Information Security Management -CSE3502

Analyzing And Implementing Latest Encryption Techniques

J Component Project

MAURYA GOYAL 19BCI0192
SHIVAM BANSAL 19BCE0930
SAUMITRA PATHAK 19BCE2411

B. Tech. Computer Science and Engineering

School of Computer Science and Engineering

Vellore Institute of Technology

Vellore

April, 2022

ABSTRACT :

1. Motivation and aim:

Cryptic Encryption techniques are advancing on a daily basis, and the new approaches give much improved security and are nearly hard to penetrate. This inspired us to learn more about these strategies, weigh their benefits and drawbacks, and provide a well-researched study and assessment of these procedures.

2. Methodology :

DNA encryption and Honey encryption are two of the most recent approaches that we will examine in order to provide a comprehensive analysis. We would evaluate these approaches with available techniques.

3. Expected Outcome:

Delivery of a research-based overview of the differences as well as instances in which these techniques solve the issues encountered by existing established encryption techniques such as RSA, DES, and so on.

INTRODUCTION:

1. Overall idea about the project:

- ✓ Through this project we are analyzing and implementing the unpopular latest encryption techniques like honey encryption and DNA encryption. We compare these techniques with the latest techniques in their respective domains and explain their advantages and why they should be used.
- ✓ As the threat of cyber security attacks grows, it is critical for internet users to understand, at the very least, the fundamental encryption strategy in order to protect your security. It is one of the most powerful ways to keep our data safe.

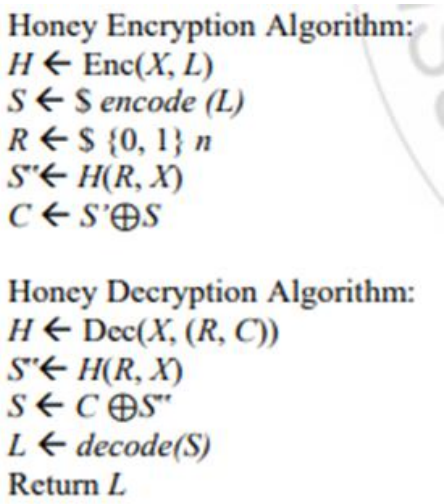
- ✓ For honey encryption we have analyzed how using it with encrypted passwords can increase the security of a system exponentially. For password protection we already use hashing and salting, but they can be cracked simply using brute force attacks. Using honey encryption or basically the art of deception, we store multiple passwords which are similar to the password, and only one of them is correct, which the system knows through honey generators. This concept is based on an intrusion resilience system where even after the compromise or partial compromise of the security of the system, we maintain security. Now of the mentioned passwords only one is correct, and if the value entered matches one of the honey words and not the passwords, the concerned authorities would be alerted and can take the specific action.

- ✓ Using DNA Encryption we have encrypted and decrypted images and the encrypted image is totally unrecognizable which maintains the encryption and can be decrypted to obtain back the original image.

2. Background of the project:

HONEY ENCRYPTION:

Honey encryption is a type of data encryption that produces a ciphertext, which, when decrypted with an incorrect key as guessed by the attacker, presents a plausible-looking yet incorrect plaintext password or encryption key. It is simply based on the principle of decoy which makes it look real. It is based on an intrusion resilience system, which means that it is secure even after a partial-compromise of security. The DTE (Distributed Transforming Encoding) is the main idea behind pure honey encryption technique. Honey encryption manages the space of plaintext via DTE. Let the probability distribution over the message space be p over the message L. The distribution encodes the message L as a K-bit seed $S \in \{0, 1\}K$ and decodes the message by the inverse DTE method; decode (S) =L. DTE is a good model of the message distribution. The internal structure of the HE includes DTE encryption and DTE decryption. The two algorithms describe the net functioning of Honey Encryption:



BASE PAPER: Click here

DNA ENCRYPTION:

DNA cryptography is a promising new data security technique that combines the principles of modern biotechnology and cryptology. It may bring forward a new hope for unbreakable algorithms. To encrypt using DNA, the sender generates a DNA encoding table, and the receiver generates another table through the same encoding technique and sends a clue to the sender to be able to generate it locally. The plaintext to be encoded is divided into two halves equally. If the plaintext is not even, we insert random padding. One half of the plaintext is converted into a DNA sequence using a sender-based table, and the other half of the plaintext is converted into a DNA sequence using a receiver-based table. DNA cryptography is a bio-inspired novel technique used for securing end-to-end communication, where DNA is used as an information carrier.

