Computational Cryptography (ÀROKÒ) in Yorùbá Tradition

LONGE I.O
Achievers University
Owo,Ondo State. Nigeria

AKINDIPE, O. T
Obafemi Awolowo University
Ile-Ife,Osun State. Nigeria

BADA, A. A
Adeyemi College of Education
Ondo, Ondo State, Nigeria

ABSTRACT
Communication (verbal and nonverbal) plays a very important role in a society. Nonverbal form of communication involves having knowledge about the signs, behavior and attitude of the sender in which response is also crucial to show that the information is passed. Information is a power tool to any organization or society especially in the preservation of our culture. Hence, there is a need for information security (Cryptography).

Yorùbá's has a peculiar and symbolic way of sending messages (Àrokò). This investigation reveals that Àrokòis a form of symmetric cryptography Algorithms. Mathematical representation is secured and with Computer program (Software) the culture of the Yoruba people can be preserved especially in the area of sending secret messages called Aroko otherwise known as cryptography. The concept is also linked to Computational security.

Keyword
Cryptography (Àrokò), Yorùbá, Communication, Culture, Symmetric and Computational cryptography

1. INTRODUCTION
Communication is a process of sharing of feelings, thoughts and information with another person or group of people; it can either be verbal or non verbal source. Information is received through taste, smell as well as through hearing and sight. Verbal communication is the used of words and non verbal involves signs, body language and facial expression [11]. Communication is important to every society and organization especially in the area of languages (Yoruba dialect, proverbs etc) which are also part of the ways of preserving the culture of an area. Culture according to[18] refers to the totality of people's ways of life which includes a mix of cherish ideas, beliefs, values, attitudes, modes of thought, language (forms of communication) and economic system.

Securing information is understood by most society and organization thereby creating means of communication that will be secured at the level of their knowledge and based on the kind of threat the society have seen based on information linkage maybe doing the time of war or confidential matters. Such forms of old secured messages are cearser cipher (the ancient Rome), and Àrokò. Information security covers a wide array of activities in the society. It includes the processes used to prevent unauthorized access to modify and delete information since some of this information is only meant for a particular person or a group (confidential messages). Before the colonization era and without the knowledge of any forms of cryptography algorithms the Yorùbá's had a symbolic way of communication (Àrokò) which as a level of security and is now growing wane.

1.1 Yorùbá's
The Yorùbá can be found in the south-western part of Nigeria even though they are in other parts of Nigeria. According to [14] Yorùbá land lies between the parallels 5.860 and 9.220 north, and between 2.650 and 5.720 east, with an estimate area of about 181,300sqKm. This area involves the following states: Ekiti, Lagos,Ondo ,Osun,Ogun and Oyo and part of Kwara State in Nigeria. Outside this homeland, their influence has spread beyond the lower Niger northwards into Nupeland, other part of Nigeria and African Countries notably Togo, Northern Ghana and also the eastern part of Republic of Benin known as Dahomey.

Yorùbá people are rich in culture and have different ways of communication (verbal and non verbal). Before the colonization era in Nigeria, the Yorùbá people have been using various signs including parts of human body to communicate to another person far and near. Example of their communication: Yorùbá use eyes (starring) - to attract ,accommodate or repel; nose (wrinkling/upward movement) - to cheapen or mock, head (nodding) - to indicate approval or disapproval, hand (waving) - to call or bid farewell, finger nails (spreading) - to castigate or insult one another, fingers (tapping) – to promise revenge. [1]

The Yorùbá's also uses dressing, drums (gangan), songs and Àrokò to communicate.

2. ÀROKÒ
Definition 2.1
Àrokò is a non verbal symbolic representation of information. [16].

Abdullahi – Idiagbon (2009) opined that Aroko is a non verbal traditional system of communication among the Yorùbá that was in vogue before the advent of the European in Nigeria. 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 materials could be the combination of plants leaves, metals (cutlass or gun), clothes etc.

Àrokò could be classified into six groups; the classification is based on discourse function the message performs:

- Group 1: The Cautionary type of Àrokò. For example, roasted yam sent to someone is to caution against taking a particular action. Again, a cult's insignia to caution a family about burying their cult member in that family without them (the cult) performing their rites.
- Group 2: The Àrokò for punishment. For example if a king sends a covered calabash to the head of a household with the name of a member of that house means the king wants that person beheaded and he

wants the person's head in the calabash he sent as evidence that his order was executed.

