Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 2, May 2015

Swarm Intelligence a Technique Using DES Algorithm

Ms.Archana S S[1], Mr.Harish H K[2]
M.Tech (CNE) Student, Dept. of Computer Science Engg. Akshaya Institute of Technology, Tumkur. India[1]
Asst.prof, Dept. of Computer Science Engg. Akshaya Institute of Technology, Tumkur. India[2]

***Abstract* — Swarm Intelligence (SI) is an Artificial Intelligence technique involving the study of collective behavior in decentralized systems. Such systems are made up by a population of simple individuals interacting locally with one another and with their environment. Although there is typically no centralized control dictating the behavior of the individuals, local interactions among the individuals often cause a global pattern to emerge. Examples of systems like this can be found abundant in nature. Including ant colonies, bird flocking, animal herding, honey bees, bacteria, and many more. SI refers to the problem-solving behavior that emerges from the interaction between individuals of such systems, and computational swarm intelligence refers to algorithmic models of such behaviors. In this Paper mainly we have proposed brief idea about swarm intelligence, data encryption and cryptography.**

Keywords — Cryptography; Cipher text, Optimization

I. INTRODUCTION

Swarm intelligence is the obedience that deals with natural and artificial systems collected of many individuals which coordinate using decentralized control and self-organization. In particular, the discipline focuses on the collective behaviors that result from the local interactions of the individuals with each other and with their environment. Examples of systems studied by swarm intelligence are colonies of ants and termites, schools of fish, flocks of birds, herds of land animals. Some human artifacts also fall into the domain of swarm intelligence, notably some multi-robot systems, and also certain computer programs that are written to tackle optimization and data analysis problems.

Swarm intelligence has a marked multidisciplinary character since systems with the above mentioned characteristics can be observed in a variety of domains. Research in swarm intelligence can be classified according to different criteria.

A. Natural vs. Artificial*:* - It is customary to divide swarm intelligence research into two areas according to the nature of the systems under analysis. We speak therefore of natural swarm intelligence research, where biological systems are studied; and of artificial swarm intelligence, where human artifacts are studied.

B. Scientific vs. Engineering: - An alternative and somehow more informative classification of swarm intelligence research can be given based on the goals that are pursued: we can identify a scientific and an engineering stream. The goal of the scientific stream is to model swarm intelligence systems and to single out and understand the mechanisms that allow a system as a whole to behave in a coordinated way as a result of local individual-individual and individual-environment interactions. On the other hand, the goal of the engineering stream is to exploit the understanding developed by the scientific stream in order to design systems that are able to solve problems of practical relevance.

The Data Encryption Standard (DES) is an outdated symmetric-key method of data encryption. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. Once the go-to, symmetric-key algorithm for the encryption of electronic data, DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm. Originally designed by researchers at IBM in the early 1970s, DES was adopted by the U.S. government as an official Federal Information Processing Standard (FIPS) in 1977 for the encryption of commercial and sensitive yet unclassified government computer data. It was the first encryption algorithm approved by the U.S. government for public disclosure. This ensured that DES was quickly adopted by industries such as financial services, where the need for strong encryption is high. The simplicity of DES also saw it used in a wide variety of embedded systems, smart cards, SIM cards and network devices requiring encryption like modems, set-top boxes and routers.

Cryptography is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.

Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". People who study and develop cryptography are called cryptographers. The study of how to circumvent the use of cryptography for unintended recipients is called cryptanalysis, or code breaking. Cryptography and cryptanalysis are sometimes grouped together under the umbrella term cryptology, encompassing the entire subject. In practice, "cryptography" is also often used to refer to the field as a whole, especially as an applied science.

II.TECHNIQUES OF CRYPTOGRAPHY

There are two techniques used for data encryption and decryption, which are:

1. Symmetric Cryptography*:* - If sender and recipient use the same key then it is known as symmetrical or private key cryptography. It is always suitable for long data streams. Such system is difficult to use in practice because the sender and receiver must know the key. It also requires sending the keys over a secure channel from sender to recipient. There are two methods that are used in symmetric key cryptography: block and stream.

The block method divides a large data set into blocks (based on predefined size or the key size), encrypts each block separately and finally combines blocks to produce encrypted data.

The stream method encrypts the data as a stream of bits without separating the data into blocks. The stream of bits from the data is encrypted sequentially using some of the results from the previous bit until all the bits in the data are encrypted as a whole.

