Logic of Perfect Secrecy in Àrokò Computational Cryptography

LONGE Idowu Oluwaseun
Mathematics, Statistics and Computer information systems Department.
Achievers University, Owo. Nigeria.

ABSTRACT.
Information Security has been a major issue in the world, such that different societies and communities design and develop different forms of cryptosystem in ages which level of security could be tested by perfect secrecy.
Àrokò is a non-verbal, symbolic material form of communication and a traditional way of sending information among the Yorùbá people formed in the ages before the Colonia era which is growing wane in this age. This paper examines the cultural heritage of the Yorùbá people with probability distribution in comparing the concept of Àrokò cryptosystem secrecy in Yorùbá tradition to logic of perfect secrecy of Shannon.

Keyword: Cryptography (Àrokò), Yorùbá, Communication Security, cryptosystem, perfect secrecy, probability distribution and cultural heritage.

1. INTRODUCTION
Information Security has been a major issue in organizations, societies and communities in the past and in the present especially during war or any form of confidential matters. It could be seen as the intersection of Physical, Operational and Management platforms of security. It is also needful for a community to creating and implementing a good cryptosystem.

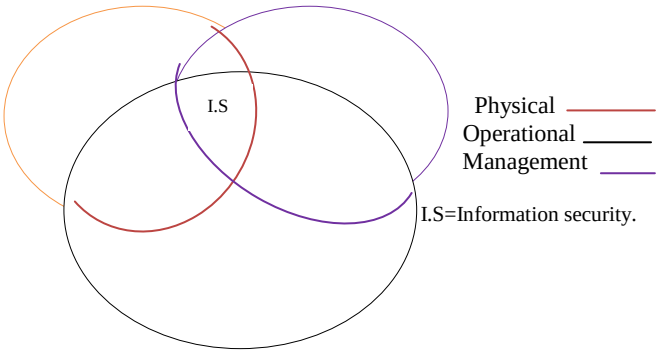

Diagram 1: intersection of forms of security.

Diagram 1 shows that information security or any form of security is not totally in form without these three major parts: Physical, Operational and Management policies on security.
A cryptosystem is a pair of algorithms that take a *key 'K'* and convert *plaintext 'M'(message)* to *ciphertext 'C'* and back, also Cryptography is the art of concealing information. Song (2008) defined cryptography as the study of the processes of encryption (mapping the original message, called the plaintext into a secret form, called the ciphertext, using the encryption key and decryption (Inverting the ciphertext back to the plaintext, using the corresponding decryption key), in such a way that only the intended recipients can decrypt and read the original message.

$$\text{Cryptography} = \text{Encryption} \oplus \text{Decryption}.$$

Claude Shannon (1949) in her paper titled "Communication Theory of Secrecy Systems" in the Bell Systems Technical Journal discovered that there was an influence on the scientific study of cryptography. Although most communities had a way with information security due to the challenges they had encounter thereby creating a particular cryptosystem to protect their information based on their knowledge in the ages like Caesar and substitution cipher, Rotor machine during the second world war, Vigenere Cipher, Àrokò (Yorùbá) etc, although some cryptosystem are vulnerable to cipher only attack and some are not. A good cryptosystem should be no way short of enumerating all possible keys to find the key from any reasonable amount of ciphertext and plaintext, nor any way to produce plaintext from ciphertext without the key, enumerating all possible keys must be infeasible and the ciphertext must be indistinguishable from true random values.
Yorùbá form of information security (cryptography) 'Àrokò' which is a form of symmetric algorithm [4] is one of the cultural heritage of the Yorùbá people and it is as old as the tradition itself. This Àrokò as now been discovered to be going wane hence the need for this cryptography to be tested maybe is vulnerable to cipher only attach or has perfect secrecy.

