

A passcode (PC) is a password usually used to receive permission to access a system. It is a combination of 4 or 6 digits or alphanumeric. A PC-based access system is typical of a digital telephone specification. Generating a PC may be done by simply guessing the combination using, for instance, a birthdate, street address, pet's name. The said approach is straightforward and easy to memorize. Application of a simple passcode is found on the Password-Authenticated Key Exchange where the participated groups share a simple password that is human-memorable and is used to attain the verification [1].

The method of using known phrases such as street address or high school's sweetheart's name may pose a danger because these phrases are vulnerable to attacks. It is because the attackers could somewhat discover the patent of used

phrases through posts in social network platforms such as the Twitter. A good internet bot or software agent can mine the necessary information from social networks according to some predefined tasks written by the attackers.

Since a PC alone is vulnerable to an access system, a multimodal access system (MMAS) that uses multiple access techniques is the fast answer for this shortcoming. Although more efficient, an MMAS is tedious to operate. A person needs to go through some processes before receiving permission to enter the system. There is an issue of time and effort (TE) to access. For example, an MMAS requests that the user scans thumbprint and to enter a PC. So, there is some time needed for the system to verify the print and the PC, hence approve.

A digital telephone uses a PC access system that is tough to hack unless the attacker uses a stolen code. Due to its simplicity, a PC finds its applications in sensitive systems such an automatic

teller machine and a safety box. A personal identification number (PIN) is the PC that if keyed correctly will open the safety box or will allow cash withdrawal for the automatic teller machine.

For a single PC access system (SPS), the critical issue is the PC assignment. If the default PIN is 12345, then it is a fragile PC. To strengthen it, one might switch the positions of a pair of the digit. For example, the code now is 12435 that is stronger than the original PIN. The problem is its arrangement is not natural. In fact, demanding to memorize. With an excellent hacking program, the code is easy to break. One can check how fast a program can crack a password at <https://howsecureismypassword.net/>. For an SPS, a user will have to live with a PIN or a password that is strong that is somewhat difficult to memorize.

The encryption is one way to generate a key that is private. The idea is to avoid unauthorized access to a system. In cryptography, an algorithm processes information and develop a unique key. The key is mostly a PC. A two-party password-authenticated key exchanging protocol, for example, provides a secure communication [2]. The protocol applies Chebyshev chaotic maps in its algorithm that scramble the concerning password data. As a result, the shared password will be complicated to steal.

Similarly, a three-party password-authenticated key exchanging protocol applies the Chebyshev chaotic maps that allow parties at play to communicate over an insecure channel [3]. Also, a disordered hash function is proposed to increase the protocol's complexity and enhance security [4]. Chaotic hash, nevertheless, is said to be insecure against off-line password guessing attacks and defy the session key security [5].

This article proposes a technique to PC production using the biographic and the biometric information. It uses an algorithm that has procedures that follow how the marriage and parenting work. At the conclusion of the computation, the algorithm generates distinct PCs.

2. Background

Marriage is a tie between a sane man and a woman. It is a legalized system of human society. Mating, however, is a biological process to

produce offspring may or may not need a legal procedure. Marriage and mating are natural for civilized human society to avoid extinction.

In natural process, the offspring will inherit a fair share of traits from both of the parents. The characters are in fact the genetic codes found in the chromosomes. The genetic information of the chromosomes forms strings that represent a particular data. For example, a child would inherit the father's brown eyes and the mother's curly hair. Alternatively, if a father is a taxi driver, the child usually has a high analytical skill. On the contrary, if the mother is a criminal, the child will probably become a criminal. Unless there external stimuli, the child will naturally inherit the parents' traits.

A boy can have two genes for eye colour if he possesses two of each chromosome that is two of each gene type on each of a chromosome [6]. A person is said to be homozygous for that gene when both genes of a given pair of chromosomes are identical.

Conversely, the individual is heterozygous when the two genes are different. There are genes called ruling genes and recessive genes. Dominant genes can exert their effects on development even in an individual who is heterozygous for that gene. A heterozygous' will show the consequences of the dominant gene but still pass the recessive genes to offspring. Only those of homozygous possess the recessive genes possess.

Research in genetic algorithm typically related to the issues in engineering. The algorithm that determines gender for particular chromosomes in a population has not been found elsewhere except in [7] where the work claims that all chromosomes are of both sexes. Clownfish, for example, is naturally able to change gender.