- Group 3: Announcement. For example when a hunter sends a monkey skin to a fellow hunter hunting outside the town, it is means that he wants to notify the hunter that his wife has just given birth to a twin. This is because twins are referred to as the offspring of a gallant monkey on tree (eulogy of twin).
- Group 4: Instruction. For example palm fronds tied around a deep ditch is meant to warn passers-by that there is a danger of falling into the pit ahead of them.
- Group 5: Expression of intention. For example sending a king's staff of office to an occasion means that the king can't be present at the occasion but he is expressing his support and love for what they are doing.
- Group 6: A Persuasive Àrokò. For example sending cam wood to someone who once has a quarrel with is meant to tell the person to forgive him or her.

These classifications of Àrokò above cover almost all types of Àrokò in Yoruba-land. Since this study is not based on classification of Àrokò.We will not emphasize more on the groups. Yorùbá's have access to send or receive Aroko and peradventure someone does not have the required knowledge in encrypting or decrypting some forms of Àrokò, there is always someone in the community to help. Àrokò can be sent between friends, families and colleagues of the same or different profession. This paper focuses on some aspect of Àrokò which are confidential. Figure 1 shows the flow of message (Àrokò) in Yorùbá community. Some individual can belong to two or more groups below, like the 'Ogboni cult' most Yoruba traditional leader, Ifa priest, hunter/warriors even normal member of the community could be member of the cult in the community. This paper does not focus on profession or any form of cult but it therefore assumed that some groups named in figure 1 might be subset of other groups.

Àrokò is sometimes sent through someone's child or personal slave to prevent one party from denying sending the message (nonrepudiation). The contents or forms that Àrokò will take depend on the intent of the sender as well as his relationship with the receiver. Yorùbás always choose the right person to deliver the message, even if it means the messenger's death so as to maintain its confidentiality (to stop intruder from understanding the message even if s/he gets intercept the message), integrity(to make sure the receiver unmodified message) and authenticity (to make sure the message received is indeed the message sent).