BASE PAPER: Click here

3. Statistics related to the methods used:

In July 2012, more than 450,000 e-mail addresses and passwords were stolen from Yahoo. Yahoo used the standard hashing and salt techniques to keep the password safe and clearly it was broken. From the analysis performed on the passwords breached, studies found out that password breach using brute force has no protection and what makes it even easier is the fact that nearly 1% of the people have the same passwords. 50% of the passwords can be cracked in less than 4mn tries, which isn't a lot considering the speed of the computer. Nowadays, most people use password vaults to keep their passwords safe, but these vaults also have a password which can be broken down easily. Using honey encryption, even if the password breach has occurred, the probability of the hacker guessing the password is 1/n where n is the total number of passwords stored using honey encryption. Since data breaches occur in clusters, this probability decreases even further exponentially if the breach is bigger and amounts to (1/n)^k where k is the number of passwords leaked.

4. Advantages and disadvantages of the various methods:

HONEY ENCRYPTION:

Advantages:

1. Protects against highly vulnerable brute force attacks.
2. Is an intrusion resilience system based on deception.
3. The probability of a big data breach increases exponentially.
4. In case of breach alerts are raised to the concerned authorities to take appropriate actions.

Disadvantages:

1. Increases the additional cost of storing the extra passwords.
2. In the worst case scenario, it has the same security as a system without honey encryption.

DNA ENCRYPTION:

Advantages:

1. DNA is extremely tiny in size. Nanoscale storage is simple to achieve.
2. Parallel on a large scale, encryption and decryption can both be accelerated.
3. To create a new password system that can withstand quantum assaults, use biological issues as the security foundation for DNA passwords.
4. DNA encryption does not involve much real time functioning, but they can control data encryption, secure data storage, identity verification, digital signatures, and information concealment.
5. Since DNA micro-points are difficult to locate, even if the ciphertext is captured, sequencing the unknown DNA combination is difficult. As a result, the Message Sequence Number is difficult to obtain, maintaining security.

Disadvantages:

1. *There is no theoretical justification.* As a result, nearly no acceptable DNA programme exists.
2. *Costliness*, restricting the usage of DNA passwords in practical operation.

3. DNA encryption flaws include the fact that it cannot be used independently, and it also has a proportional influence on the accuracy and decipherability of DNA passwords.
4. Only physical transit is possible for the carrier and primer in the DNA password.
5. A substantial amount of human power and reaction processes are required, limiting the feasibility of big-scale DNA encryption implementations.

LITERATURE SURVEY:

SNo.	Paper	Methodology	Result	Limitation
1.	**Data Security Techniques Based on DNA Encryption.** **Mousomi Roy, Shouvik Chakraborty, Kalyani Mali, Raja Swarnakar, Kushankur Ghosh, Arghasree Banerjee and Sankhadeep Chatterjee**	This Encryption mechanism follows this step by converting a plain text into its equivalent ASCII code and then converted into binary code then it is mapped to DNA sequence and the index number is stored. This array of integers is the ciphertext, and it is decrypted by the receiver with the help of key and index pointer.	Here, DNA encryption and its many methodologies are reviewed based on DNA encryption. This study has the potential to be extremely useful for future DNA encryption research. DNA encryption makes use of a variety of biological processes and concepts. Traditional cryptography approaches are effectively utilized with many biological ideas and methodologies such as DNA replacement, central dogma, PCR amplification, and DNA synthesis.	Several issues, like environmental effects and quantum assaults, remain important obstacles that must be solved.
2.	**A robust and lossless DNA encryption scheme for color images.** **Xiangjun Wu, Jürgen Kurths, Haibin Kan**	The plain image is first divided into three grey-level components, which are then converted into three DNA matrices at random using DNA encoding principles. The XOR procedure is then done twice on the DNA matrices. The scrambled DNA matrices are then converted into three grayscale pictures using DNA decoding principles. Finally, a diffusion process is used to modify the picture pixel values using a keystream, resulting in the cipher-image. The plain image is connected to the keystream created by OCML.	The experimental findings and security analysis show that the suggested method has a decent encryption effect and can survive a variety of common assaults. Furthermore, it is resistant to several popular picture editing procedures including noise addition, cropping, JPEG compression, and so on.	Some disadvantages include small key space and weak security. Some attacks such as chosen-ciphertext attack, known-plaintext attack, chosen-plaintext attack, were recommended to break the chaos-based cryptosystems. So it is essential to improve the image encryption techniques for strengthening the security.