2. Asymmetric Cryptography*:*-If sender and recipient use different keys then it is known as asymmetrical or public key cryptography. The key used for encryption is called the public key and the key used for decryption is called the private key. Such technique is used for short data streams and also requires more time to encrypt the data. Asymmetric encryption techniques are almost 1000 times lower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key; symmetric encryption is then used to transfer data between sender and receiver.

III.COMMON GOALS IN CRYPTOGRAPHY

In spirit, cryptography concerns four main goals. They are:

1. Message Confidentiality*:* - Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information.
2. Message Integrity*:* - The recipient should be able to determine if the message has been altered.
3. Sender Authentication*:* - The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled (or combinations) so to validate claims from emitter or to validated the recipient expectations.
4. Sender Non-Repudiation*:*- The emitter should not be able to deny sending the message.

1V.DATA ENCRYPTION STANDARD KEY LENGTH AND BRUTE-FORCE ATTACKS

The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit cipher text by means of permutation and substitution. The process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. For any cipher, the most basic method of attack is brute force, which involves trying each key until you find the right one. The length of the key determines the number of possible keys -- and hence the feasibility -- of this type of attack. DES uses a 64-bit key, but eight of those bits are used for parity checks, effectively limiting the key to 56-bits. Hence, it would take a maximum of 2^56, or 72,057,594,037,927,936, attempts to find the correct key.

Even though few messages encrypted using DES encryption are likely to be subjected to this kind of code-breaking effort, many security experts felt the 56-bit key length was inadequate even before DES was adopted as a standard. (There have always been suspicions that interference from the NSA weakened IBM's original algorithm). Even so, DES remained a trusted and widely used encryption algorithm through the mid-1990s. However, in 1998, a computer built by the Electronic Frontier Foundation (EFF) decrypted a DES-encoded message in 56 hours. By harnessing the power of thousands of networked computers, the following year EFF cut the decryption time to 22 hours.

Apart from providing backwards compatibility in some instances, reliance today upon DES for data confidentiality is

a serious security design error in any computer system and should be avoided. There are much more secure algorithms available, such as AES. Much like a cheap suitcase lock, DES will keep the contents safe from honest people, but it won't stop a determined thief.

V.ADVANTAGE & DISADVANTAGE SWARM INTELLIGENCE

Advantages:

1. Flexible*:* The colony respond to internal disturbances and external challenges.

2. Robust*:* Tasks are completed even if some agents fail.

3. Scalable: From a few agents to millions

4. Decentralized: There is no central control in the colony.

5. Self-organized*:* The solutions are emergent rather than pre-defined.

6. Adaptation: The swarm system can not only adjust to predetermined stimuli but also to new stimuli.

7. Speed: Changes in the network can be propagated very fast.

8.Modularity: Agents act independently of other network layers.

9.Parallelism: Agents' operations are inherently parallel.

Disadvantages

1.Behaviour: Difficult to predict the behaviour from the individual rules.

2.Knowledge: The functions of colony could not be understood with the knowledge of functioning of a agent.

3.Sensitivity: Even a small change in the simple rules results in different group level behavior

.4.Action: Agent behavior looks like noise as action of choice is stochastic.

VI. PRINCIPLES OF GENERAL SWARM

1. Proximity principle: The basic units of a swarm should be capable of giving the respond back to environmental variance triggered by interactions among agents. However, some fundamental behaviors are shared such as living-resource searching and nest-building.

2.Quality principle: A swarm should be able to respond to quality factors such as determining the safety of a location.

3.Principle of diverse response: Resources should not be concentrated in a narrow region. The distribution should be designed so that each agent will be maximally protected facing environmental fluctuations.

4.Principle of stability: The population should not change its mode of behavior every time the environment changes.

5.Principle of adaptability: The swarm is sensitive to the changes in the environment that result in different swarm behaviour.

VII.STUDY AND APPLICATION OF SWARM INTELLIGENCE

This section briefly presents a few examples of scientific and engineering swarm intelligence studies.

A.Clustering Behavior of Ants*:*- Ants build cemeteries by collecting dead bodies into a single place in the nest. They also organize the spatial disposition of larvae into clusters with the younger, smaller larvae in the cluster center and the older ones at its periphery. This clustering behavior has motivated a number of scientific studies. Scientists have built simple probabilistic models of these behaviors and have tested them in simulation (Bonabeau et al. 1999). The basic models state that an unloaded ant has a probability to pick up a corpse or a larva that is inversely proportional to their locally perceived density, while the probability that a loaded ant has to drop the carried item is proportional to the local density of similar items. This model has been validated against experimental data obtained with real ants. In the taxonomy this is an example of natural/scientific swarm intelligence system.