Suppose a population of some data assumes a living entity. It is the designer's full control over the structure of the society. Be it male or female, or both sexes depend primarily on the results expected. So conceive offspring, there must be marriages. Unless there is a precise orientation of chromosomes that have been defined to represent a gender, then the process of blending can take place. In [8], the cross-over leads to offspring production. There are two offspring resulted from a crossover. Any information containing different

types of the gene, nevertheless, would generate illegitimate offspring [9].

We may select parents randomly. By partial cross-over, it yields to two children. Could there be twins? One can define such that for each union, there will be a certain number of offspring.

In some applications, there might exist the need for producing the heterozygous offspring. It is likely to occur a situation where the number children dwindle, but a population must expand. As such, adoption is necessary. The genetic string's orientation of an adopted offspring must have a strong resemblance to its adopting parents.

In Charles Darwin's theory of evolution, individuals with specific genetically controlled characteristic reproduce more successfully than others. A person is evolutionary successful if he has five healthy offspring before dying at the age of thirty [6]. In fact, animal and plant breeders use the artificial selection to generate new strains. For the new population created, the qualified ancestors or the first parents can be said to be evolutionarily advantageous. It is because their unions have successfully produced offspring with unique genetic string patterns. Consequently, the fittest chromosomes belong to the parents.

3. Methods

3.1. Gene Encoding

We use the notion of genetic information that represents a particular issue. As a note, from this point onward our discussion reflects a synthetic life. A set of multiple chromosomes (SMC) then corresponds an overall problem. As such, an offspring carries information to a unique solution while a generation offers a complete solution. Every SMC has a fitness level that needs measurement. In general, a fitness value larger than zero defines a good solution. Otherwise, the fitness value specifies a wrong solution. A neutral value, zero denotes neither a right nor an incorrect solution.

For example, if a primary parent has chromosome 110-011 and a secondary parent has chromosome 101-010. By a simple switching, an offspring may receive 110-101 or 110-010 or 101-

110 or 101-011. If the switching implements the concept of single-point crossover, a child may obtain 110-010 or 101-011. These are processes of breeding of a generation or a new SMC. The mutation may occur while breeding at a rate. For example, a chromosome of an offspring 110-011 can mutate by a new chromosome 110-111. A digit changes from 0 to 1 describes that the mutation has occurred. The genetic algorithm uses this concept in the breeding process [10].

Gene encoding (GE) introduces a concept of inheritance derived from the genetic information. In GE, there is a particular framework of the data saving, recording, and extracting. For example, GE has a process of conservation, recording, and retrieving biometric information in the form of fingerprints. A separate algorithm will be able to execute the framework which recipes are sophisticated enough to deter intrusion.

Figure 1 explains the steps in GE. There are eight processes. It begins with creating an SMC. The first SMC forms a community. It contains the problem statements. Next are the gender definition and the marriage rules. The rules are the procedures for transmission of genes and the allowable number of offspring for a family. There is also a possibility of adopting children in the case when a family is unfit to bear children. Lastly, the system yields a new SMC or a new community. Of this new SMC, there are some of the fittest genes belong to the offspring that trace back to the ancestors.

The type of data input determines the shape of a community. Every community is unique. There will be none community that shares the same characteristics. So, cloning a community is impossible. For example, if a problem has two sets of input data: the abscissa (x) and the ordinate (y). Therefore, two SMC- x and SMC- y represent the abscissa and the ordinate, respectively. So that cloning SMC- x to interact with the SMC- y is redundant.

The strings found in the SMCs follows the framework of the defined encoding scheme where a permutation of all genes becomes ancestral chromosomes [11]. The scheduling of job-shop and flow-shop are examples where the chromosomes represent a series of operation in a manufacturing system [9]. Also, a genetic string

(GS) that accounts for a chromosome applies to objective functions a and b through parameter coding [8]. One-half of the GS results from coding of a and another half comes from coding of b. The length of a GS is to be defined and optionally the size of a chromosome.

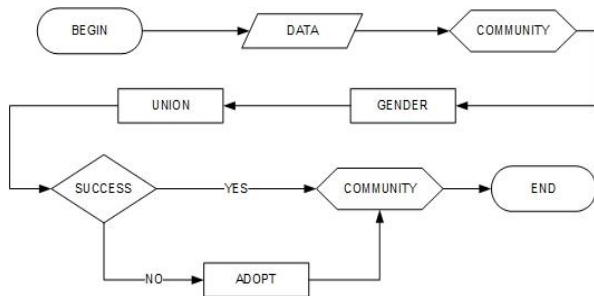


Fig. 1. Three processes play the crucial roles in GE. They are the gender definition, the union rules, and the adoption.