Definition
Suppose X and Y are random variables. We denote the probability that X takes on the value x by $Pr\,[x]$, and the probability that Y takes on the value y by $Pr\,[y]$. The joint probability $Pr\,[x,y]$ is the probability that X takes on the value x and Y takes on the value y. The conditional probability $Pr[x|y]$ denotes the probability that X takes on the value x given that Y takes on the value y. The random variables X and Y are said to be independent
if $Pr[x,y] = Pr[x] \cdot Pr[y]$ for all possible values x of X and y of Y.
Joint probability can be related to conditional probability by the formula

$$Pr[x,y] = Pr[x|y] \cdot Pr\,[y]$$

Interchanging x and y, we have that

$$Pr[x,y] = Pr[y|x] \cdot Pr\,[x]$$

From these two expressions, we immediately obtain the following result, which is known as Bayes' Theorem.
Theorem 1: (Bayes ' Theorem)
If $Pr\,[y] > 0$ then

$$Pr[x|y] = \frac{Pr[x] \cdot Pr\,[y|x]}{Pr\,[y]} \quad .$$

X and *Y* are independent variables if and only if $Pr[x|y] = Pr\ [x]$ for all *x, y*.

Definition:
A conventional Secret key cryptosystem (or secret – key encryption or secret – key cipher) S may be formally defined as follow

$$E_K : M \rightarrow C$$

S = (*M,C,K,m,c,k,E,D*)
where
M = the set of plaintexts (plaintext space)
C = the set of ciphertext (cipherext space)
K = the set of keys
$m \in M$ is a piece of plaintext
$c \in C$ is a piece of ciphertext
K is the key for both encryption and decryption
E is the encryption function

$$E_K(M): M \rightarrow C$$

Where *M* maps to *C*, using the key *K*, such that

$$C = E_K(M)$$

D is the decryption function

$$D_K : C \rightarrow M$$

Where *C* maps to *M*, using the same key *K* again such that

$$M = D_K(C)$$

Satisfying
$E_K D_K = 1$ and $D_K(C) = D_K\big(E_K(M)\big) = M$ …. {1.2}
Since a cipher defined over (*K,M,C*) is a pair of 'efficient' algorithms (*E,D*) where
$E : K \times M \rightarrow C$, $D : K \times M \rightarrow M$
s.t for all $m \in M, k \in K$, $[D(K, E(K, M))] = M$ {1.3}
Equation {1.2} and {1.3} show that the decryption of an encrypted message gives *M* (the message)

Definition :
A symmetric encryption scheme is a tuple of algorithms (*Gen;E*$_k$*;D*$_k$) with message-space *M* and key-space *K* where Gen and E_k are possibly randomized and D_k is deterministic such that for all messages $m \in M$ and keys $k \in K$
$Pr[\ D_k\big(E_k(m)\big) = m] = 1$ …… {1.4}
Equation {1.4 } shows that the probability of decrypting an encrypted message '*m'* using the same key (knowledge) back to the message '*m'* is sure or constant.

Probability distribution is important to ideology of information security and Shannon 1949 used it in proving the concept of perfect secrecy. This paper adopted it to see it the computational cryptography (Àrokò) in Yorùbá tradition [9] proses the properties of perfect secrecy.

2. PERFECT SECRECY

Definition (perfect secrecy)
An encryption scheme satisfies perfect secrecy if for all messages $m_1, m_2 \in M$ and ciphertexts $c \in C$, we have

$$Pr_{K \leftarrow \mathcal{K}}[E(K, m_1) = c] = Pr_{K \leftarrow \mathcal{K}}[E(K, m_2) = c] \quad \text{..} \{2.1\}$$

Theorem 2: variation. An encryption scheme (*E,D*) over a message space *M* is perfectly secret if and only if for every probability distribution over *M*, every message $m \in M$ and every ciphertext $c \in C$:

$$Pr[\ C = c|M = m] = Pr\ [C = c] \quad \text{…… } \{2.2\}$$

Proof
Fix a distribution over *M* and arbitrary $m \in M$ and $c \in C$. Say

$$Pr[\ C = c|M = m] = Pr\ [C = c]$$

Multiplying both sides of the equation by $\frac{Pr\ [M=m]}{Pr\ [C=c]}$ gives

$$\frac{Pr[\ C=c|M=m] \cdot Pr[M=m]}{Pr\ [C=c]} = Pr\ [M = m]$$

Using theorem 1, the left hand-side is exactly equal to

$$Pr\ [M = m|C = c]\ .$$

Thus, $Pr[M = m|C = c] = Pr\ [M = m]$.
and the scheme is perfectly secret.
To prove in the other direction we start with $Pr[M = m|C = c] = Pr\ [M = m]$ and multiply both sides by $\frac{Pr\ [C=c]}{Pr\ [M=m]}$ It give .