B.Nest Building Behavior of Wasps and Termites:- Wasps build nests with a highly complex internal structure that is well beyond the cognitive capabilities of a single wasp. Termites build nests whose dimensions (they can reach many meters of diameter and height) are enormous when compared to a single individual, which can measure as little as a few millimeters. Scientists have been studying the coordination mechanisms that allow the construction of these structures and have proposed probabilistic models exploiting stigmergic communication to explain the insects' behavior. Some of these models have been implemented in computer programs and used to produce simulated structures that recall the morphology of the real nests (Bonabeau et al. 1999). In the taxonomy this is an example of natural/scientific swarm intelligence system.

C.Flocking and Schooling in Birds and Fish:- Flocking and schooling are examples of highly coordinated group behaviors exhibited by large groups of birds and fish. Scientists have shown that these elegant swarm-level behaviors can be understood as the result of a self-organized process where no leader is in charge and each individual bases its movement decisions solely on locally available information: the distance, perceived speed, and direction of movement of neighbours. These studies have inspired a number of computer simulations (of which Reynolds' Boids simulation program was the first one) that are now used in the computer graphics industry for the realistic reproduction of

flocking in movies and computer games. In the taxonomy these are examples respectively of natural/scientific and artificial/engineering swarm intelligence systems.

D.Ant Colony Optimization:- Ant colony optimization (Dorigo, Maniezzo and Colorni 1991; Dorigo and Stützle 2004) is a population-based metaheuristic that can be used to find approximate solutions to difficult optimization problems. It is inspired by the above-described foraging behavior of ant colonies. In ant colony optimization (ACO), a set of software agents called "artificial ants" search for good solutions to a given optimization problem transformed into the problem of finding the minimum cost path on a weighted graph. The artificial ants incrementally build solutions by moving on the graph. The solution construction process is stochastic and is biased by a pheromone model, that is, a set of parameters associated with graph components (either nodes or edges) the values of which are modified at runtime by the ants. ACO has been applied successfully to many classical combinatorial optimization problems, as well as to discrete optimization problems that have stochastic and/or dynamic components. Examples are the application to routing in communication networks and to stochastic version of well-known combinatorial optimization problem, such as the probabilistic traveling salesman problem. Moreover, ACO has been extended so that it can be used to solve continuous and mixed-variable optimization problems (Socha and Dorigo in press). Ant colony optimization is probably the most successful example of artificial/engineering swarm intelligence system with numerous applications to real-world problems.

E.Particle Swarm Optimization:- Particle swarm optimization (Kennedy and Eberhart 1995; Kennedy, Eberhart and Shi, 2001) is a population based stochastic optimization technique for the solution of continuous optimization problems. It is inspired by social behaviors in flocks of birds and schools of fish. In particle swarm optimization (PSO), a set of software agents called particles search for good solutions to a given continuous optimization problem. Each particle is a solution of the considered problem and uses its own experience and the experience of neighbor particles to choose how to move in the search space. In practice, in the initialization phase each particle is given a random initial position and an initial velocity. The position of the particle represents a solution of the problem and has therefore a value, given by the objective function. While moving in the search space, particles memorize the position of the best solution they found. At each iteration of the algorithm, each particle moves with a velocity that is a weighted sum of three components: the old velocity, a velocity component that drives the particle towards the location in the search space where it previously found the best solution so far, and a velocity component that drives the particle towards the location in the search space where the neighbor particles found the best solution so far. PSO has been applied to many different problems and is another example of successful artificial/engineering swarm intelligence system.

F.Swarm-based Network Management:- The first swarm-based approaches to network management were proposed in 1996 by Schoonderwoerd et al., and in 1998 by Di Caro and Dorigo. Schoonderwoerd et al. proposed Ant-based Control (ABC), an algorithm for routing and load balancing in circuit-switched networks; Di Caro and Dorigo proposed AntNet, an algorithm for routing in packet-switched networks. While ABC was a proof-of-concept, AntNet, which is an ACO algorithm, was compared to many state-of-the-art algorithms and its performance was found to be competitive especially in situation of highly dynamic and stochastic data traffic as can be observed in Internet-like networks. An extension of AntNet has been successfully applied to ad-hoc networks (Di Caro, Ducatelle and Gambardella 2005). These algorithms are another example of successful artificial/engineering swarm intelligence system.

