
Revista INGENIERÍA UC
ISSN: 1316-6832
ISSN: 2610-8240
revistaing@uc.edu.ve
Universidad de Carabobo
Venezuela

Norouzzadeh-GilMolk, Ali; Ramazani-Khorshiddoust, Reza; Aref, Mohammad
Determination of factors that affect the design of cryptographic algorithms by a cybernetic meta-model, validated with Q-analysis
Revista INGENIERÍA UC, vol. 27, no. 1, 2020, -, pp. 29-40
Universidad de Carabobo
Venezuela

# Determination of factors that affect the design of cryptographic algorithms by a cybernetic meta-model, validated with Q-analysis

Ali Norouzzadeh-GilMolk [a], Reza Ramazani-Khorshiddoust * [,b], Mohammad Aref [c]

[a] *Islamic Azad University, North Tehran Branch. Tehran, Iran.*
[b] *Amirkabir University of Technology. Tehran, Iran.*
[c] *Sharif University of Technology. Tehran, Iran.*

**Abstract.-** Encryption is the most important mechanism to protect information. A variety of factors affect the design and implementation of cryptographic algorithms, such as symmetric, asymmetric, and hash functions. In other words, all the necessary components of information security must be considered from the technical, organizational, procedural and human aspects in a model of excellence. To meet these requirements in this study, a methodology was used that enables the development of a metamodel that allows evaluating the different factors that affect cryptographic design, taking into account various attributes. The encryption metamodel has four main components: *policy and strategy*, *main processes*, *support processes*, *process control*, highlighting that the interactions between the main and support processes configure the structure of the encryption system. The evaluation of these interactions was carried out using a score allocation system, which resulted in a complex matrix, which was transformed into incidence matrices, which are addressed by means of a Q-analysis. The results of the Q-analysis indicate that The most significant group of components to develop an encryption system consists of the following: *human resources*, *R&D*, *standards and regulations*, *IT* and *standards*.

**Keywords:** cryptography algorithms; cybernetic meta-model; Q-analysis.

# Determinación de los factores que afectan el diseño de algoritmos criptográficos por medio de un meta-modelo cibernético, validado con análisis-Q

**Resumen.-** El cifrado es el mecanismo más importante para proteger la información. Una variedad de factores afecta el diseño e implementación de algoritmos criptográficos, como funciones simétricas, asimétricas y hash. Es decir, todos los componentes necesarios de la seguridad de la información deben considerarse desde los aspectos técnicos, organizativos, de procedimiento y humanos en un modelo de excelencia. Para cumplir con estos requisitos, en este estudio se utilizó una metodología que posibilita el desarrollo de un metamodelo que permite valorar los diferentes factores que afectan el diseño criptográfico, teniendo en consideración diversos atributos. El metamodelo de cifrado tiene cuatro componentes principales: *política y estrategia*, *procesos principales*, *procesos de apoyo*, *control procesos*, destacando que las interacciones entre los procesos principales y de apoyo configuran la estructura del sistema de cifrado. La valoración de estas interacciones fue realizada por medio de un sistema de asignación de puntajes, lo cual resultó en una matriz compleja, que fue transformada en matrices de incidencia, que se abordan por medio de un análisis-Q. Los resultados del análisis-Q indican que el grupo de componentes más significativos para desarrollar un sistema de cifrado consta de lo siguiente: *recursos humanos*, *I+D*, *normas y reglamentos*, *TI* y *estándares*.

**Palabras clave**: algoritmos criptográficos; meta-modelo cibernético; análisis-Q.

Received: February 17, 2020.
Accepted: March 31, 2020.

## 1. Introduction

Cryptography is a main component of the world's information security to transfer data from transmitter to receiver in the safest way [1]. The security of the cryptographic systems depends on

* Correspondence author:
*e-mail:*ramazani@aut.ac.ir ( R. Ramazani-Khorshiddoust)

two key factors; *strength of algorithms* and *key size*. Various cryptographic algorithms are in three types of hash functions, symmetric key and asymmetric key algorithms. Therefore, the power of cryptography is strongly dependent on the design and implementation of cryptographic algorithms [2].

A user mainly desires a cryptographic algorithm with low cost and high performance [3]. Many researches compare different cryptographic algorithms [4][5][6]. Also, various technologies such as social engineering, mathematical science, physiological signals, and biometrics have been used for the design of cryptographic algorithms [7][8].

Depending on the usage of an algorithm, different technical and non-technical requirements should be considered for its design [9]. The constituent factors of the algorithms are put into a coherent system with logical integrity to analyze and measure their interactions. In [10] different algorithms are evaluated based on some factors such as *key size* and *block size*. Also in [11] explained cryptographic standards. As cited in a research by CompTIA, it was a fast growing industry with a rate of 5 to 7 percent in the first quarter of 2018 [12]. To raise the level of information security has been a significant concern. For a desired security system, the components should be developed considering technological, organizational, process and human dimensions [13], fit to a model of excellence to ensure acceptable level of security, and ensure stability and continuity [14][15]. At the organizational level, the information security management system (ISMS) [16][17] is the only known and pervasive system of this kind. ISMS is a general system and based on the first edition of the British Standards Institute (BSI). The International Telecommunication Union (ITU) also developed an information security management system for communication networks based on the 2008 edition of ISMS [18]. Later, the International Organization for Standardization (ISO) published an information security management for communication organizations [19], particularly for telecom operators. According to the management system, the formation and realization of sustainable security for a communication network require two features, i.e., *the use of a suitable set of security controls* and *deployment based on an excellence model*. In latter management system, the proper set of security controls is at least composed of process controls and excellence for security cycles. The cycles consist of four stages of design, implementation, measurement and improvement.

At the international level, the International Telecommunication Union has provided the example of the National Cyber Security Strategy for the systematic deployment of information security for the member states [20]. The European Network and Information Security Agency (ENISA) also has recommended the deployment of national cybersecurity strategies (NSCC) for the EU member states [21]. Other types of security architecture patterns are also recommended for the realization of desired security. The most important one is the end-to-end security architecture pattern [22][23], which is based on the network architecture model. The pattern of enhancing the information security of critical infrastructures is an alternative type [24], which is based on a functional architectural model. Finally, the organizational security architecture of Sherwood Applied Business Security Architecture (SABSA) [25] is also based on organizational architectural model [24]. In [26], a generic model is provided to design cryptographic algorithms with six parameters such as goal, input, activities, output, outcomes and performance. This model ignores some significant factors like *key size*, *block size*, *round number* as well as their interactions.