$$\frac{Pr[M = m|C = c] \cdot Pr[C = c]}{Pr\ [M=m\ ]} = Pr\ [C = c]$$

which is equal to our starting equation,
$Pr[C = c|M = m] = Pr\ [C = c]$, hence proving both definitions equivalent.
Theorem 3 *(E,D)* is perfectly secure if and only if .Pr$[Adv\ successful] \leq \frac{1}{2}$
Theorem 4
An encryption scheme (*E,D*) over a message space *M* is perfectly secret if and only if for every probability distribution over *M*, every $m_1, m_2 \in M$, and every $c \in C$:

$$Pr\ [C = c|M = m_1] = Pr\ [C = c|M = m_2] \quad \text{……} \{2.3\}$$

Proof
Assume that encryption scheme is perfectly secret and fix messages $m_1, m_2 \in M$ and ciphertext $c \in C$. By earlier theorem we have,

$$Pr\ [C = c|M = m_1] = Pr\ [C = c] = Pr\ [C = c|M = m_2]$$

completing the proof in the first direction. Assume next that for every distribution over *M*, every $m_1, m_2 \in M$, and every $c \in C$ it holds that

$$Pr[C = c|M = m_1] = Pr\ [C = c|M = m_2].$$

Fix some
distribution over *M*, and an arbitrary $m_1 \in M$ and $c \in C$. Define

$$p \stackrel{\text{def}}{=} Pr\ [C = c|M = m_1]$$ Since

$\Pr[C = c|M = m] = \Pr[C = c|M = m_1] = p$ for all *m*, we have

$$Pr[C = c] = \sum_{m \in M} Pr\ [C = c|M = m] \cdot Pr\ [M = m]$$

$$= \sum_{m \in M} p \cdot Pr\ [M = m]$$

$$= p \sum_{m \in M} Pr\ [M = m\ ]$$
$$= p$$
$$= Pr\ [C = c|M = m_1]$$

Theorem 5: if (*E,D*) is perfect secret ,then

$$|K| \geq |M| \quad \text{…….. } \{2.4\}$$

Proof
The condition of perfect secrecy specifies that,$\forall\ m \in M$, $\forall$ $c \in C$ for which $\Pr[C = c] > 0$

$$Pr[M = m|C = c] = Pr\ [M = m] \quad \text{……} \{2.5\}$$

by contradiction ,let assume that $|k| < |m|$,

$$m(c) = \{m|\exists k = K \text{ such that } E_k(m) = c\}$$

Roughly the above equation is saying that there exists a key *k* such that the encryption of the message ' *m'* with ' *k* ' yields cyphertext ' *c* '.
in figuring out which messages correspond to specific cipher text. The set of decryption

$\{D_k(c): k = K \quad \text{for a } c \in C\}$
Implies $|m(c)| \leq |k| < |m|$.
it is less than or equal to the number of keys, since decrypting using all the keys might derive same message twice but at best it might be a deferent message for each key and assumption stated that number of keys is less than message so it shows the last inequality. This also suggests that there exists '*ḿ*' that cannot be recovered from '*c*' meaning that '*ḿ*' cannot be encrypted to '*c*' no matter what the key. Mathematically, ∃ $ḿ \in M$ such that $ḿ \notin M(c)$.
But then $Pr[M = ḿ|C = c] = 0 = P\,r[M = ḿ]$ and so the scheme is not perfectly secret. This is because the probability that the message '*ḿ*' is the message becomes '0' if there is no way to produce cyphertext '*c*' from it. The conclusion of this proof is that in order for a scheme to be perfectly secret there must be at least as many possible keys as possible messages. We need an alternate (equivalent) definition of perfect secrecy that can be relaxed.