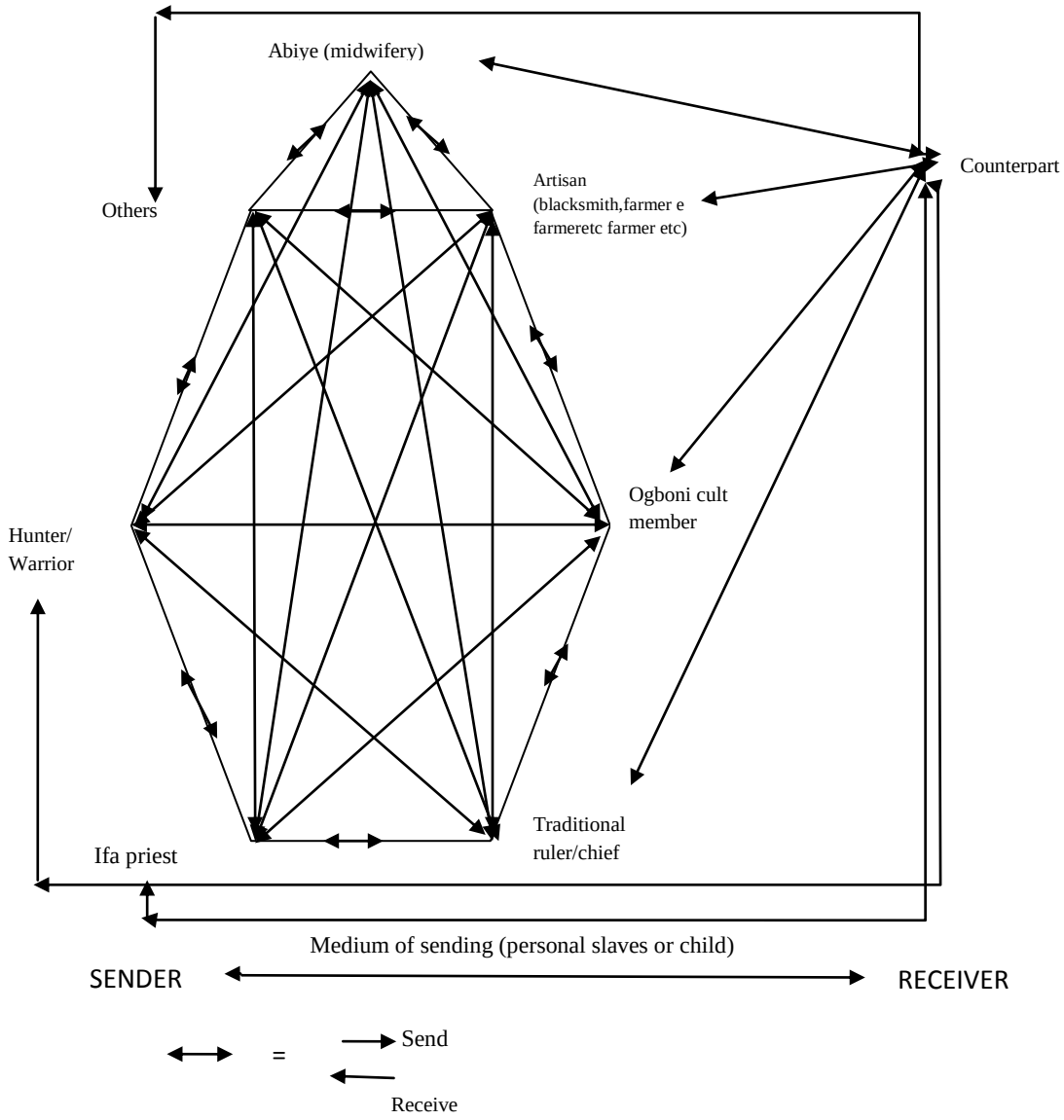

Fig 1 (Àrokò in Yorùbá community)

Àrokò code is almost going into extinction, this is partly because of the following reason explain by [1]

- 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.

These among other reasons (like politic, act of imitating foreign lands way and Religion) have contributed in no small amount to the reduction in the use of these non-verbal signs in Yoruba communities, although the new ways of technology has made encryption and sending messages easy, getting a message along does not have to involve the long process of gathering different items together unlike Àrokò. One of the important of the National Policy on Education according to [18] promotion of the study of Nigerian languages as a means of preserving the people's unity and maintaining peace among the ethnic groups. In other to achieve this, adequate measures need to be put in place so that the cultural heritage of people can be preserved.

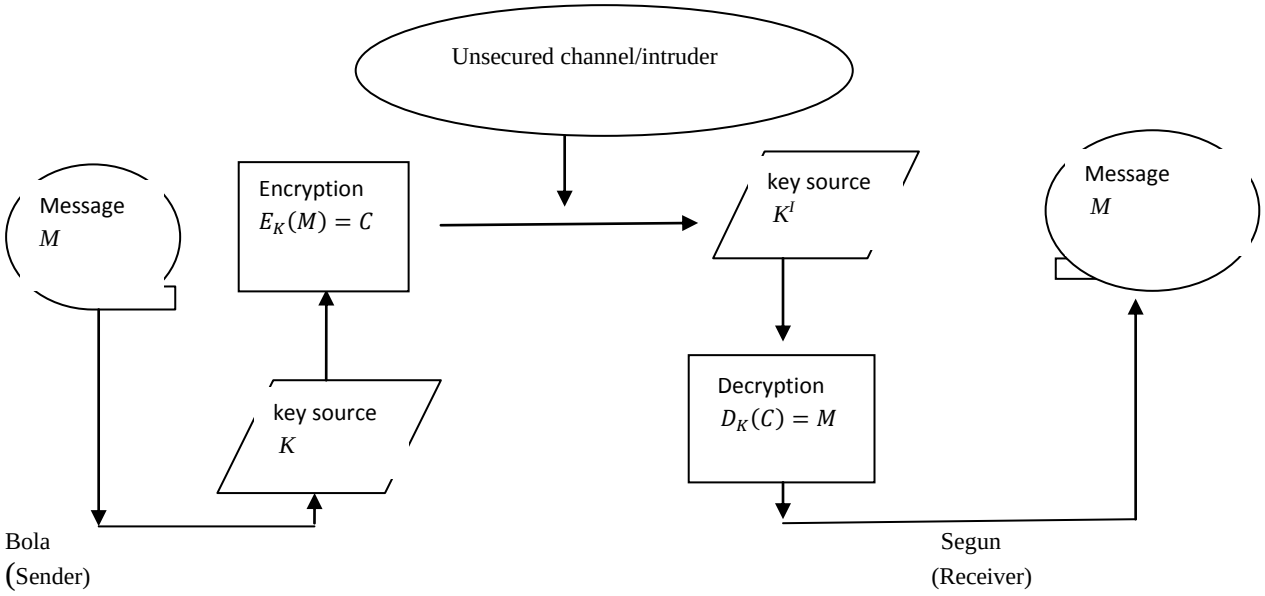

Fig 2 (Àrokò sense of encryption anddecryption)