3.2. Models

We presume that every test would result in a unique sequence of number. A candidate (c) represents a test. All c become the community of a culture (C). In turns out that a marriage (m) can proceed if a pair of candidates possesses the same type of codes. If yes, then they would become the parents of an offspring (o). All marriages (M) yield to a new community of all offspring (O). Any union of parents that do not produce a child deem unfit. Therefore, the procedure would abandon the pair of candidates.

$$C = \{c \in C | \exists c \models \langle \mathbb{N} \vee \mathbb{R} \vee \mathbb{Z} \rangle\} \quad (1)$$

$$\{\forall c \text{ of } C: m \models M \vdash o \text{ of } O\} \quad (2)$$

Essentially, Fig. 1 is a generalized procedure that is open to modification. It has a straightforward algorithm and is flexible. The gender definition, union rules, and offspring adoption are the flexible processes. The methods may need some tunings according to the requirement of a problem.

In gene expression programming (GEP) the constraints of the head-tail mechanism contribute to the legality of the chromosome [6]. In GE, however, the union or the adoption rules would determine the validity of the chromosome. Cluster

analysis is a primary method to study gene function and gene regulation information for there is lacked prior knowledge of gene data.

At present, many clustering methods usually need a manual operation or pre-determined parameters [12]. In GE, nevertheless, there is absent of the clustering of data but during the process of determining the community. Depending on the type of function; it puts in manual or automatic mode. It sets to manual mode if the purpose is distinct and occasional. Otherwise, it sets to automatic mode if the function is routine and repeating.

In GEP, the expression tree (ET) evaluates each chromosome. An ET-based, the expression and evaluation are computationally expensive, and the intelligibility of the chromosome is low [13]. Conversely, in GE the ET does not evaluate the chromosome. It exists naturally through procedures in community determination. If there is a need for adoption, then only create a chromosome. Indefinite cross-over determines the inheritance.

Definition 1: Let \mathcal{J} be the image matrix. A computer algebra system (CAS) reads \mathcal{J} from the file directory. The CAS show the picture on the display after it has transformed the image to a grayscale where Fig. 2 depicts the process.



Fig. 2. The process of creating a grayscale image from a color image.

Definition 2: Using the grayscale image that is the offshoot of \mathcal{J} , an image histogram may be computed. Solving for the descriptive statistics, it yields mean μ , standard deviation σ , and size N where Fig. 3 explains the process.

Definition 3: There exists a data column with the largest standard deviations, σ_{\max} . The column data is the most significant image pixels set and is the reference for analysis where Fig. 4 clarifies the process.

Definition 4: Let \mathcal{G} be the data related to the image matrix. The data are the gender class, age, and identification where G , A , and I are gender, age, and subject identification, respectively.

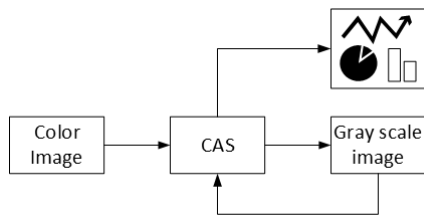


Fig. 3. The process of finding the

$$\mathcal{G} = \{G, A, I\} \quad (3)$$

Definition 5: Let X and Y be a code. Therefore, Eq. (4) defines code based on the image matrix, whereas Eq. (5) defines code based on the data belong to the owner of the thumbprint. Both equations transform the parameters from decimal to hexadecimal.

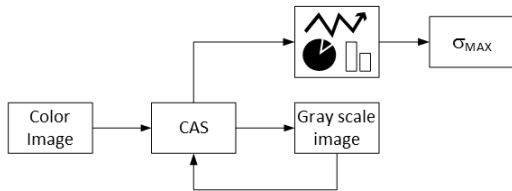


Fig. 4. The process of finding a maximum standard deviation from the descriptive statistics.

$$X = \{x_i \in X | x_i = \{\mu, \sigma, N\}, i = 1, 2, \dots, n\} \quad (4)$$

$$Y = \{y_i \in Y | y_i = \mathcal{G}\} \quad (5)$$

Definition 6: Let M_{\cup} represent the graph that depicts the union of the male parent of x_i and female parent y_i that are also represented as graphs. Suppose that we assign number to the respective parameters such that $\sigma \leftarrow 0$, $\mu \leftarrow 1$, $N \leftarrow 2$, $G \leftarrow 3$, $A \leftarrow 4$, $I \leftarrow 5$. At anyone union operation, we choose a node as the root, always belong to the male parent.