2.1 Example of perfect secrecy: One Time Pad(OTP)[8]

$M: \{0,1\}^l$, where *l* is the message length.
$K: \{0,1\}^l$.
$c = E(k,m) = m \oplus k$, for $m \in M, k \in K$, where ' stands for bit-wise or
$m = D(k,c) = c \oplus k$, For $m \in M, k \in K$
Decryption works due to

$$(c \oplus k) = \big((m \oplus k) \oplus k\big) = m \oplus (k \oplus k) = m$$
$$D_k\big(E_k(m)\big) = m$$

Theorem 6: OTP encryption satisfies the perfect secrecy requirement.
Proof: take any $m \in M$ and $c \in C$, let $k^* = m \oplus k$ .since

$$Pr_{k\leftarrow K}[\,E(k,m) = c = Pr_{k\leftarrow K}[(k \oplus m) = c],$$
$$= Pr_{k\leftarrow K}[k = c \oplus m]$$
$$= Pr_{k\leftarrow K}[k = k^*]$$
$$= \frac{1}{2^l}$$

The equation holds for every $m \in M$, it follows that for every $m_1, m_2 \in M$ we have $Pr[E(k,m_1) = c] = \frac{1}{2^l}$
As well as $Pr[E(k,m_2) = c] = \frac{1}{2^l}$
This implies that

$$Pr[E(k,m_1) = c] = \frac{1}{2^l} = Pr[E(k,m_2) = c]$$

This establishes perfect security of OTP

2.2 Limitations of One-Time Pad

Unfortunately , One-time pad encryption scheme has limitation on perfect secrecy since there is a requirement that the length of the key be long as the message (equation {2.4}) and the long key must be securely stored which is sometimes problematic in nature or not really achievable.
In particular, say two messages *m, ḿ* are encrypted using the same key *k*. An adversary who obtains

$$c = m \oplus k \text{ and } \check{c} = ḿ \oplus k \text{ then}$$
$$c \oplus \check{c} = (m \oplus k) \oplus (ḿ \oplus k)$$
$$= m \oplus ḿ$$

And thus learn something about the exclusive-or of the two messages. While this may not seem very significant, it is enough to rule out any claims of perfect secrecy when encrypting two messages. Furthermore, if the messages correspond to English-language text, then given the exclusive-or of two sufficiently long messages, it has been shown to be possible to perform frequency analysis and recover the messages themselves.[8]

3. ÀROKÒ

Yorùbá's which are located in the south-western part of Nigeria; they are very rich in culture and have different ways of communication (verbal and non-verbal) even though there are some in other parts of Nigeria. The culture is rich to the extent that it is possible to communicate to a crowd with the intention of communicating to some particular listener. For instance the talking drum (gongon), owe (proverb) and Ìjálá (hunter's song**)** are forms of coding information to the people. There are many types of art among the Yorùbá's, and many objects are placed on shrines to honor the gods and ancestors or placed in the communities to send a message (e.g a palm frond tied round a place or shrines: means: - *a sacred place or do not trespass*).
Traditionally, writing has not been the main way for the Yorùbá to talk about their history and experiences. Instead, stories and histories are passed down from generation to generation by word of mouth. see [14]. Then to need to communicate within a long distant that must maintain messages confidentiality, integrity etc, was solved by Àrokò [9]
Àrokò is a non-verbal symbolic representation of information [1],[13]. Some scholars like [11], [12] and [13] shows that Àrokò could be used to warn, resolved conflict, inflict punishment (Fig 6 and Fig 7) and instigate war (Fig 5) .
[10] proved that cowrie is used as legal tender in the ages past and can also be use to send Àrokò (Fig 1 and 2) .
[1] and [13] explained the classifications of Àrokò and different forms and reasons why Àrokò is growing wane such as: The invention of modern transportation and communication facilities (Cars, Airplanes, Post offices, phone, email, fax etc.), shortage of personals equipped with the arts of encoding and decoding the contents of an Àrokò, drastic reduction in the influence and power of the traditional rulers, availability of conventional road signs that often make the ancient ones unpopular, constitutional and judicial system of regulating the power of an individual or a community or an institution. [9] later added politic, act of imitating foreign lands way and Religion to the reasons. They also viewed Àrokò as, a form of concealing information in a symbolic material (cryptography) , symmetric algorithm (with the knowledge as the key *K*) and computationally secured ,whereby defining Àrokò cryptography as follows:

"Àrokò cryptography is study of the art of concealing or encryption (collecting items and materials to form a symbolic representation of intended message) called symbolic cipher using the encryption key (in-depth knowledge of involved items and materials) and decryption (inverting the symbolic cipher back to the message) using the corresponding key as the decryption key in such a way that the receiver will get the intended meaning of the message."[9]

This portends that the dissemination of information through Àrokò is as old as the Yorùbá culture itself. The symbolic aspect of it necessitates the need for one to be vast in the knowledge of the materials put together in the Àrokò and in the function of the materials. The particular form of the Àrokò strongly rests on the intent of the sender and his/her relationship with the receiver. Àrokò includes single or combined edible or non – edible items i.e. kola nut, comb, bitter kola, pepper, arrow and bow, cowry shells, pieces of textile, chalk or barks of trees, rock, seeds, feathers tools , , metals (cutlass or gun), clothes e.t.c

Àrokò involves sending an item or a combinable number of items to a person from which the decoder is expected to infer a piece of information [1]. Àrokò can be classified based on the discourse functions they perform: warning, admonition, punishment, conflict, announcement/marketing strategy, indicator/directive, expression of affection and pleading [1]. Àrokò could be sent by a traditional ruler, a chief, Ifa priest, Ogboni cult member, hunter, artisan, warrior or an ordinary person to a counterpart or any other person, group or body [1] and [6].

There are three factors that are exigent and expedient to an effective Àrokò.
These are: the sender, the receiver and the bearer [1][9][10][11][12] and [13]. Both sender and receiver need to be Skilful in the encryption' E_k 'and decryption' D_k' using the in-depth knowledge of the material involve in the Aroko '$k \in K$' as key [9] but the bearer could be trustworthy slave or most trusted son. The Aroko must be protected to maintain confidentiality, integrity, authentication, authorization and nonreduation. Both sender and receiver have to operate within encompassing elements and the context to make Àrokò meaningful [2].
Àrokò is useful for some following purposes: to convey confidential messages(whereby maintaining the integrity, nonreduation, authentication and authorization using the bearer , the massage might even leads to the bearers death,),to avoid verbal (problematic features like manipulations or distortion, misconception etc) see [11][12]

This form of symmetric and computational cryptosystem is difference not that is symbolic only but the encryption of a

particular $m \in M$ using key k could give difference cipher:
$c_1 , c_2 \in C$ such that $c_1 \neq c_2$

$$Pr\,[D(k, c_1) = m = Pr\,[D(k, c_2)],\ \ c_1 \neq c_2 \quad \ldots\ldots \{3.1\}$$

3.1 ÀROKÒ LIMITATIONS IN 21ST CENTURIES

Àrokò has competency and security limitations in 21st centuries due to the following issues:

- Bearer (availability of trusted Slaves or individual person to deliver the symbolic cipher) .
- Inadequate Knowledge (key) of the symbolic materials involved in preparing (Encrypting) and decrypting of the symbolic information passed to the new generation.
- Inappropriate documentation of the material and the meaning of the materials involved.