3.	**A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme.** **Vijay Choudhary, Tushar Mandge**	Utilization of the MATLAB language to develop this encryption approach, which is a matrix-based language that is well suited to the proposed mechanism. Matlab also has a bio-informatics toolbox and biological computing tools. We encrypted the plaintext "SECRET MESSAGE" with the first key, "AX085769*12." Using the key generation algorithm, the initial key creates a new key. The advantage of this key generation technique is that given the same plaintext and key, we always receive fresh cipher data.	It provides a solid security layer that conceals plaintext. Hybrid security can be obtained by integrating DNA cryptography with conventional encryption. We get mini-cipher after applying matrix manipulations. This mini-cipher is processed further by applying DNA encryption nucleotide sequence and applying amino acid conversion final cipher text is occurred. We also recovered original message successfully in decryption process.	Computer background people face difficulties of understanding of biological terms; also, the rate of developing security by using biological operations is very low.It is still taking its initial steps, so there is a lot of scope to work in this area of cryptography and need more works and researches to reach the realization and to enhance the technical issues.
4.	**An Encryption Scheme Using DNA Technology.** **Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang**	An encryption scheme via using the technologies of DNA synthesis, PCR amplification, and DNA digital coding & idea of traditional cryptography. The intended PCR two primer pairs were used as the key to this scheme that was now not independently designed by way of sender or receiver, but respectively designed by way of the whole cooperation of sender and receiver. Traditional encryption techniques and DNA digital coding are used to preprocess the plaintext.	By this preprocess operation we can get absolutely one-of-a-kind ciphertext from the same plaintext, which could efficiently prevent the assault from possible words as PCR primers.	It is possible that this biological difficult problem may be broken with the development of biological technology after many years or adversary has caught the correct primer sequences from two parties. The proposed encryption scheme is still far away being a perfect scheme.
5.	**Index-Based Symmetric DNA Encryption Algorithm.** **Richard O.Sinnott, Wang Zhong, Zhu Yu, Zhang Yunpeng**	The algorithm encodes each character into ASCII codes. And then, according to the nucleotide sequence, the researcher should convert it to the DNA coding. Then select the special DNA sequence as the encryption index, and likewise, the pretreated plaintext will be divided into different groups. Next, the key created by the Chaos Key Generator based on the Logistic Mapping and initialized by the number x0 and μ will take XOR operation with the block-plaintext. The type of number x0 and μ, is selected , is double.	Result of these processes are translated into the DNA sequence. Compared to a special DNA sequence, the algorithm finds the sequence which has no difference from it. Then, the algorithm will store the position as the Cipher-text. Validity is proven through simulation and theoretical analysis, including biosecurity and math security.It has been proved that the algorithm has achieved the computing-security level in the encryption security estimating system.	A theoretical proof of DNA cryptosystem's validity to make it be provable security level, and perfection of the algorithm's security model is required. Need to make full use of DNA computing & biological characteristics to eliminate the disadvantages of block cipher mode.