## 2. A cybernetic cryptographic algorithm meta model

The methodology for designing a model for cryptography algorithms was cybernetic approach (CA). CA is capable to encompass a process-oriented modeling to the nature of control in man, animal and machine and therefore is widely used in a broad fields such as engineering, mechanics, biology, psychology, and management [27][28]. CA is comprehensive, hierarchical, and physically understandable by

applying a graph structure; it is capable to communicate among various components. CA is properly apt to the combinatorial nature of the cryptographic algorithms [29][30]. The cybernetic model constitutes four main parts, which are strategy/policy, main, support and control components [31]. Main Process: This type of process involves the raison d'etre of the system. In fact, by examining the cause of existence of each system, we can get to main process.

- Strategy/Policy Development: In this component, based on the expected and approved strategies and policies in the system, a functional and comparison basis can be determined and designed (e.g., reference or standard values). As a result, based on these, we can recognize and control the functionality of the system.

- Supportive Process: These processes are necessary for the fulfillment of the main processes. The support processes are classified into "hard" and "soft" ones. "Hard-support" processes are concrete and quantitatively measurable, such as the processes of development and supply of equipment, materials and infrastructure. "Soft-support" processes, such as many soft aspects, are not concrete but mainly measurable such as the development of management, organization, information and communication technologies (ICT), rules and regulation, standards, human resources, and so on.

- Process/Product Control (Feedback) Process: It is referred to the activities which help system to monitor, measure, evaluate and finally control all processes in the main and supportive process modules and correct the deviations.

The cryptographic system includes algorithms, keys and protocols [32], and the main process or the raison d'etre of a typical cryptographic algorithm, in highest level, is shown in Figure 1.

The selection of cryptographic algorithm depends on its intended services. For instance,

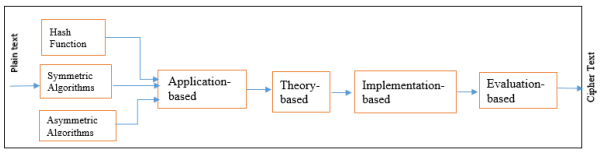


Figure 1: A typical main process of a cryptographic algorithm, in highest level

some cryptographic algorithms are better for confidentiality, but they are very weak for integration (e.g. one-time-pad). Similarly, some cryptographic algorithms are better for integration, but they do not provide proper confidentiality (e.g. ciphers of message confirmation). In designing a cryptographic algorithm, various fields of mathematical knowledge such as pseudo-random functions, Boolean functions [33], and symmetric random functions [34] are very important. There are many metrics for evaluating cryptographic algorithms, the most important of which are: key length, attack steps, attack time, rounds, algorithm strength, types, functions, complexity, speed, block size, flexibility, scalability, memory consumption, and encryption rate [35, 36, 37]. The components of the encryption algorithms are "hash function", "symmetric algorithm" and "asymmetric algorithm". Each of these components has a number of attributes that have assigned some variables to it, as shown in Figure 2.

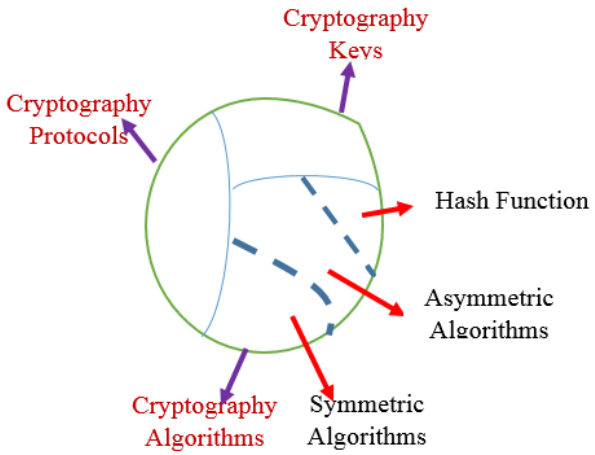


Figure 2: Cryptographic system (Level 1)

The proposed cybernetic cryptography model in the conceptual level is presented in Figure 3. The model consists of four parts:

the policy development, main, support and control processes. The main process includes cryptography algorithms. The support component is divided into two main categories, hard, soft sub-components. Soft component includes ten development sub-components as follows: the development of management, organization, human resources/education, research and development, standard, rule and regulation, financial resources, ICT, public/international relations or relations, and cultural aspects. The hard components include three sub-components namely, the development of infrastructure, equipment and materials. Finally, the control component encompasses both the controls of process and outputs as products. Also a more detailed cybernetic cryptography model is shown in Figure 4.

## 3. Model of influence of factors Affect the Design of Cryptographic Algorithms

To design an efficient hierarchical cryptography algorithm, the significant factors are to be chosen and grouped properly. Based on the cybernetic model, there exist 13 meta-factors (Figure 4) that interacts with 4 modules in the core process (Figure 1). The interaction and importance of these factors were determinate by a broad interviews from a group of 30 experts. Then, the factors are grouped depending upon their interaction to the modules of the core process of the cryptography algorithm.

The indices of interaction matrix are shown in Table 1. These indices are in the range of 0 to 10 in the matrix to indicate the significance of the interaction, determined by the experts.

### *3.1. Incidence Matrix and implementation of the model*

To indicate the impact of support indices on the core processes of the cryptographic algorithms design, an incidence matrix is created for data Matrix A (Table 1). Data Matrix $A$ consists of two sets. Set $D$ represents the support components indices and set $C$ represents the four stages of the cryptographic algorithms.

$$D = \{d_1, d_2, \cdots, d_{13}\}$$

Table 1: Interaction matrix of 13 support components Vs four stages of cryptographic algorithms

| | Support Process | Core/Main Process Cryptography algorithms [A] | [B] | [C] | [D] | Level 1 Level 2 Level 3 |
|---|---|---|---|---|---|---|
| soft | Cutural | 5 | 6 | 5 | 2 | |
| | Organization | 8 | 7 | 8 | 8 | |
| | Public international relation | 5 | 4 | 4 | 7 | |
| | Financial resources | 7 | 6 | 7 | 6 | |
| | Human Resource/Education | 8 | 10 | 10 | 9 | |
| | Research and Development | 10 | 8 | 8 | 10 | |
| | Rule and regulation | 7 | 4 | 5 | 10 | |
| | Development of management | 9 | 7 | 8 | 7 | |
| | ICT | 10 | 5 | 8 | 7 | |
| | Standard | 10 | 3 | 8 | 10 | |
| hard | Equipment | 8 | 6 | 7 | 8 | |
| | Development of infrastructure | 9 | 5 | 5 | 7 | |
| | Materials | 7 | 2 | 5 | 5 | |

[A]:Application-based ; [B]:Theory-based
[C]:Implementation-based, [E]: Evaluation-based

$$C = \{c_1, c_2, c_3, c_4\}$$

Tables 2 and 3 show entities of the two sets above.