Àrokò is sometimes interpreted in the public in the present of other Yorùbá's with explanation to teach the next generation the concert and meaning but not all is done publicly so as to keep the secrecy.
Each Àrokò symbolic cipher always has more than one meaning (the decoy meaning and the literal in-depth meaning): If eight cowrie shells are sent to someone, it means such an individual is free from danger and in ages or Three cowry shells: It is an Aroko which conveys the message to the recipient that the sender has rejected his/her proposal, offer or request (Fig 8) . cowrie shells were legal tender used to buy and sell goods. See [10][9] .
The statement also implies: for all messages $m_1 , m_2 \in M$ and symbolic cipher $c \in C$, we have

$$Pr[E(K, m_1) = c] = Pr\,[E(K, m_2) = c] \quad \ldots. \{3.2\}$$

This shows there is no symbolic cipher attach only without key *K* (equation {3.2} satisfy {2.1}, {2.2} and {2.3})

4. CULTURAL HERITAGE

Definition
Cultural heritage is a group of resources inherited from the past which people identify, independently of ownership, as a reflection and expression of their constantly evolving values, beliefs, knowledge and traditions. It includes all aspects of the environment resulting from the interaction between people and places through time. see [16] and [5].
Cultural heritage conservation helps a community not only to protect economically and valuable physical assets, but also preserves its practices, history, and environment, and a sense of continuity and identity.
Although Communities must prioritize which cultural assets to preserve, considering both cultural meaning and livelihood implications. Reaching a consensus may be difficult but Àrokò cryptosystem level of extinction is increasing.
Cultural heritage conservation plans are best designed before a disaster, but, in their absence, heritage authorities can and should collaborate to develop effective post-disaster heritage conservation strategies

The world bank 2013 had this following key decision on cultural heritage:

- The lead agency for heritage conservation should collaborate with the lead disaster agency and local governments to ensure cultural resources are considered in post-disaster damage and loss assessments.
- Communities in collaboration with local government and the lead agency for heritage conservation should identify and prioritize cultural resources that require conservation during recovery and reconstruction and document the condition of these resources.
- Communities in collaboration with local government and the lead agency for heritage conservation should decide whether adequate instruments or plans are in place to address post-disaster cultural heritage risks. If so, they should be activated. If not, stakeholders should work together to carry out the cultural heritage planning.
- The lead agency for heritage conservation should decide whether available local resources are adequate to address the post-disaster cultural heritage risks that have been identified. If not, it should identify and mobilize outside financial and technical assistance
- Churches, tribal organizations, and other guardians of cultural resources should ensure that their resources are included in post-disaster assessments and should request assistance in conserving them, if required.etc

5. PERFECT SECRECY AND ÀROKÒ

Àrokò cryptosystem as design by Yorùbá people whose has no idea on how to write, not to imagine probability distribution satisfy some interest theorem of perfect secrecy, but has a particular and fundamental equation{3.1} stated below
'Given a random symbolic ciphers $c_1, c_2 \in C$, there exist a message $m \in M$ such that

$$Pr\,[D(k, c_1) = m = Pr\,[D(k, c_2)] \quad \text{Where} \quad c_1 \neq c_2$$

Which is not indicated or analyzed in a perfect secrecy of a symmetric algorithm ,equation {3.2} and {2.1} looks alike although equation {2.4 } could not be assumed to be satisfy by Àrokò, due to some unknown basic key of Àrokò formation (all materials that could be used) and secrete that are kept by Ogboni cult and the tradition priest

Example: from [11]

1 , Warning of war (*m*) : If a community sent **A bow and some arrows** $'c_1'$to other community as a form of Àrokò it means the community which sent the materials of war is sending message of war to the recipient community. If the recipient community embraces peace, the matter will be settled amicably, but not without payment of tribute. However, the recipient community may decline in sending message of peace, which may eventually lead to both communities engaging in warfare. A **gun or a cutlass tied with palm front** $'c_2'$ may be sent too, as an Àrokò of war (see figure 5). Palm frond is a symbol synonymous with Ogun, who is god of war and cutlass is one of his military weapons. It specified equation {3.1}

2, Warning against Adultery or Illicit Sexual Relationship (*m*)