6.	**Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations.** **Diyar Qader Zeebaree, Subhi R. M. Zeebaree, Habibollah Haron, Dilovan Asaad Zebari**	To provide a better security and reliable data transmission, an efficient method of DNA based on cryptography technique is introduced and implemented by the following sequence of operations. The proposed technique works on block cipher with a key of 2 bytes, which is composed of three levels. The secret data not only going through different levels but also several DNA operations are used to provide enhanced security layer. A new technique based on DNA is proposed and a new key generation procedure which followed by 4 x 4 matrix manipulation is used. Furthermore, generate a new DNA reference based on real DNA reference from NCBI, random DNA reference based on BBSG, arithmetic and biological operations also provide an injective mapping to produce a cipher data.	Experimental results showed that the proposed approach meets security requirements and can resist exhaustive attacks very effectively. Security analysis and robustness showed that the probability guessing attackers to retrieve the original plaintext is near to zero, this means it provides a very high security. The proposed scheme has good randomness which is considered as a most important measure of the security techniques. Depending on the p-value results, the success of the proposed scheme has been proved where high p-value considered as a big indicator.	The key generation can be improved in order to provide more security. Using arithmetic and biological operations in security separately have several disadvantages. Feasibility is a disadvantage of biological operations, which increased the cost of encryption because of the feasibility in proper laboratory only. Due to depending arithmetic operations on the key totally; key dependency and key transmission between sender and receiver are considered as disadvantages of arithmetic operations.
7.	**An encryption algorithm inspired from DNA.** **Habiba Drias, Souhila Sadeg, Mohamed Gougache, Nabil Mansouri**	The algorithm contains a DNA module that uses principles of the central dogma of molecular biology that are transcription and translation. In the transcription process, a genetic code table called amino acids is used, while the inversed Amino acids table is used in the decryption method. In all the steps of the algorithm, substitutions and permutations were performed to concretize the diffusion and confusion principles and, consequently, enforce the security of the method.	The results show that there is no great difference between the run times with key of 128 bits and those with key of 256 bits because the key-generator generates in both cases, sub-keys of 128 bits. Other results illustrate that the run time grows with the number of rounds in the iteration phase, it goes without saying that the security of the algorithm grows with the number of rounds. On comparison of run times of this algorithm with those of the AES OpenSSL (Secure Socket Layer)provided with FEDORA distribution of the Linux operating system and the results showed that the AES OpenSSL is faster. The results showed that shortest run times were obtained with our algorithm.	The current main difficulties of DNA cryptography are the absence of theoretical basis, the high tech lab requirements and computation limitations. More effort and study is required to achieve realization and conquer non-theoretical problems.

8.	**Image Encryption Using DNA Complementary Rule And Chaotic Maps** **Hongjun Liua, Xingyuan Wanga, Abdurahman Kadir**	This methodology utilized the MD5 hash to verify that the chaotic maps' starting conditions vary with the plain picture. Following the diffusion of the original image's rows and columns by arrays created by the PWLCM technology, each pixel is encoded into four nucleotides through DNA coding. The complementary rule of DNA is then used to convert each nucleotide into its base pair for random time(s), resulting in the pseudo-random sequence created by Chebyshev chaotic maps.	The findings of the experiment demonstrate that using more than one chaotic map might result in a bigger key space. The results revealed that the PWLCM map outperformed the Logistic map. Experiment findings and security analysis demonstrate that the scheme can not only produce strong encryption results and a huge key space, but also withstand typical assaults.	Because this research is still in its early phases, there is a lot of space for advancement in the field of cryptography and DNA Encryption, and more effort and study is required to achieve realization and overcome technical problems.
9.	**Honey Encryption: Security Beyond the Brute-Force Bound** **Ari Juels and Thomas Ristenpart**	HE schemes has syntax and semantics equivalent to that of a symmetric encryption scheme. Decryption recovers messages from ciphertexts. Instead of giving rise to some error, decryption will emit a plaintext that looks plausible. Provides uses of HE for Credit Card Numbers, PINs, CVVs , RSA Secret keys.	Low-entropy secrets such as passwords are likely to persist in computer systems for many years. Honey encryption can offer valuable additional protection in such scenarios. HE also offers a gracefully degrading hedge against partial disclosure of high min-entropy keys, and, by simultaneously meeting standard PBE security notions should keys be high entropy, HE never provides worse security than existing PBE schemes.	For the case where plaintexts consist of passwords, e.g., password vaults, the relationship between password-cracking and DTE construction deserves further exploration. HE security does not hold when the adversary has side information about the target messages.
10.	**Secure pin authentication in java smart card using honey encryption.** **Sadeq mohammed, Sefer KURNAZ, Alaa Hamid Mohammed**	honey encryption base scheme in order to countermeasure the brute force attacks aimed at guessing the user's password without having to face the risk of DoS attacks which results from limiting the maximum number of tries. Honey encryption is the concept of presenting the attacker with fake yet believable data that resemble the sensitive hidden data in the smart card but does not indicate the type of information that is hidden. instead of blocking the attacker from re-entering the incorrect PIN after the random number of PIN tries is maxed out.	instead of using prestored fake data, we propose a Deep learning approach such as the generative adversial network GAN to generate data from the sensitive data stored in the memory that resemble the nature of the stored data but does not indicate any information related to it. honey card resisted the attacks and was able to stop the brute-force attack without allowing any of the modifications inflicted to the other cards.	Generator function not so clearly explained and can be improved in many ways.