Table 2: Indicators of support components

| Indicator | Support component |
|---|---|
| $d_1$ | Cultural |
| $d_2$ | Organization |
| $d_3$ | International Relation (IR) |
| $d_4$ | Financial |
| $d_5$ | Human resource/Education (HR) |
| $d_6$ | Research & Development (R& D) |
| $d_7$ | Rule & Regulation (R& R) |
| $d_8$ | Management |
| $d_9$ | Information and Communication Technology (ICT) |
| $d_{10}$ | Standard |

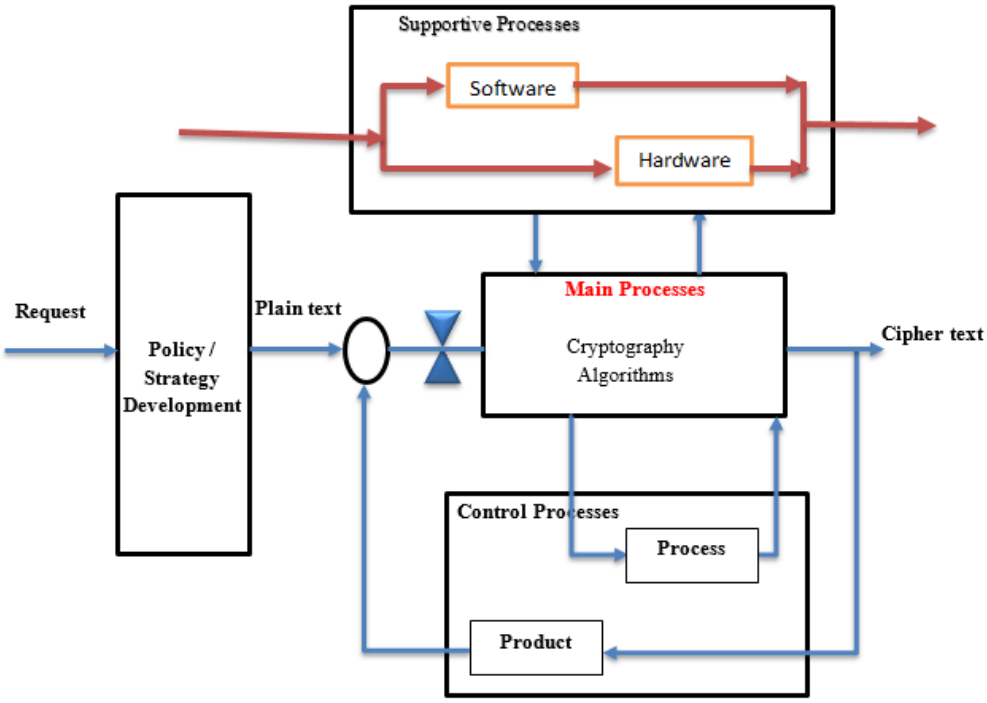


Figure 3: Proposed cybernetic cryptography model in conceptual level (Level 2)

Table 3: Indicators of four stages of cryptographic algotithms

| Indicator | Stage |
|---|---|
| $c_1$ | Use |
| $c_2$ | Science |
| $c_3$ | Programming Skills |
| $c_4$ | Evaluation |

The incidence matrix, calculated from data matrix $A$, indicates the relationship between the members of the two sets. The matrix indicates the existence/nonexistence of a relationship between each member of the two sets. Matrix $A$ is transformed into an incidence matrix B with using a "$\alpha$–cut parameter", by defining a one-to-one function as is presented in equation (1):

$$\lambda \text{ or } b_{ij} = \begin{cases} 1 & \text{if } a_{ij} \geq \alpha, \\ 0 & otherwise, \end{cases} \quad (1)$$

Where $b_{ij}$ or $\alpha_{ij}$ is the entity of the ith row and the jth column in the incidence matrix (zero or one) and $a_{ij}$ is equivalent to the given matrix $A$. Therefore, the entity $b_{ij} = 1$ if and only if the entity $i$ of set $C$ interacts with the entity $j$ of set $D$. The incidence matrix calculated from matrix $A$ for $\alpha_{\%70}$ is shown in Table 4.

By assigning different values for the $\alpha$-cut parameter, different "incidence matrices" are obtained. The $\alpha$-cuts intended for analysis include: $\alpha_{(\%50)} = 5$, $\alpha_{(\%60)} = 6$, $\alpha_{(\%70)} = 7$, $\alpha_{(\%80)} = 8$, $\alpha_{(\%90)} = 9$, $\alpha_{(\%100)} = 10$.

## 4. Analysis-Q

### *4.1. Geometrical representation*

Multidimensional properties of the system are defined by a simplical complex set, or $KD(C, \lambda)$, such that: The entities of set "$D$" represent the simplexes (support indicators) $\sigma_p$ $(d_i)$ and the entities of set $C$ are vertices (cryptographic algorithm four stages). The simplexes of this complex are geometric shapes that represent the relationships that exist in the incidence matrix.

Conventionally, the dimensions of the simplex $(p)$ are shown as captions, and the simplex is denoted by the element shown in parentheses [38]. The simplex dimension is equal to the number of corresponding vertices minus one. In the sample, the $d_i$ are:

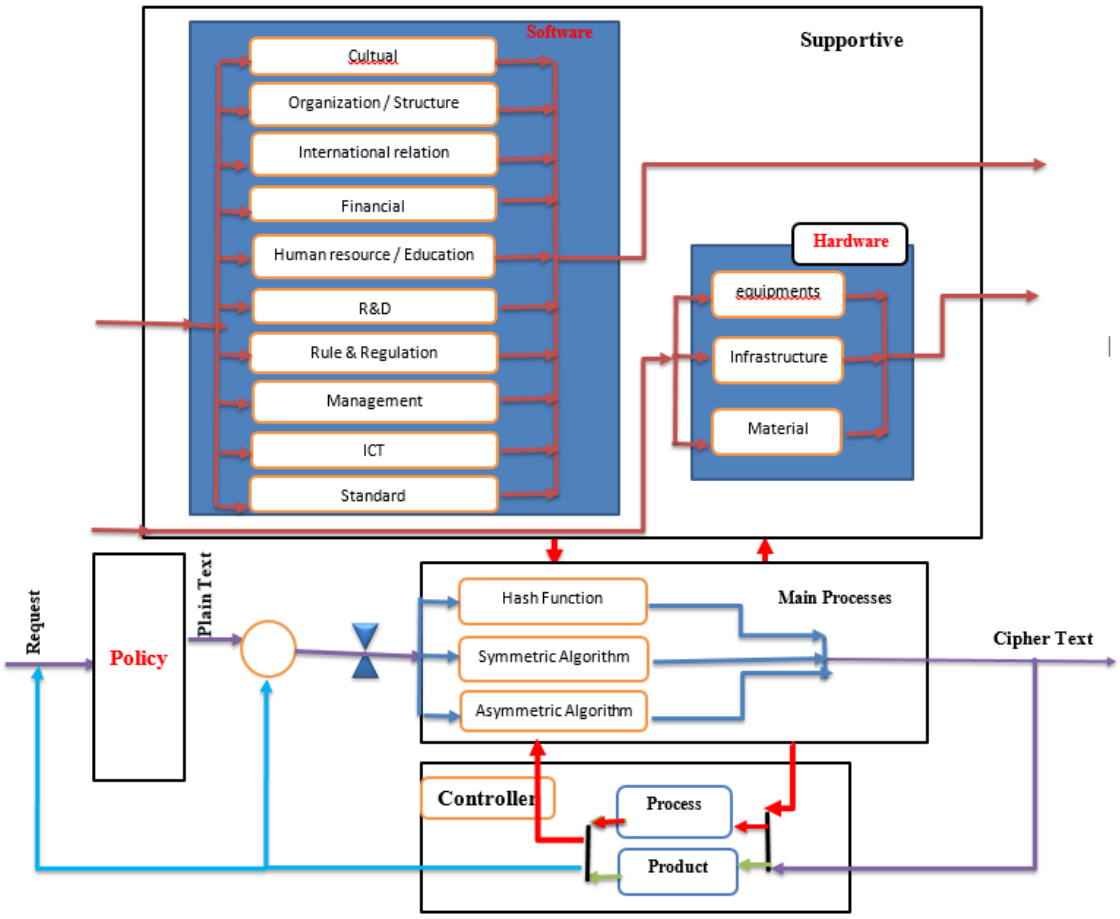


Figure 4: A detailed cybernetic cryptography model (Level 3)

$d_{(1)} = \{\}$, $d_{(2)} = \{c_1, c_2, c_3, c_4\}$, $d_{(3)} = \{c_4\}$,
$d_{(4)} = \{c_1, c_3\}$, $d_{(5)} = \{c_1, c_2, c_3, c_4\}$,
$d_{(6)} = \{c_1, c_2, c_3, c_4\}$, $d_{(7)} = \{c_1, c_4\}$,
$d_{(8)} = \{c_1, c_2, c_3, c_4\}$, $d_{(9)} = \}c_1, c_3, c_4\}$,
$d_{(10)} = \{c_1, c_3, c_4\}$, $d_{(11)} = \}c_1, c_3, c_4\}$,
$d_{(12)} = \{c_1, c_4\}$, $d_{(13)} = \{c_1\}$. Also the $\sigma_p(d_i)$ simplexes are:

$\sigma_1(d_7)$, $\sigma_3(d_6)$, $\sigma_3(d_5)$, $\sigma_1(d_4)$, $\sigma_0(d_3)$, $\sigma_3(d_2)$, $\sigma_{(d_{-1})}(d_1)$, $\sigma_0(d_{13})$, $\sigma_1(d_{12})$, $\sigma_2(d_{11})$, $\sigma_2(d_{10})$, $\sigma_2(d_9)$, $\sigma_3(d_8)$. Therefore, the maximum complex dimension is 3.

### 4.2. *Computation of Dimensions and q-connectivity*

The q-connectivity between a subset is represented by the weakest relationship (The smallest common face) between the two consecutive di in the chain d1 to dn is expressed. The simplex relation that described by q-connectivity, is an equivalence relation that is a symmetric, reflective, and transitive relation. The q-Connectivity between the two consecutive $d_i$ is as follows:

$$\begin{aligned}
\sigma_{(-1)}(d_1), \sigma_3(d_2) &\rightarrow -1 \quad \sigma_3(d_2), \sigma_0(d_3) \rightarrow 0 \\
\sigma_1(d_4), \sigma_3(d_5) &\rightarrow 1 \quad \sigma_3(d_5), \sigma_3(d_6) \rightarrow 3 \\
\sigma_1(d_7), \sigma_3(d_8) &\rightarrow 1 \quad \sigma_3(d_8), \sigma_2(d_9) \rightarrow 2 \\
\sigma_2(d_{10}), \sigma_2(d_{11}) &\rightarrow 2 \quad \sigma_3(d_{11}), \sigma_1(d_{12}) \rightarrow 1 \\
\sigma_0(d_3), \sigma_1(d_4) &\rightarrow -1 \quad \sigma_3(d_6), \sigma_1(d_7) \rightarrow 1 \\
\sigma_2(d_9), \sigma_2(d_{10}) &\rightarrow 2 \quad \sigma_1(d_{12}), \sigma_0(d_{13}) \rightarrow 0
\end{aligned}$$

The maximum connection dimension is 3.

### 4.3. *Computation of structure vectors*

For each dimension q of the complex set $K$, we define integer $Qq$ as the number of distinct equivalence classes, such that each equivalence class is composed of q-connectivity simplexes.

Table 4: Incidence matrix with $\alpha_{\%70} = 7$

| | Support Process | Core/Main Process Cryptography algorithms [A] | [B] | [C] | [D] | Level 1 Level 2 Level 3 |
|---|---|---|---|---|---|---|
| soft | Cutural | 0 | 0 | 0 | 0 | |
| | Organization | 1 | 1 | 1 | 1 | |
| | Public international relation | 0 | 0 | 0 | 1 | |
| | Financial resources | 1 | 0 | 1 | 0 | |
| | Human Resource/Education | 1 | 1 | 1 | 1 | |
| | Research and Development | 1 | 1 | 1 | 1 | |
| | Rule and regulation | 1 | 0 | 0 | 1 | |
| | Development of management | 1 | 1 | 1 | 1 | |
| | ICT | 1 | 0 | 1 | 1 | |
| | Standard | 1 | 0 | 1 | 1 | |
| hard | Equipment | 1 | 0 | 1 | 1 | |
| | Development of infrastructure | 1 | 0 | 0 | 1 | |
| | Materials | 1 | 0 | 0 | 0 | |

[A]:Application-based ; [B]:Theory-based
[C]:Implementation-based, [E]: Evaluation-based

This $Qq$ vector is a simplification basis that came into being for eliminating redundant effects in the set of equivalence simplexes.