$$M_{\cup} : \sigma \leftarrow 0, \mu \leftarrow 1, N \leftarrow 2, G \leftarrow 3, A \leftarrow 4, I \leftarrow 5 \quad (6)$$

Definition 7: The derivatives of the union graph yield to a new generation. The derivative of the marriage M'_{\cup} is the offspring who is male if it is X -dominant, whereas the offspring who is female if it is Y -dominant.

$$O_X = \{o_{x,j} \in O_X | o_{x,j} = \{M'_{\cup,X}\}, j = 1, 2, \dots, m\} \quad (7)$$

$$O_Y = \{o_{y,j} \in O_Y | o_{y,j} = \{M'_{\cup,Y}\}\} \quad (8)$$

3.3. Experimental Setups

The experiments were conducted in a controlled environment where the subjects were requested to follow the instructions given. The computation were done offline using the data gathered.

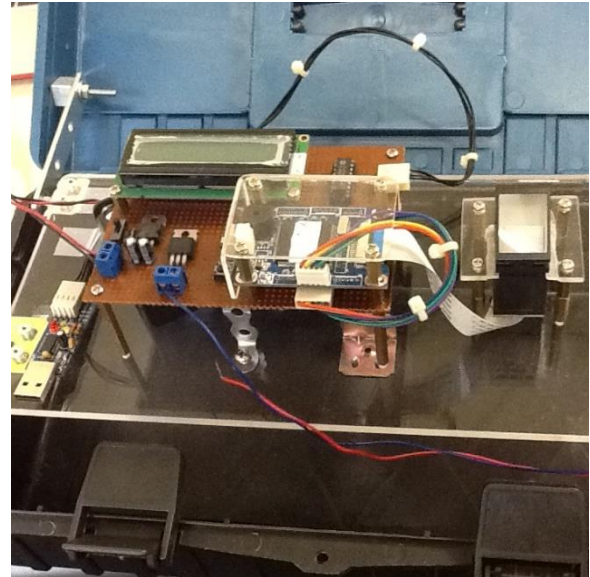


Fig. 5. Hardware setup consists of an off-shelf-product (the fingerprint scanner and the interfaces) that was used to register a user, whose print data was recorded in a database with an assigned identification number some other related personal information. The fingerprint scanner is the device at the right-hand side of the picture. It allows a finger scan one at a time.

The experimental setup consisted of subjects and hardware to register and give access to registered users. There were ten subjects participated in this study of five males and five females. The age ranges from 20-year-old to 26-year-old, all of whom have had no trauma on the thumb. The subjects were asked to register by applying any one of the thumbs on the scanner. The system would assign an identification number automatically once the user logs.

Figure 5 exhibits the hardware setup consists of an off-shelf-product (the scanner and the interfaces). The equipment was used to register a user while recording the fingerprint. The thumbprint data that belonged to a participant was

stored in two separate databases, of sets X and Y . The thumbprint that was saved through the fingerprint scanner was the one registered with an assigned ID, whereas the same thumbs were stamped on plain paper using a print ink. The stamps were scanned using a generic scanner. The scanned images were saved as pictures in a Joint Photographic Group (jpg) image file format.

4. Results and Discussion

Table 1 lists the subjects' raw data upon registrations. Registrations were done with one thumb for a user. For thumbprints of two hands, Left = 0 represents a left side's thumbprint, otherwise Right = 1. Similarly, for Gender process, it represents male = 1 or female = 0. In case there was traumatic experience on the thumb such as an accident, then it represents Yes = 1 or No = 0.







The data in Table 1 represent the Y set. All the subjects had registered with the chosen thumbprint of the left or right hand. In Table 1, it is evident that those who opted to record with a right-hand thumbprint had digit 1. Likewise, the data in Table 2 shown that scanned left and right thumbprint of the same subjects. So, if the subject opted for 1 in Table 1 for the chosen thumbprint to register then the elected print in Table 2 would be the right-print.

Suppose that we arrange a marriage for the data of the first row taken from Table 1 and Table 2. We create graphs for the respective data where data-1 assume the root of the unioned graph as depicted in Fig. 6. It shows the two sets X and Y are combined into a graph in Fig. 6(b) where set X assume father's role while set Y assume mother's role.