Culture, inculcating national consciousness and national

In the Figure 2 above key source $K = K^I$ is the in-depth knowledge of the item or materials and in assembly it. Bola needs the knowledge *K* to change the message to a symbolical cipher (*C*) and the form of knowledge *K* is needed by Segun to decrypt the symbolical cipher (*C*) back to the message (*M*).

M =Message, E_K = act of encrypting, D_K= act of decrypting

3. CRYPTOGRAPHY

Definition 3.1:

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.

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

From the definition 2.1 above, the representation ofinformation into symbolic materials or items shows that the message is concealed in the symbolic materials in form of encryption and also needs to be decrypted when received. With definition 2.1 and 3.1 then Aroko cryptography should be defined as

Definition 3.2

"Aroko 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 intension and the original message sent."

Definition 3.3:

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

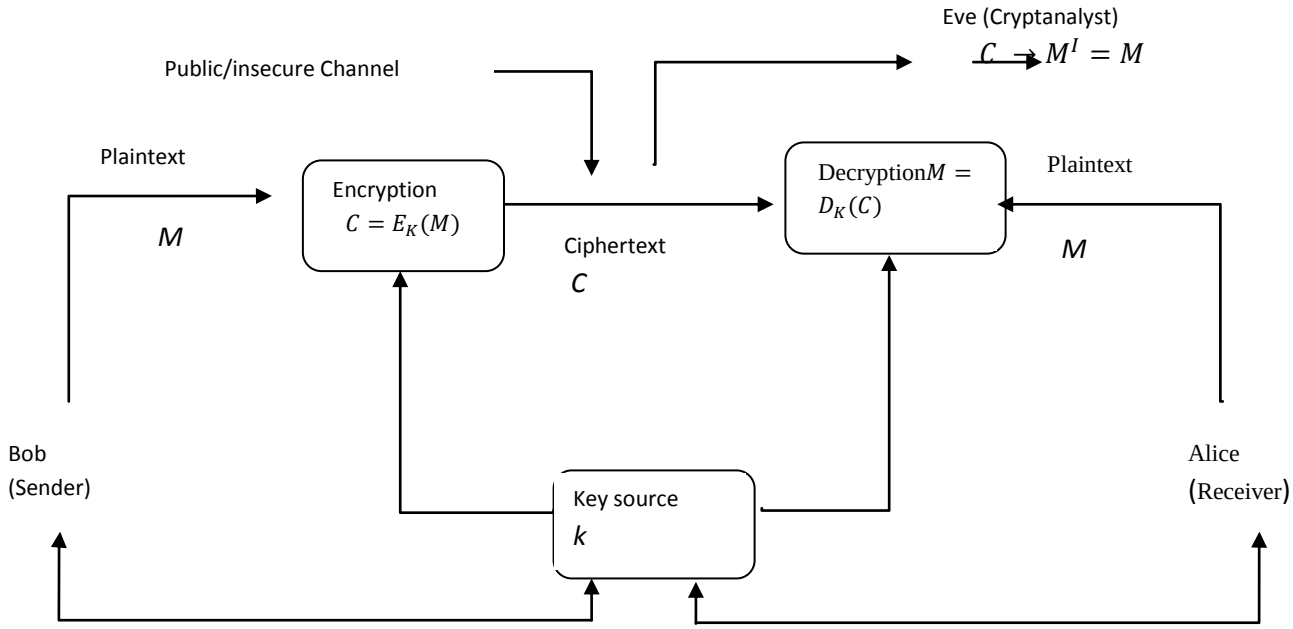

Figure 3: Secret-key Cryptography (See [19])

K is the key for both encryption and decryption

E is the encryption function

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

Where M maps toC, using the keyK, such that

$$C = E_K(M)$$

D is the decryption function

$$D_K : C \rightarrow M$$

Where C maps to M ,using the same keyK 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}

Since a cipher defined over (K,M,C) is a pair of 'efficient' algorithms (E,D) where

$E : K \times M \rightarrow C, \quad D : K \times M \rightarrow M$

s.t for all $m \in M, k \in K, [D(K, E(K, M))] = M$. …{2}

Equation {1} and {2} show that the decryption of an encrypted message gives M (the message).Aroko does not involve mathematical algorithms but only specifics knowledge of material things.