The first structure vector, $Q$ is:

$Q = (Q_{dim3}, Q_{dim2}, Q_{dim1}, Q_{dim0})$

$Q = (4, 3, 3, 2)$

The second structure vector, $P$ is:

$P = (P_{dim3}, P_{dim2}, P_{dim1}, P_{dim0})$

$P = (4, 7, 10, 12)$

$Pq$ represents the number of simplexes larger than or equal to $q$ in the set $K$. Where, $P$ denotes the number of repetitions of the simplexes connectivity (support indicators) to vertices (cryptographic algorithm four stages). The larger the $P$ values for the higher dimensions, the greater the connection. In contrast, the $Q$ vector represents the extent of the connections between the simplexes connected (support indicators) by a set of vertices (cryptographic algorithm four stages) [39].

### *4.4. Obstruction or inflexibility vector*

Obstruction vector ($Q^*$) that specifies the information flow limitation during the complex. ($Q^*$) means whether the members of the simplex (each of the support indicators) in any of the equivalence classes in the k-dimension can interact directly or indirectly at the k-level (have effect on each other). The number of barriers to these interactions in the k-dimension is the number of "gaps" between the equivalence categories. Therefore, ($Q^*$) is created by subtracting a vector I from the structure vector, which includes all categories. That is mean:

$Q^* = [4, 3, 3, 2, ] - [1, 1, 1, 1, ]$

$Q^* = [3, 2, 2, 1]$

The value of ${Q^*}_K$ represents the number of structural constraints for the simplex interactions in the $k$ dimension. Depending on the type of problem, high or low values of Q* elements may be preferred. For example, we prefer to have high obstruction between diagnostic values so that they are easily recognizable.

Due to the obtained values, it can be concluded that the effective indicators in designing the cryptographic algorithms are varied and sometimes independent. The obstruction vector and the equivalence classes at each level q with the cutoff parameter $\alpha = 7$ are shown in Table 5.

Table 5: Structure vector, obstruction vector and equivalence classes at each level $q$ with $\alpha = 7$

| q | Q | P | $Q^*$ | equivalence classes |
|---|---|---|---|---|
| 3 | 4 | 4 | 3 | $\{d_2\}, \{d_5\}, \{d_6\}, \{d_8\}$ |
| 2 | 3 | 7 | 2 | $\{d_2, d_5, d_6, d_8, d_9\}$, $\{d_2, d_5, d_6, d_8, d_{10}\}$, $\{d_2, d_5, d_6, d_8, d_{11}\}$ |
| 1 | 3 | 10 | 2 | $\{d_2, d_5, d_6, d_8, d_9, d_{10}, d_{11}, d_4\}$, $\{d_2, d_5, d_6, d_8, d_9, d_{10}, d_{11}, d_7\}$, $\{d_2, d_5, d_6, d_8, d_9, d_{10}, d_{11}, d_{12}\}$ |
| 0 | 2 | 12 | 1 | $\{d_2, d_4, d_5, d_6, d_7, d_8, d_9, d_{10}, d_{11}, d_{12}, d_3\}$, $\{d_2, d_4, d_5, d_6, d_7, d_8, d_9, d_{10}, d_{11}, d_{12}, d_{13}\}$ |

The high value of this vector indicates system inflexibility [40]. Instead, its low value indicates high flexibility for the system. In fact, this vector is an appropriate index for the qualitative evaluation of system data in mathematics language. This flexibility or lack thereof can be attributed to the behavior of any of the q-levels. It is therefore necessary that all q-levels in the inflexibility vector

be evaluated individually to obtain the degree of flexibility of each element. The high amount of flexible vector indicates that the system is more stable and less susceptible to oscillations caused by external stimuli [38].

### 4.5. Computation of Eccentricity

While the structure vectors and the obstruction vectors describe the overall structural properties; the eccentricity indicates the degree of integration of a particular simplex throughout the complex. Conventional measurement of eccentricity for a simplex is the method defined in [41], called ecc according to equation (2). But Chin et al. in [42] offer another way of measuring eccentricity called ecc'according to equation (3):

$$ecc(\sigma) = \frac{\hat{q} - q^*}{q^* + 1} \tag{2}$$

$$ecc'(\sigma) = \frac{2\sum q_i/\sigma_i}{q_{max}\,(q_{max}+1)} \tag{3}$$

where in: is the simplex of $\sigma$. $q^*$ is the largest common dimension of the simplex $\sigma$ with other simplexes (the relation value) in an equivalence class. $q_i$ is any q-level of $\sigma$ that exists. $\sigma_i$ The number of elements in the $\sigma_i$ equivalence classes at the level of $q_i$. $q_{max}$ is the maximum q of the complex set level.

Difference $(\hat{q} - q^*)$ is a criterion for determining the joint range of $\sigma$ with another simplex which it has the most common vertices with it. Therefore, $ecc$ depends only on one simplex over the others, while $ecc'$ also depends on all other simplexes. In addition, the value of ecc is in the range $[0, \infty]$ and $ecc'$ is in the range $[0, 1]$.

For each simplexes of set (support indices), the degree of eccentricity can be defined in two ways, according to the conventional method proposed by Casti ($ecc(\sigma)$) and based on the results of the Q-analysis performed for the data matrix A (Table 1), the eccentricity for all parameters equals zero. As a result, this method is not a suitable method for measuring the degree of eccentricity in the indices communication. Therefore, we use the Chinese method ($ecc'(\sigma)$) for this purpose. The results can be seen in Table 6.

Table 6: Eccentricity of Cryptographic algorithms Parameters in Data Matrix $A$ for cutoff parameter $\sigma_{\%70}$

| $\sigma$ | $q_i$ | $\sum q_i/\sigma_i$ | $q_{max}$ | $ecc'(\sigma)$ |
|---|---|---|---|---|
| $d_2, d_5, d_6, d_8$ | {3,2,1} | 3,64 | 3 | 0,61 |
| $d_9, d_{10}, d_{11}$ | {2,1} | 0,64 | 3 | 0,11 |
| $d_4, d_7, d_{12}$ | {1} | 0,14 | 3 | 0,02 |

The lower eccentricities, the simplex corresponds better to the overall complex structure.