Table 1. (a) The graphs of two parents. (b) The union of the two graphs where x -parent is the father that assume the dominant chromosomes. Node-1 of the x -parent has been assigned as root. (c) The derivative of the marriage where the end results is the derivation of seven offspring. It takes a trail passing through three vertices at a time. The kind of arrangement in the union produces at most seven children. The graphs were drawn using the GraphTea.

Subject №	Left	Right	Gender	Trauma	Age	ID
1	0	1	1	0	24	85
2	1	0	1	0	23	99
3	1	0	1	0	25	35
4	0	1	1	0	25	27
5	0	1	1	0	26	11
6	1	0	0	0	24	75
7	1	0	0	0	23	5
8	0	1	0	0	20	8
9	0	1	0	0	25	55
10	0	1	0	0	24	1

Table 2. A sample of subjects' thumbprints scan from the prints stamped on plain paper using generic fingerprint ink. The raw data represents set X .

Subject №	Left	Right	Gender	Age	ID
1			1	24	85
2			1	23	99
3			1	25	35

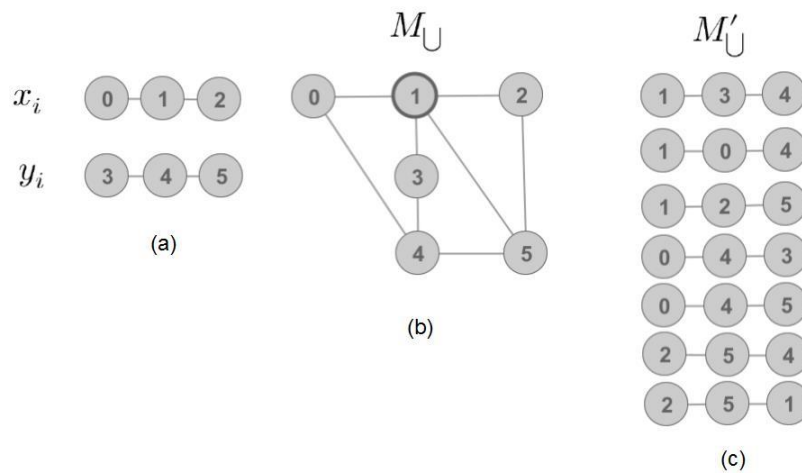


Fig. 6. (a) The graphs of two parents. (b) The union of the two graphs where x-parent is the father that assume the dominant chromosomes. Node-1 of the x-parent has been assigned as root. (c) The derivative of the marriage where the end results is the derivation of seven offspring. It takes a trail passing through three vertices at a time. The kind of arrangement in the union produces at most seven children. The graphs were drawn using the GraphTea.

The connections between the nodes begin from node-0 trailing node-1 until connecting to the last node-5. Node-5 returns to node-0 and closing the loop. Node-1 takes the information of data-1 and assumes as the root node. For this case, the selection of the root merely by choice since it is the intermediate node of X. In fact, any node among the three nodes of X may assume the root role. Since the father is dominant, the root may only come from X.

For this circumstance, there are at most seven

(<http://www.passwordmeter.com/>). The results seen in Table 3 shows various levels of complexity ranging from the lowest (33%) to the highest (72%). We suggest adding a pair of a symbol to the BPC, and it becomes the new PC that has been tempered to increase the level of complexity. It is evident that the degree of complexity would increase and the results suggest that indeed enhances the complexity from the lowest (60%) to the highest (100%). So, tempering a BPC by adding some symbols would indeed make it

Table 3. Testing the complexity of the PCs using the readily available programs. The password strength was tested on the following page: <http://www.passwordmeter.com/>.

No	Base Passcode	Score (%)	Complexity	Tempered Passcode (+\$, base passcode, +\$)	Score (%)	Complexity	Dominance
1	CD118	33	weak	\$CD118\$	60	strong	Y
2	CD1B18	41	good	\$CD1B18\$	75	strong	X
3	C4B9055	60	strong	\$C4B9055\$	95	very strong	X
4	1B181	41	good	\$1B181\$	69	strong	Y
5	1B1855	49	good	\$1B1855\$	87	very strong	Y
6	4B905518	72	strong	\$4B905518\$	100	very strong	Y
7	4B9055CD	60	strong	\$4B9055CD\$	95	very strong	X
		33	weakest		100	strongest	

offspring that the marriage produces. Depending on the dominance of passing data, a child is a male of it has more of X, where a child is a female of it has more of Y. So, Fig. 6(c) indicated that we have three males and four females.