G.Cooperative Behavior in Swarms of Robots:- There are a number of swarm behaviors observed in natural systems that have inspired innovative ways of solving problems by using swarms of robots. This is what is called swarm robotics. In other words, swarm robotics is the application of swarm intelligence principles to the control of swarms of robots. As with swarm intelligence systems in general, swarm robotics systems can have either a scientific or an engineering flavour. Clustering in a swarm of robots was mentioned above as an example of artificial/scientific system. An example of artificial/engineering swarm intelligence system is the collective transport of an item too heavy for a single robot, a behavior also often observed in ant colonies.

VIII.INTRODUCTION ABOUT DATA ENCRYPTION STANDARD (DES)

As mentioned earlier there are two main types of cryptography in use today – symmetric or secret key cryptography and asymmetric or public key cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's1. Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption (hence the use of the term symmetric). Figure 1 depicts this idea. It is

necessary for security purposes that the secret key never be revealed.

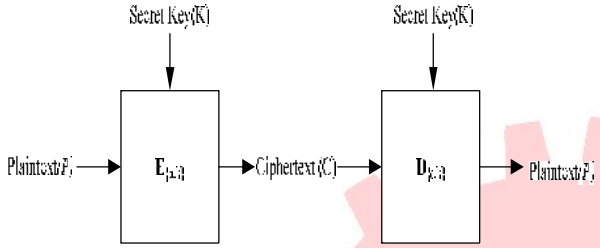

Figure.1: Secret Key Encryption

To accomplish encryption, most secret key algorithms use two main techniques known as substitution and permutation. Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called rounds. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible without the secret key. This is achieved with the use of S-boxes which are basically non-linear substitution tables where either the output is smaller than the input or vice versa.

IX.PRIOR STUDIES WORK

Selcuk [1] presented an analytical calculation of the success probability of linear and differential cryptanalytic attacks. The results apply to an extended sense of the term \success" where the correct key is found not necessarily as the highest-ranking candidate but within a set of high-ranking candidates. Experimental results show that the analysis provides accurate results in most cases, especially in linear cryptanalysis. In cases where the results are less accurate, as in certain cases of differential cryptanalysis, the results are useful to provide approximate estimates of the success probability and the necessary plaintext requirement. The analysis also reveals that the attacked key length in differential cryptanalysis is one of the factors that affect the success probability directly besides the signal to noise ratio and the available plaintext amount.

Rinza et al. [2] decrypted the information using probability leads to a more thorough job, because you have to know the percent- age of each of the letters of the language that is being analyzed here is Spanish. You can consider not only the probabilities of the letters also syllables, set of three, four letters and even words. Then you have this thing to do is make comparisons of the frequencies of cipher text and the frequencies of the language to begin to replace by a correspondence.

Laskari et al. [3] applied the particle swarm optimization method, which originates from the field of evolutionary computation, to address an interesting problem introduced by the cryptanalysis of block-cipher cryptosystems. The results on the data encryption standard reduced to four rounds indicate that this is a promising approach.

MSVS et al. [4] presented an attempt is made to analyze the text based crypto model using frequency distribution of character code points as a parameter with specific study on Indic scripts. The encryption and decryption process is tested in comparison with English and also on Telugu with different key sizes. Evaluation of the model is carried out with the help of frequency distribution as one of the prominent characteristic of text. Crypto analysis is carried out on both the languages with 8-bit key and the percentage of matches in the reverse transformation is presented. The mapping for English text ranges from 23 % to 50 % where as for Telugu it ranges from 10% to 20%. The analysis is extended to 16-bit key size on Telugu text. The mapping for 16-bit is observed in the range of 1% to 10%. If the text complexities are considered for each script, greater levels of security are observed with smaller key sizes. Evaluation of the proposed model on other Indic scripts of the same nature is in progress. The proposed cryptographic model is implemented now by considering 16-bit key on Telugu using the above mentioned approach. Mapping is carried out between the characters of plain text and cipher text based on these frequencies.The results indicate that the percentage of retrieved plain text is varying between 10- 20% whereas for 16-bit key the observed results are found in the range 1-10% only. This is an

Wiener et al. [5] have used to find the full cost of several cryptanalytic attacks. In many cases this full cost is higher than the accepted complexity of a given algorithm based on the number of processor steps. The full costs of several cryptanalytic attacks are determined, including Shanks' method for computing discrete logarithms in cyclic groups of prime order n, which requires n1/2+o(1) processor steps, but when all factors are taken into account, has full cost n2/3+o(1). Other attacks analyzed are factoring with the number field sieve, generic attacks on block ciphers, attacks on double and triple encryption, and finding hash collisions. In many cases parallel collision search gives a significant asymptotic advantage over well-known generic attacks.