### 4.6. Complexity

The results of the Q-analysis can also be used to describe the complexity of the system structure. The complexity criterion, proposed in [43], is presented in equation (4):

$$\Psi(K) = 2\left[\sum_{k=0}^{dimK} \frac{(k+1)Q_k}{(dimK+1)(dimK+2)}\right] \tag{4}$$

So $Q_k$ is part of $k$ of the vector structure of $Q$. The scale satisfies the principles outlined above. Explicitly states that both the dimension and the number of equivalence classes factors are related to the complexity of the structure. For $\alpha - cut = 7$:

$Q = (Q_{dim3}, Q_{dim2}, Q_{dim1}, Q_{dim0})$

$Q = (4, 3, 3, 2)$

$$\Psi(K) = 2\left[\frac{(4+6+9+8)}{(4\cdot 5)}\right] = 2{,}7$$

It is obviously that due to the variety of supporting indexes that are effective in designing cryptographic algorithms, there is a relatively high degree of complexity between the indexes, which number 2,7 confirms this.

The results of implementing the Q-Analysis model using a C++ code, for $\alpha_{\%70} = 7$, are shown in Figure 5.

## 5. Ranking of the support components

The result of applying Q-analysis on the "interaction matrix" cited in Figure 5, is shown in Table 7. The strength of the connectivity of the factors in a group is determined by $\alpha - cut$, shown in percentage. Thus, the support components are

```
-1  -1  -1  -1  -1  -1  -1  -1  -1  -1  -1  -1  -1
    3   0   1   3   3   1   3   2   2   2   1   0
        0  -1   0   0   0   0   0   0   0   0  -1
            1   1   1   0   1   1   1   1   0   0
                3   3   1   3   2   2   2   1   0
                    3   1   3   2   2   2   1   0
                        1   1   1   1   1   1   0
                            3   2   2   2   1   0
                                2   2   2   1   0
                                    2   2   1   0
                                        2   1   0
                                            1   0
                                                0
```

```
q     Q       SETS
---   ---     ------------------------------
3     1       {X2,X5,X6,X8}
2     1       {X2,X5,X6,X8,X9,X10,X11}
1     1       {X2,X4,X5,X6,X7,X8,X9,X10,X11,X12}
0     1       {X2,X3,X4,X5,X6,X7,X8,X9,X10,X11,X12,X13}
```

Figure 5: Results of implementing the Q-Analysis model using a C++ code, for $\alpha_{\%70} = 7$

grouped in 5 levels or ranks. Each level indicates the priority and importance of the group in the process of developing a cryptographic algorithm.

For a proper resource allocation, the components in the higher level of the pyramid (Figure 6) have higher priority.

Table 7: Ranking of support components using Q-Analysis

| Connectivity of the support components for developing cryptographic algorithms ($q = 0$) (no connection: $\alpha = 0\%$, full connection: $\alpha = 100\%$) | |
|---|---|
| Human resources, R&D, Rules and regulations, ICT, Standards | $\alpha_{(\%100)} = 10$ |
| Development of Management, Infrastructure | $\alpha_{(\%90)} = 9$ |
| Organization, Equipment | $\alpha_{(\%80)} = 8$ |
| Public and international relations, financial resources, Material | $\alpha_{(\%70)} = 7$ |
| Culture | $\alpha_{(\%60)} = 6$ |
| All components | $\alpha_{(\%60)} = 5$ |

The results about the priority and importance of the group in the process of developing a cryptographic algorithm were compared to the Global Cybersecurity Index (GCI) reports of 2015, 2017 and 2018 issued by International

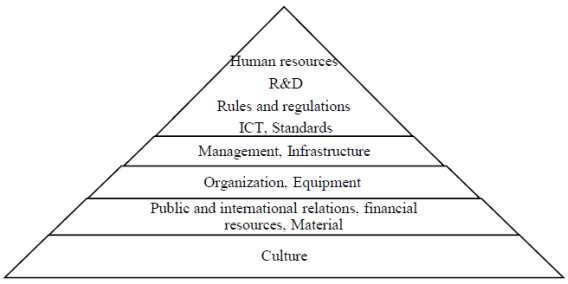


Figure 6: The pyramid of ranking of support components using Q-Analysis

Telecommunication Union (ITU) [44][45][43]. results of the cybernetic model and Q-analysis to group and rank the support components is determined. The results are compared to the Global Cybersecurity Index (GCI) reports of 2015, 2017 and 2018 issued by International Telecommunication Union (ITU) [44][45][43]. The focus was on cryptography. The reports focus on five indices that are "legal, organization, technical, capacity building, and cooperation. The relevant sub-indices are as follows:

- Legal: Cybercrime legislation, Cybersecurity Regulation, Containment/curbing of spam legislation.
- Technical: National/ Government/ Sectorial CERT/CIRT/CSIRT, Standard, technical mechanisms.
- Organization: Strategy, Responsible Agency, Cybersecurity Metrics.
- Capacity Building: Public Awareness, Cybersecurity Standards and Certification for professionals, Cybersecurity Professional Training Courses, National Education Programs and Academic Curriculums, Cybersecurity Research & Development Programs, Incentive Mechanisms.
- Cooperation: Bilateral Agreements, Multilateral Agreements, Public-private partnership, Interagency/intra-agency partnerships.