Definition 3.4: symmetric algorithm

A secret key algorithm (sometimes called a symmetric algorithm) is a cryptographic algorithm that uses the same key(K) to encrypt and decrypt data(information) see figure 3. it can also be described as a class of algorithms for cryptography that use the same cryptographic keys(K) for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This kind of algorithm is one of best algorithm in 1970's , the U.S. Department of Defense's Data Encryption Standard (DES), which was developed at IBM in 1977, was thought to be so difficult to break that the U.S. government restricted its exportation at that time.

A very simple example of how a secret key algorithm works might be substituting the letter in the alphabet prior to the target letter for each one in a message. The resulting text - "rcrgt," for example - would make no sense to someone who didn't know the algorithm used

$K = (X + 2)$ where 'x' is the normal alphabet, but would be easily understood by the parties involved in the exchange as "paper." Symmetric algorithms have the advantage of not consuming too much computing power.A few well-known examples are: DES, Triple-DES (3DES), IDEA.

Encrypting a message does not guarantee that this message is not changed while encrypted. Hence, often a message authentication code is added to a cipher-text to ensure that changes to the cipher-text will be noted by the receiver (in as much to keep this message authentication code the Yorubas always send the most loyal and trusted slave or son to deliver their message). The use of secret key has the same concept with Àrokò, the knowledge of the key (K) in Aroko might be the historical or behavioral trait of those object involved or it may be a secret between the sender and the receiver and It must be known by the owner or individual(sender or receiver) or the social group he/shebelongs to (e.g. ogboni cult)) so as to decrypt the Àrokò message.

4. COMPUTATIONAL CRYPTOSYSTEM

According to Song (2008) 'A cryptosystem 'S' is computationally or polynomially secure if a cryptanalyst cannot decrypt 'C' to get M in a polynomial – time (or space). The Mathematical Algorithm in [19], Cook-Karp thesis and other forms of Mathematical Algorithm, non is really relevant in encrypting and decrypting Àrokò symbolic cryptosystem, and if cryptosystem S in computationally unbreakable ,if it is unbreakable in polynomial-time that is ,it is computationally

secure. According to the Cook – Karp thesis stated in [19] says thatany problem that cannot be solved in polynomial-time is computationally infeasible, thus if the cryptanalytic attack on acryptosystem is computationally infeasible, then the cryptosystem is computationally secure and computationally unbreakable'. He also forged ahead in defining 'Practical / Conjectured secure as A cryptosystem 'S' is practical secure if the breaking of the system S is conjectured as difficult as solving a well known and supposedly difficult mathematical problems such as the integer factorization problem IFP or thediscrete logarithm problem DLP .Example: most of the public-key and secret-key cryptosystem." since Àrokò iscombinations of material things like plants, metals etc which are not computationally infeasible, then is computationally secured. For further knowledge on IFP, DLP and Secret key see [19].

5. SECRET KEY AND ÀROKÒ

Àrokò involves the knowledge of almost all plant and some material things, which makes it difficult to use in encrypt or decrypt without the requirement knowledge (K). Àrokò encryption and decryption involve knowing the message, the relationship between the sender and the receiver and the in-depth knowledge (secret key) of the materials in the Àrokò.example : a family sent another family a full or half keg of palm wine (if full , it will be along side with white cloth stain with blood), this means the state the groom meant his bride either virgin or not(in-depth knowledge (K)) but literal meaning implies the grooms family just sent wine for enjoyment . It is also involves two form of knowledge's (literal and in-depth knowledge) but the literal knowledge is not the secret key. It is just a way of decoy (form of a security- to deceive intruders etc) so as to allow the person with the secret key to decrypt it. Figure 2 and Figure 3 shows different forms of similarities' (both have a need for secret key in encrypting and decrypting) which makes Àrokò to be linked to the form of symmetric cryptography (use of secret key). In sending Àrokò there is a web of three people involved: they are the sender, receiver and the medium.

The sender: It is observed that the sender must have an in-depth knowledge of the right materials to use in preparing the Àrokò so as not to mislead or give room for misunderstanding between him and the receiver.