Vimalathithan and Valarmathi [6] have presented an algorithm for the cryptanalysis of Simplified Data Encryption Standard is presented. The time complexity of the proposed approach has been reduced drastically when compared to the Brute-Force attack. Though SDES is a simple encryption

algorithm, this is a promising method and can be adopted to handle other complex block ciphers like DES and AES. The cost function used here can be applied for other block ciphers also. The future works are extending this approach for attacking DES and AES ciphers.

Khan et al. [7] presented a novel swarm based attack called Ant-Crypto (Ant- Cryptographer) for the cryptanalysis of Data Encryption Standard (DES). Ant-Crypto is based on Binary Ant Colony Optimization (BACO) i.e. a binary search space based directed graph is modeled for efficiently searching the optimum result (an original encryption key, in their case). The reason that why evolutionary techniques are becoming attractive is because of the inapplicability of traditional techniques and brute force attacks against feistel ciphers due to their inherent structure based on high nonlinearity and low autocorrelation. Ant-Crypto uses a known-plaintext attack to recover the secret key of DES which is required to break/ decipher the secret messages. Ant-Crypto iteratively searches for the secret key while generating several candidate optimum keys that are guessed across different runs on the basis of routes completed by ants. These optimum keys are then used to find each individual bit of the 56 bit secret key used during encryption by DES. Ant-Crypto is compared with some other state of the art evolutionary based attacks i.e. Genetic Algorithm and Comprehensive Binary Particle Swarm Optimization. The experimental results show that Ant-Crypto is an effective evolutionary attack against DES and can deduce large number of valuable bits as compared to other evolutionary algorithms; both in terms of time and space complexity.

X.CONCLUSION

The Data Encryption Standard was once a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. In this Paper we have illustarted about cryptography , Data Encryption standard and as well as we have presented about swarm intelligence.

REFERENCES

[1] Selçuk, Ali Aydın. "On probability of success in linear and differential cryptanalysis." Journal of Cryptology 21, no. 1, pp.131-147, 2008

[2] Rinza, B., Fernando Zacarias Flores, Luna Pérez Mauricio, and M. C. Antonio. "Decryption through the likelihood of frequency of letters." Benemerita Universidad Autonoma de Puebla.

[3] Laskari, E. C., G. C. Meletiou, Y. C. Stamatiou, and M. N. Vrahatis. "Evolutionary computation based cryptanalysis: A first study." Nonlinear Analysis: Theory, Methods & Applications 63, no. 5 (2005): e823-e830.

[4] Bhadri Raju MSVS1, Vishnu Vardhan B2, Naidu G A3, Pratap Reddy L4, and Vinaya Babu, “Effect of Language Complexity on Deciphering Substitution Ciphers - A Case Study on Telugu” , International Journal of Security and Its Applications Vol. 4, No. 1, January, 2010

[5] Wiener, Michael J. "The full cost of cryptanalytic attacks." Journal of Cryptology 17, no. 2 (2004): 105-124.

[6] Vimalathithan.R1, Dr.M.L.Valarmathi, “Cryptanalysis of S-DES using Genetic Algorithm”, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009

[7] Salabat Khan, Armughan Ali and Mehr Yahya Durrani, “Ant-Crypto, a Cryptographer for Data Encryption Standard”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013

BIOGRAPHY

Archana S S, presently pursuing M.Tech in Computer Network and Engineering, Akshaya Institute of Technology, Tumkur. Affiliated to VTU, Belguam, India.
Email:archana91ss@gmail.com.

Mr.Harish H.K, M.Tech in Computer Science and Engineering. Presently working as Assistant Professor, Dept. of Computer Science and Engineering, Akshaya Institute of Technology, Tumkur. Affiliated to VTU, Belguam, India.
Email:harishhk0909@gmail.com.