By taking the offspring of Fig. 6(c) as base passcodes (BPCs), we test on each of the BPCs for password strength on The Password Meter website

adamant PC.

The characteristics of the base codes and the tempered codes listed in Table 3 were analyzed using the StatsGen program of PACK-0.0.4 (Password Analysis and Cracking Toolkit).

From Fig. 7, the base codes have a maximum length of 8 (No 6 & No 7). A minimum length of 5

(№ 1 & № 4). A 100% upper case and alphanumerical. The password complexity for the

```
[*] Analyzing passwords in [base_codes.txt]
[*] Analyzing 100% (<?/?>) of passwords
NOTE: Statistics below is relative to the number of analyzed passwords, not
total number of passwords

[*] Length:
[+] 8: 28% (<2>)
[+] 5: 28% (<2>)
[+] 6: 28% (<2>)
[+] 7: 14% (<1>)

[*] Character-set:
[+] upperalphanum: 100% (<?>)

[*] Password complexity:
[+] digit: min<3> max<7>
[+] lower: min<0> max<0>
[+] upper: min<1> max<3>
[+] special: min<0> max<0>

[*] Simple Masks:
[+] digitstringdigit: 42% (<3>)
[+] othermask: 42% (<3>)
[+] stringdigit: 14% (<1>)

[*] Advanced Masks:
[+] ?d?u?d?d?d?d?u?u: 14% (<1>)
[+] ?d?u?d?d?d: 14% (<1>)
[+] ?u?u?d?d?d: 14% (<1>)
[+] ?u?d?u?d?d?d?d: 14% (<1>)
[+] ?d?u?d?d?d?d?d: 14% (<1>)
[+] ?d?u?d?d?d?d: 14% (<1>)
[+] ?u?u?d?u?d?d: 14% (<1>)
```

Fig. 7. The statistics generated by the statsgen.py program of the PACK-0.0.4 (thesprawl.org). The statistics depict the length, the character set, the password complexity, the simple masks, and the advanced masks of the base codes listed in Table 1.

```
[*] Analyzing passwords in [base_codes.txt]
[*] Analyzing 100% (<?/?>) of passwords
NOTE: Statistics below is relative to the number of analyzed passwords, not
total number of passwords

[*] Length:
[+] 8: 28% (<2>)
[+] 5: 28% (<2>)
[+] 6: 28% (<2>)
[+] 7: 14% (<1>)

[*] Character-set:
[+] upperalphanum: 100% (<?>)

[*] Password complexity:
[+] digit: min<3> max<7>
[+] lower: min<0> max<0>
[+] upper: min<1> max<3>
[+] special: min<0> max<0>

[*] Simple Masks:
[+] digitstringdigit: 42% (<3>)
[+] othermask: 42% (<3>)
[+] stringdigit: 14% (<1>)

[*] Advanced Masks:
[+] ?d?u?d?d?d?d?u?u: 14% (<1>)
[+] ?d?u?d?d?d: 14% (<1>)
[+] ?u?u?d?d?d: 14% (<1>)
[+] ?u?d?u?d?d?d?d: 14% (<1>)
[+] ?d?u?d?d?d?d?d: 14% (<1>)
[+] ?d?u?d?d?d?d: 14% (<1>)
[+] ?u?u?d?u?d?d: 14% (<1>)
```

Fig. 8. The statistics generated by the statsgen.py program for the tempered codes listed in Table 1.

digit where there is a minimum of 3 (№ 1) and a maximum of 7 (№ 6). The upper case of a minimum of 1 (№ 4) and a maximum of 3 (№ 7).

The simple masks of digit-string-digit passcode arrangement where there are 3: (№ 4), (№ 5), (№ 6). The simple masks of ‘other mask’ (string-digit-string-digit/digit-string-digit-string) where there are 3: (№ 2), (№ 3), (№ 7). The simple masks of string-digit where there is one: (№ 1).

From Fig. 8, the tempered codes have a maximum length of 10 (№ 6 & № 7) and a minimum length of 7 (№ 1 & № 4). A 100% uppercase and special alphanumerical. The password complexity for the digit where there is a minimum of 3 (№ 1) and a maximum of 7 (№ 6).

The upper case of a minimum of 1 (№ 4) and a maximum of 3 (№ 2 & № 7) The distinctive character of a minimum 2 and a maximum of 2 indicating that all passcodes have a pair of ‘\$’ character. The simple masks are only the ‘other mask’ where the ‘\$’ that acts as the mask. It turned out that all passcodes possess the mask.