The receiver: the receiver must be vast in the knowledge of the material sent to him since it is the key involved to decrypt/decode the message. If the receiver has difficulty in interpreting the message, he can give it to an elderly person or someone with the knowledge of Àrokò to help with its interpretation but this will affect the confidentiality of the message.

The medium (the conveyer of the message): is the most important part of the process. Also, The medium must be sensible and trustworthy in other to ensure a proper delivery of the message. If he chose to not deliver the message the way it has been encrypted the meaning of the message will be lost. Hence, the medium must make ensure that the message is delivered accurately and accordingly. Is the responsibility of the bearer of the message to protect these messages thereby keeping the integrity, confidentiality and access control .Most bearer are always known with the sender whereby confirming the authenticity and non-repudiation of the message.

In sending Àrokò these three must work in harmony to avoid any form of misrepresentation or misinterpretation of the message and to protect it secrecy.

Examples

If eight cowrie shells are sent to someone, it means such an individual is free from danger, if two cowrie shells are tied back to back and sent, it means 'I shun you', if another cowrie is added to the other two and sent in return, it means 'I don't want to have anything to do with you', but if a piece of coal is sent in return, it means, 'I fail to comprehend the cause of your shunning me' and in ages, cowrie shells were legal tender used to buy and sell goods . see [14] .

Therefore there is a knowledge (K) needed in numbers of cowries sent.

Aroko also shows two forms of meanings: To a novice – the bearer is just paying the receiver {literal meaning} while the real meanings of the Àrokò are stated above. Also with these, the integrity of the bearer is put to test. Sometimes Yorùbás believe that it is a bad omen to give gifts or send messages with objects in odd numbers.

Also in example stated above 'in Group 1', the roasted yam could also serve as food, but that is not the meaning of the Àrokò.

6. CONCLUSION

Àrokò is a very interesting way of sending message among Yorùbá people which involves a comprehensive knowledge (K) of plant, animal and human part and any other material (used in preparing it), since the key (K) of encrypting and decrypting lies the in knowledge of materials involved, it involved two forms of knowledge (the literal knowledge and the in-depth knowledge of the materials) ,without the knowledge of any form of algorithm before the colonial era Arokowas created and has aconcept ofsymmetric algorithm (use secret key) and it proved computationally secured since it is not computationally feasible, although Aroko is not as secured and generally known in the world but it's a cultural heritage with needs to be preserved and taught ,so people can gain from Yoruba ways of life .

7. RECOMMENDATION

The following recommendations were considered appropriately.

1. The rich culture and tradition of the people can be preserved by using the Àrokò system to educate people of the Yorùbá in-depth meaning of the items in Aroko.
2. A computer program based on the 'Àrokò' could be developed in encoding and decoding information so as to preserved and applied Àrokò in the modern age.

8. REFERENCES

[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] Adeoye, C. L. 2005. Asa ati Ise Yorùbá. Ibadan. *University Press PLC*

[3] Ajibade, G. O. 2006. Hearthstones: Religion, Ethics and Medicine in the Healing Process in the Traditional Yorùbá Society. Nicolini, B. (ed). Studies in Witchcraft, Magic, War and Peace in Africa: Nineteenth and Twentieth Centuries

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

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

[6] Davidson, B. 1981. A History of West African 1000 – 1800: Longman U.K.

[7] Eco, U 1979. A Theory of Semiotics. Bloomington: Indiana University Press

[8] Eco, U 1984. Semiotics and the Philosophy of Language. London: Macmillan

[9] Erebinulu, S. O. 1966. Kokoro Isiro Owo, Ibadan: African University Press.

[10] Fadipe, N. A. 1970. Sociology of the Yorùbá. Ibadan University Press.

[11] Goffman, E. 1981. Forms of Talk. Basil Blackwell: Oxford.

[12] Grice, H. P. 1975. "Logic and Conversation" (in) Cole and J. Morgan (eds) Semiotic and Semantics, Vol. 3 Speech Acts, New York: Academic Press

[13] Johnson, S. 1921. History of the Yorùbás.YEAR CMS Bookshop Press.

[14] 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

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

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

[17] Opefeyitmi, A. 1997. Tíọ́rì àti Ìṣọwọ́lo-èdè. Osogbo: Tanimehin-ola Press.

[18] Oyekan, O. O. 2000. Foundations of Teacher Education, Ibadan. Ben Quality Prints Ibadan.

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