Adultery is an outrageous crime among the Yorùbá natives. It is an offence against the religious objects of the husband, including his ancestors. It is also a criminal act against the gods (Adewale 1994). Hence, adultery is a total abomination. A person who is having an illicit sexual affair with another man's wife can be warned through Àrokò. For instance, if **feathers of a fowl are plucked** $'c_1'$ and deposited at the door of a man (see figure 9), it is an indication that the man is having an illicit sexual affair with a woman who is not his wife, and probably the wife of the sender of the Àrokò or the relative of the sender. The message encoded in such Àrokò is that, the husband of the woman he is having illicit sexual affair with, is aware of the illicit relationship, and therefore, the erring man should desist from such woman, otherwise, a doom will be let loose on the erring man. Apart from plucked feathers of a fowl, **firebrands** $'c_2'$ could also be used as the Àrokò . (see figure 10). Firebrands represent fire and the interpretation of this is that, if the adulterous man does not stop his illegal sexual relationship with the wife of the sender, his house will be eventually burnt down by the offended rightful husband of the woman. Hence, there is a popular saying which goes thus: "Eni ba se n nkan Itufu, ni boju wehin ikule" –
meaning (it is somebody who is wayward in his character that will always fear that firebrands might have been deposited his house).Feathers of a fowl and the
firebrands are Àrokò, warning against adulterous man within Yorùbá context. satisfy {3.1})

3, Break up *(m)*

If a man or a woman sends a **comb** $'c_1'$ to his/her lover it signifies that their union, love and affection have ended. It is a symbol of total separation. Fig 3

Cowry shells strung back to back $'c_2'$and sent to a recipient means the sender is breaking his/her relationship with the recipient. Fig 2. Satisfy {3.1})

6. CONCLUSION

In this 21th century there are easier, faster and more secured form of cryptography but Àrokò is a cultural heritage of the Yorùbá people which needs to be documented and preserved, some Àrokò are formulated or prepared based on Yorùbá proverbs (Example 2) . by research Àrokò has not been proven diabolical, although most of the vital information of the key (knowledge of encrypting and decrypting) are kept with the occult and Yorùbá priest, but been diabolic or not, this rich Yorùbá traditional cryptosystem could be roughly say it has perfect secrecy if theorem 5 is relaxed (since some of the length of the keys *K* is still kept secret by the rulers of Yorùbá communities[1]and [13]) and it has a probability statement which is not in basic properties applicable to perfect secrecy suggested by Shannon 1949.

This form of brilliant cryptography idea by the old Yorùbá empire in the ages, in which it has no symbolic cipher attack only since it satisfied basic properties of perfect secrecy, and it computationally secured [9] should not just be extinct. Although the economic value of Aroko is not basically stated in this paper.

7. RECOMMENDATION

Perfectly secured or not, Àrokò is the Yorùbá cultural heritage so the following recommendations were considered appropriately:

- Àrokò should be computer based and sent through computer network (secured channels) to enhance its security and fit for the 21th century.
- The knowledge of the keys should at least be taught in Nigeria Schools.
- The United Nations Educational, Scientific and Cultural Organization (UNESCO) and/or the International Centre for the Study of the Preservation and Restoration of Cultural Property (ICCROM) should come to the aid of saving this Àrokò Yorùbá cultural heritage.

8. REFERENCE

[1] Abdullahi-Idiagbon, M. S. 2009. African Tradition Semiotics: The example of Àrokò in Yorùbá Tradition". International Journal on Culture and Tradition, Vol 3, pp 115-*135.*

[2] Afolabi, Olabode. 2004. '*Aroko: The Traditional Mean of Communication among the Yoruba People'*. Retrieved from ww.utexas.edu/conference/ Africa/2004/data base on 30/2/2014.

[3] Antonio, R.N 2011. *Foundations of Cryptography,* Italy : Spring

[4] Boaz, B. 2010. '*Lecture2 perfect Secrecy and its Limitations'*, New Jersey: Princeton University, Spring.