Table 8: GCI most committed countries globally in 2015 (normalized score)[44]

| Country | Legal | Technical | Organizational | Capacity Building | Cooperation | Index | Global Rank |
|---|---|---|---|---|---|---|---|
| U.S.A | 1 | 0,8333 | 0,875 | 1,000 | 0,5 | 0,8235 | 1 |
| Canada | 0,75 | 1 | 0,875 | 0,875 | 0,5 | 0,7941 | 2 |
| Australia * | 0,75 | 0,6667 | 0,875 | 0,875 | 0,625 | 0,7647 | 3 |
| Malaysia * | 0,75 | 0,8333 | 1 | 0,625 | 0,625 | 0,7647 | 3 |
| Oman * | 0,75 | 0,6667 | 1 | 0,75 | 0,625 | 0,7647 | 3 |
| Norway * | 1 | 0,6667 | 0,75 | 0,875 | 0,5 | 0,7353 | 4 |
| New Zealand * | 1 | 0,8333 | 0,875 | 0,625 | 0,5 | 0,7353 | 4 |
| Brazil * | 0,75 | 0,6667 | 0,875 | 0,75 | 0,5 | 0,7059 | 5 |
| Estonia * | 1 | 0,6667 | 1 | 0,5 | 0,5 | 0,7059 | 5 |
| Germany * | 1 | 1 | 0,625 | 0,625 | 0,5 | 0,7059 | 5 |
| India * | 1 | 0,6667 | 0,755 | 0,875 | 0,375 | 0,7059 | 5 |
| Japan * | 1 | 0,667 | 0,75 | 0,625 | 0,625 | 0,7059 | 5 |
| Republic of Korea* | 1 | 0,6667 | 0,875 | 0,625 | 0,5 | 0,7059 | 5 |
| United Kingdom * | 1 | 0,6667 | 0,75 | 0,75 | 0,5 | 0,7059 | 5 |
| Average | 0,9107 | 0,75 | 0,8482 | 0,7411 | 0,5268 | | |

*:Based on secondary data

Table 9: GCI most committed countries globally in 2017 (normalized score)[45]

| Country | GCI Score | Legal | Technical | Organizational | Capacity Building | Cooperation |
|---|---|---|---|---|---|---|
| Singapore | 0,92 | 0,95 | 0,96 | 0,88 | 0,97 | 0,87 |
| United States | 0,91 | 1 | 0,96 | 0,92 | 1 | 0,73 |
| Malaysia | 0,89 | 0,87 | 0,96 | 0,77 | 1 | 0,87 |
| Oman | 0,87 | 0,98 | 0,82 | 0,85 | 0,95 | 0,75 |
| Estonia | 0,84 | 0,99 | 0,82 | 0,85 | 0,94 | 0,64 |
| Mauritius | 0,82 | 0,85 | 0,96 | 0,74 | 0,91 | 0,7 |
| Australia | 0,82 | 0,94 | 0,96 | 0,86 | 0,94 | 0,44 |
| Georgia | 0,81 | 0,91 | 0,77 | 0,82 | 0,9 | 0,7 |
| France | 0,81 | 0,94 | 0,96 | 0,6 | 1 | 0,61 |
| Canada | 0,81 | 0,94 | 0,93 | 0,71 | 0,82 | 0,7 |
| Average | | 0,934 | 0,91 | 0,8 | 0,943 | 0,701 |

Table 10: GCI most committed countries globally in 2018 (normalized score)[43]

| Rank | Member States | GCI Score | Legal | Technical | Organizational | Capacity Building | Cooperation |
|---|---|---|---|---|---|---|---|
| 1 | United Kingdom | 0,931 | 0,2 | 0,191 | 0,2 | 0,189 | 0,151 |
| 2 | U.S.A | 0,926 | 0,2 | 0,184 | 0,2 | 0,191 | 0,151 |
| 3 | France | 0,918 | 0,2 | 0,193 | 0,2 | 0,186 | 0,139 |
| 4 | Lithuania | 0,908 | 0,2 | 0,168 | 0,2 | 0,185 | 0,155 |
| 5 | Estonia | 0,905 | 0,2 | 0,195 | 0,186 | 0,17 | 0,153 |
| 6 | Singapore | 0,898 | 0,2 | 0,186 | 0,192 | 0,195 | 0,125 |
| 7 | Spain | 0,898 | 0,2 | 0,18 | 0,2 | 0,168 | 0,148 |
| 8 | Malaysia | 0,893 | 0,179 | 0,196 | 0,2 | 0,198 | 0,12 |
| 9 | Norway | 0,892 | 0,191 | 0,196 | 0,177 | 0,185 | 0,143 |
| 10 | Canada | 0,892 | 0,195 | 0,189 | 0,2 | 0,172 | 0,137 |
| | Average | | 0,1965 | 0,1878 | 0,1955 | 0,1839 | 0,1422 |

The indices of Cybersecurity for the highest ranked countries, issued in GCI 2015, 1017, and 2018 are presented in Tables 8, 9 and 10.

Based on the indices presented in Tables 8, 9 and 10 the relevant sub-indices, GCI reports indicate that *regulation*, *standard*, *R&D*, *education*, and *management* have the highest priority in developing cybersecurity or cryptographic algorithms.

## 6. Conclusion

The cybernetic meta-model of encryption has the following four components: *policy and strategy*, *main processes*, *supportive processes*, *control processes*. The *main processes* has four processes. Also, the *supportive processes* encompasses 13 processes, grouped in *hard* and *soft* ones. These processes have four *development stages* which determine *type of applications*, proper *theoretical basis*, *implementation*, and *evaluation*.

The interactions of *main* and *supportive* processes shape the structure of the encryption system. These interactions result in a complex graph. A proper method to tackle such a complex entity is Q-analysis, which groups and ranks the components due to their interactions. Each interaction is also evaluated, based on its four *development stages*. A questionnaire is developed to evaluate the interactions. Then, a group of 30 ICT evaluated the interactions by assigning scores from 0 to 10, which indicate significance of an interaction.

The outputs of Q-analysis indicate that the most significant components, or the group with the highest priority, for developing an encryption system consists *Human resources*, *R&D*, *Rules and regulations*, *ICT*, and *Standards* components. These result is accordance with the GCI 2015, GCI 2017 and GCI 2018 reports issued by ITU.

## 7. References

[1] W. Liu, B. Ying, H. Yang, and H. Wang, "Accurate modeling for predicting cryptography overheads on wireless sensor nodes," in *Advanced Communication Technology. ICACT 2009. 11th International Conference*, vol. 2, Phoenix Park, 2009, pp. 997–1001.

[2] D. Nilesh and M. Nagle, "The new cryptography algorithm with high throughput," in *2014 International Conference on Computer Communication and Informatics*, Coimbatore, 2014, pp. 1–5.

[3] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, Dec. 2016.

[4] M. Rashid, M. Imran, and A. Jafri, "Comparative analysis of flexible cryptographic implementations," in *2016 11th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)*, Tallinn, 2016, pp. 1–6.

[5] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. Mazurek, and C. Stransky, "Comparing the Usability of Cryptographic APIs," in *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2017, pp. 154–171.

[6] A. Poojari and H. Nagesh, *Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing*. Singapore: Springer, 2019, vol. 755, ch. A Comparative Analysis of Symmetric Lightweight Block Ciphers, pp. 705–711.