The combination of parameters such as shown in Fig. 6 may be expanded to other different arrangement illustrated in Fig. 9. There are at most other six mixtures of parameters with various root node assignments. Knowing that the root node is among the nodes of X, the second of the graphs chooses node-0 as the root for the graphs in the second row, while node-0 as the root for the graphs in row 3.

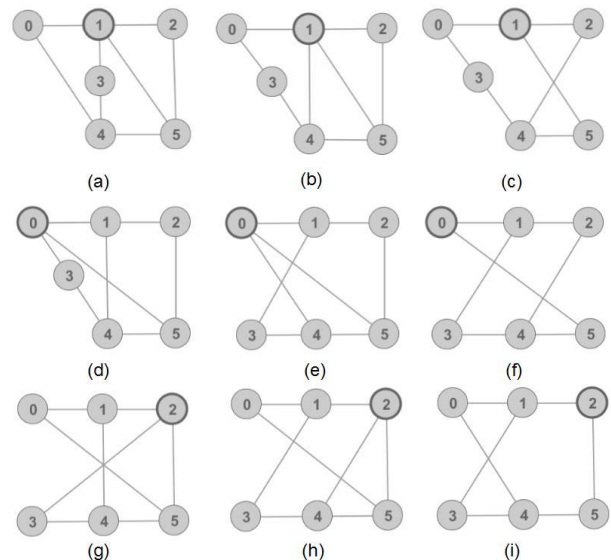


Fig. 9. (a)-(c) The graphs of two parents where the root is node-1. (d)-(f) The graphs of two parents where the root is node-0. (g)-(i) The graphs of two parents where the root is node-2.

Using the same methodology, we choose the graphs of the second row of Fig. 9 to generate the PCs and analyze their strengths. We list the results by the graph numbers. For example, row one to row three have results for graphs A1, A2, and A3. We compare the results of the BPC and the tempered passcode (TPC) for the weakest, as well as, for the most reliable complexities. All of which belong to Subject-1 of the study.

The results seen in Table 2, on the other hand, compare the outcomes according to different graph configurations other than type-A. These graphs are

Fig. 9(d) to Fig. 9(i). Note that the root assignment determines the uniqueness of the graphs. C3 produces the weakest as well as the strongest scores of the base code. The other graphs that provide the weakest score are B3 and C2. For the TPCs, all graph types achieve the highest score 100% while the weakest score 52% offers by B3, C2, and C3.

There is a similar trend that B3, C2, and C3 possess that is node-1 connects node-3. The linking of the average and the gender parameters induce weak PCs. According to the overall results in Table 4, the C3 graph is the most optimum configuration. Nevertheless, all graph settings are useful for creating a BPC, which its strength enhances when tempered with additional symbols. The addition of other symbols to the BPCs have unlimited combinations. We do not touch on this issue because it is beyond our scope of the study.

Table 4. Testing the complexity of the passcodes using the readily available programs. PC complexity among the various graph configurations of subject-1 is compared.

Graph №	Base Passcode		Tempered Passcode	
	Weakest Score (%)	Strongest Score (%)	Weakest Score (%)	Strongest Score (%)
A1	33	72	60	100
A2	34	72	60	100
A3	25	72	59	100
B1	34	72	60	100
B2	33	77	60	100
B3	24	72	52	100
C1	33	69	60	100
C2	24	72	52	100
C3	24	84	52	100
Weakest/Strongest	24	84	52	100

Table 4 exhibits some patterns where C3 seems to offer higher PC complexity as well as lower complexity. We hypothesize that C3 as the generalized configuration. The next tests would create PCs of the remaining subjects. Using the existing methodology in producing the PCs, we analyze each of the subjects' data.

Table 5 lists the overall results of the tests. It is evident the C3 does offer stronger PC complexity as well as weaker complexity. Since each graph configuration has at most seven choices of PCs ranges from the weakest to the lowest, one may choose among the available PCs. Adding some combination of symbols increases the PC's strength.

Table 5. The comparison of PC complexity according to C3 graph configuration of all subjects. There were ten subjects as already seen in Table 1 where the data belong to each of the participants were tested following the similar steps conductor for subject-1. The idea was to compare the complexity of the PCs when C3 configuration was applied.