[5] Cornelia Dümcke and Mikhail Gnedovsky 2013. '*The Social and Economic Value of Cultural Heritage: literature review'* European expert network on culture (EENC)

[6] Falola, T and Adebayo, A. G 2000. Culture, Politics and Money among the Yorùbá. Retrieved from www.booksgoogle.com.ng/ books on 30/12/2012

[7] Fayemi A.K 2010 "*Logic in Yoruba proverbs*" Itupale Online Journal of African Studies 2 (2010) 1-14

[8] Kannan S 2009 '*Lecture Notes 2: Shannon's theory on Perfect Secrecy'*. Crypto-Scope retrieved http://www.eit.lth.se/fileadmin/eit/courses/edi051/lecture_notes/LN3.pdf on 15/05/2014

[9] Longe I.O , Akindipe O.T and Bada A.A 2014 *'Computational Cryptography (Àrokò) in Yorùbá tradition'* International journal for computer application; foundation of computer science,New York,U.SA. 85(2):6-12

[10] Odunbaku, B. 2012. "*Importance of Cowrie Shell in Pre-colonial Yorùbá Land South Western Nigeria: Orile-Keesi*", International Journal of Humanities and Science. Vol. 2 No 18

[11] Ojo Matthias O 2013 *'Symbols of warning, conflict, punishment and war and their meanings among the pre-colonial Yorùbá natives: A case of Àrokò '* Originalni naučni rad.

[12] Ogundeji, P. A. 1997. "*The Communicative and Semiotic Context of Àrokò among the YorùbáSymbol-Communication System*",African Languages and Cultures, Vol 10 No 2.

[13] Opadokun, O. 1986. *Àrokò.* Ibadan: Vantage Publishers Ltd.

[14] Phoebe A 2004 '*Yoruba Art and Culture'* hearst museum of anthropology, University of California

[15] Song, Y. Y. 2008.' *Cryptanalytic Attacks on RSA'*. New York; London: Spring .*pp*:57-59

[16] World Bank 2010 "*Safer Homes, Stronger Communities: A Handbook for Reconstructing after Natural Disasters*,". Retrieved from www.housingreconstruction.org.

[17] Yu Zhang 2012 '*Perfectly Secret Encryption' HIT*/CST/NIS Cryptography, Spring

The following Figures (pictures) are retrieved from [11] Ojo Matthias O 2013

Figure 1: Two cowry shells tied together with black thread

Fig 1 as an Àrokò, for an Impending bad incidence. Black thing among Yorùbá signifies doom or Mournful incidence.

Figure 2: Four cowry shells strung together back to back

Fig 2 It is an Àrokò which Means "I am breaking my relationship or friendship with you". The back to back position of the cowry shells is an indication that the sender does not what to see the receiver or recipient face to face again.

Figure 3: local traditional comb

Fig 3 If a person sends this to his/her lover as an Àrokò, it means their love, affection and relationship as lovers have ended and no reconciliation can be made **(break up)**

Figure 4: torn piece of palm frond

Fig 4 It is an Àrokò which signifies that the sender is breaking up the blood ties or kinship relationships with the receiver or recipient. This is usually common among the fighting siblings. **(break up)**

Figure 5: cutlass with a fresh palm front tied to it

Fig 5 it is an Aroko which signifies that a war is looming against the recipient community. Cutlass and palm fronts are the symbols attributed to Ogun (the Yoruba god of war and hunting).

Figure 6: handful of sand in a leaf

Fig 6 It is an Aroko which tells the recipient to go on self exile for the offence he/she has committed against the community, ancestors or the gods of the land.

Figure 7: parrot egg in a calabash

Fig 7 It is an Aroko which signifies the rejection of a king or traditional chief. Such a king or traditional chief has been symbolically requested to impose self punishment by committing suicide. A parrot is a sacred bird in Yoruba land.

Figure 8 : Three cowry shells

Three cowry shells(*Fig 8*): It is an Aroko which conveys the message to the recipient that the sender has rejected his/her proposal, offer or request.

Fig 9: plucked feathers of fowl

If *Fig 9* is Deposited at the backyard of a house: as an Aroko, warning an adulterous man in that house to desist from the act, otherwise, the doom will let lose. It is a symbol that the illicit sexual act has been discovered or exposed.

Figure 10: Firebrand

Fig 10 at the back of a house as an Aroko, warning an adulterous man in that house to quit his illicit affair with another man's wife. The meaning of the firebrand is that, if he does not desist, his house will be burnt down.