[7] D. Karaoğlan Altop, A. Levi, and V. Tuzcu, "Deriving cryptographic keys from physiological signals," *Pervasive and Mobile Computing*, vol. 39, pp. 65–79, Aug. 2016.

[8] O. Uzunkol and M. S. Kiraz, "Still wrong use of pairings in cryptography," *Applied Mathematics and Computation*, vol. 333, pp. 467–479, Sep. 2018.

[9] S. Feizi, A. Ahmadi, and A. Nemati, "A hardware implementation of Simon cryptography algorithm," in *2014 4th International Conference on Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, 2014, pp. 245–250.

[10] A. Gupta and N. Walia, "Cryptography Algorithms: A Review," *International Journal of Engineering Development and Research*, vol. 2, no. 2, pp. 1667–1672, 2014.

[11] National Institute of Standards and Technology (NIST), "NIST Cryptographic Standards and Guidelines Development Process," U.S. Department of Commerce, United States of America, Technical report, 2016.

[12] CompTIA Information Technology, "IT INDUSTRY OUTLOOK 2018," CompTIA, Research report, 2018.

[13] P. Pawlak and P.-N. Barmpaliou, "Politics of cybersecurity capacity building: conundrum and opportunity," *Journal of Cyber Policy* , vol. 2, no. 1, p. 123–144, 2017.

[14] The Global Cyber Security Capacity Centre, "Cyber Security Capability Maturity Model (CMM) – V1.2," Oxford Martin School, University of Oxford, United Kingdom, Technical report, 2014.

[15] J. Cristopher, F. Muneer, and J. Fry, "Cyber Security Capability Maturity Model (C2M2)," U.S. Department of Homeland Security (DHS), United States of America, Technical report, 2014.

[16] ISO/IEC JTC1, *ISO/IEC 27002: Information Technology- security techniques-information security management systems –code of practice for information security controls*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2013.

[17] ISO/IEC JTC1, *ISO/IEC 27001: Information Technology- security techniques-information security management systems–Requarments*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2013.

[18] ISO/IEC JTC1, *ISO/IEC 27011: Information Technology-security techniques-information security management guidelines for telecommunications organizations based on ISO/IEC 27002*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2016.

[19] ISO/IEC JTC1, *ISO/IEC 27005: Information Technology-security techniques-information security risk management*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2011.

[20] F. Wamala, "The ITU National Cybersecurity Strategy Guide," International Telecommunication Union (ITU), Geneve, Switzerland, Technical report, 2001.

[21] N. Falessi, R. Gavrila, M. Klejnstrup, and K. Moulinos, "National Cybersecurity Strategies: Practical Guide on Development and Execution," European Network and Information Security Agency (ENISA), Technical report, Dec. 2012.

[22] International Telecomunication Union, *Recommendation X.805: Security Architecture for system providing end-to-end Communications*, ITU, Oct. 2003.

[23] I. T. Union, *Security in Telecommunications and Information Technology Security in telecommunications and Information Technology*, ITU, Sep. 2015.

[24] K. Stine, K. Quill, and G. Witte, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, Feb. 2014.

[25] J. Sherwood, C. Andrew, and L. David, "Enterprise Security Architecture," SABSA, Technical report, 2016.

[26] I. Damaj and S. Kasbah, "An analysis framework for hardware and software implementations with applications from cryptography," *Computer and Electrical Engineering*, vol. 69, pp. 572–584, Jul. 2018.

[27] W. Norbert, *Cybernetics: or the Control and Communication in the Animal and the Machine*. Wiley, 1948.

[28] D. Novikov, *Cybernetics: From Past to Future*. Springer, 2016.

[29] R. Ramazani, "The Current Challenges of Universities and the National Science Development System," *Journal of Research and Planning in Higher Educatio*, vol. 8, no. 3, pp. 37–62, 2002.

[30] R. Ramazani, "Feasibility study of network on science and technology parks Inter-Islamic Network On Science & Technology Parks," in *Comstech*, 2010.

[31] A. Mirzadeh Phirouzabadi, M. Moattar Husseini, and M. Arasti, "General cybernetic model for innovation network Management," in *International Conference on Leadership, Technology and Innovation Managment*, Istanbul, Turkey, 2011.

[32] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, 1996.

[33] S. Picek, D. Jakobovic, J. Miller, L. Batina, and M. Čupić, "Cryptographic Boolean Functions: One Output, Many Design Criteria," *Applied Soft Computing*, vol. 40, pp. 635–653, 2015.

[34] R. Saha and G. Geetha, "Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms," *Chaos, Solitons & Fractals*, vol. 104, pp. 371–377, 2017.

[35] M. A. Hossain, M. Hossai, M. Uddin, and S. Imtiaz, "Performance Analysis of Different Cryptography Algorithms," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 3, pp. 659–665, 2016.

[36] N. Jorstad, "Cryptographic Algorithm Metrics," Institute for Defense Analyses Science and Technology Division, Technical report, 1997.

[37] M. Ebrahim, S. Kham, and U. Khalid, "Symmetric algorithm survey: A comparative analysis," *International Journal of Computer Applications* , vol. 61, no. 20, pp. 12–19, 2013.

[38] J. Johnson, "Some structures and notation of Q-analysis," *Environment and Planning B: Planning and Design*, vol. 8, pp. 73–86, 1981.

[39] L. Duckstein, "Evaluation of the Performance of a Distribution System by Q-Analysis," *Applied Mathematics and Computation*, vol. 13, pp. 173–185, 1983.

[40] R. Atkin, *Mathematical Structure in Human Affairs*. Heinemann Educational Publishers, 1971.

[41] J. L. Casti, *Connectivity, Complexity, and Catastrophe in Large-Scale Systems*. J. Wiley Chichester [Eng.] ; New York, 1979.

[42] M. Heinonen, A. Lampi, L. Hyvönen, and D. Homer, "Dietary sources of conjugated dienoic isomers of linoleic acid, a newly recognized class of anticarcinogens," *Journal of Food Composition and Analysis*, vol. 5, no. 3, pp. 198–208, 1992.

[43] International Telecommunication Union, "Global Cybersecurity Index (GCI) 2018," ITU, Technical report, 2018.

[44] International Telecommunication Union, "Global Cybersecurity Index &Cyberwellness Profiles," ITU, Technical report, 2015.

[45] International Telecommunication Union, "Global Cybersecurity Index (GCI) 2017," ITU, Technical report, 2017.