Subject №	Base Passcode		Tempered Passcode	
	Weakest Score (%)	Strongest Score (%)	Weakest Score (%)	Strongest Score (%)
1	24	84	52	100
2	16	70	54	100
3	15	84	60	100
4	33	65	60	100
5	30	72	56	100
6	36	80	61	100
7	12	54	60	93
8	33	63	62	99
9	15	88	69	100
10	10	55	59	91
Weakest/Strongest	10	84	52	100

Now we would argue how secure is the most intricate PCs found in Table 5. We use a platform on the internet known as the How Secure Is My Password? (<https://howsecureismypassword.net>) to test the level of security of the generated PCs.



Fig. 9. The duration required to break 4C92374C92.

From Table 5, the most complex PCs belong to subject-9 where the BPC is 4C92374C92, and the TPC is \$4C92374C92\$. The results show that the

BPC requires one day to crack (see Fig. 9), whereas the TPC needs two hundred years to break (see Fig. 10).



Fig. 10. The period to break \$4C92374C92\$.

5. Conclusions

Using the two thumbprints of the left and the right hands as the data belong to the subjects who participated in this study, at most seven PCs were generated. The algorithm to creating the PCs uses other data pertaining to the subjects to churn out the PCs that are supposedly sophisticated enough and able to withstand attacks. In doing so, this approach proposed in this article avoids the elegant models of numbers and symbols sequencing. Instead, it uses a unique algorithm where the data are made alive and has a community of its own. The algorithm arranges the unions of the sets of data so that the fruitful unions would produce offspring, which inherited the parents' data.

Consequently, the parents' and the child's chromosomes become the PCs. The results suggest that the outcomes of the algorithm able to produce the strongest to the weakest PCs. The method has its strength in giving solutions from selective procedures. It is the artist's total control on how the algorithm would run the processes. Therefore, the steps in constructing the codes discussed in this work are mere guidelines for generating PCs.

References

- [1] J. Ding, S. Alsayigh, J. Lancrenon, S. RV, and M. Snook, "Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-Quantum World," in *Topics in Cryptology – CT-RSA 2017: The Cryptographers' Track at the RSA Conference 2017*, San Francisco, CA, USA, February 14–17, 2017, Proceedings, H. Handschuh, Ed., ed Cham: Springer International Publishing, 2017, pp. 183-204.
- [2] C.-M. Chen, W. Fang, K.-H. Wang, and T.-Y. Wu, "Comments on "An improved secure and efficient password and chaos-based two-party key agreement protocol"," *Nonlinear Dynamics*, vol. 87, pp. 2073-2075, February 01 2017.
- [3] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps," *Nonlinear Dynamics*, vol. 77, pp. 399-411, July 01 2014.
- [4] X. Guo and J. Zhang, "Secure group key agreement protocol based on chaotic Hash," *Information Sciences*, vol. 180, pp. 4069-4074, 2010/10/15/ 2010.
- [5] T.-F. Lee, "Enhancing the security of password authenticated key agreement protocols based on chaotic maps," *Information Sciences*, vol. 290, pp. 63-71, 2015/01/01/ 2015.
- [6] J. W. Kalat, *Introduction to psychology*: Nelson Education, 2016.
- [7] A. Y. Bani Hashim, "Development of Artificial Intelligent Techniques for Manipulator Position Control," *Universiti Putra Malaysia*, 2002.
- [8] H. Ismail and K. Hon, "The nesting of two-dimensional shapes using genetic algorithms," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, vol. 209, pp. 115-124, 1995.
- [9] J. Psarras, "GA-based decision support systems in production scheduling," *International journal of intelligent systems technologies and applications*, vol. 2, pp. 58-76, 2006.
- [10] A. Y. Bani Hashim, "Representing System by Gene Encoding," *International Journal of Research and Reviews in Computer Science*, vol. 2, pp. 247-249, 2011.
- [11] W. Wang and P. Brunn, "An effective genetic algorithm for job shop scheduling," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, vol. 214, pp. 293-300, 2000.
- [12] G. Liu, X. Jiang, and L. Wen, "A clustering system for gene expression data based upon genetic programming and the HS-model," in *Computational Science and Optimization (CSO), 2010 Third International Joint Conference on*, 2010, pp. 238-241.
- [13] Y. Chen, C. J. Tang, R. Li, M. F. Zhu, C. Li, and J. Zuo, "Reduced-GEP: improving gene expression programming by gene reduction," in *Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2010 2nd International Conference on*, 2010, pp. 176-179.