11.	**A Novel Approach for the Adaptation of Honey Encryption to Support Natural Language Message** **Abiodun Esther Omolara, Aman Jantan, Oludare Isaac Abiodun and Howard Eldon Poston**	The proposed system is divided into the encoding and decoding process. Messages are encoded and sent by the sender and at the other end, they are decrypted by the receiver. Using Standford Dependency Parser, each sentence in the message is parsed into a tree of Noun, Verb, Adjective, Adverb or Modifier Phrase for encoding. y objective of this research is to design an algorithm that generates fake but valid-looking message from the original message encoded so as to deceive the attacker. We are concerned with how human language is generated. Therefore, we opted for tools that work with human language.	The proposed method conceals the content and structure of the true message. Also, it secures the length of the original message. The messages scales, they produce real-looking decoy. Also, an attacker cannot distinguish the fake message from the original plaintext. There is no way the adversary can tell the original message from the fake message even if he acquires the original message.	Results of the experiment are not well described. The method doesn't provide any significant improvement for the high entropy values. decoys/fake messages for natural language messages. It produces reasonable length decoy messages capable of fooling the adversary.
12.	**Review on Honey Encryption Technique** **Nahri Syeda Noorunnisa, Dr. Khan Rahat Afreen**	Although the passwords are considered secure, but if enough computations are done then the passwords are vulnerable to brute-force attacks. The DTE is the main idea behind pure honey encryption technique.	The distribution transforming encodes the message L as a K bit seed S∈{0, 1}K and decodes the message by inverse DTE method, decode (S) =L. DTE is a good model of the message distribution. The internal structure of the HE includes DTE encryption and DTE decryption .The two algorithms describes the net functioning of the Honey Encryption.	The model only discusses about the uses in respect to passwords and doesn't explain well about the generator function.
13.	**Password Typos Resilience in Honey Encryption** **Hoyul Choi, Hyunjae Nam, Junbeom Hur**	n this paper, we propose two kinds of schemes for the password typos problem for different system and threat models. A-Type scheme is designed for a conventional client-server model. Even it is the simplest and most efficient among the schemes, it has a drawback in terms of false positive rate. B-Type scheme is designed for an extended system model with additional database manager. It solves the accuracy problem of A-Type. In addition to password, it provides high accuracy of detecting typos by exploiting additional side-information e.g., personal identification number .	Honey encryption is a novel encryption scheme that provides security beyond the brute-force bound. However, it has a typos problem that the typos in password may confuse a legitimate user, since decryption under a wrong key produces fake but valid-looking messages. For this reason, typos problem in HE is more critical than in other password-based schemes. Recent studies showed that typos in password occur very frequently, thus the solutions that deal with the typos problem should be proposed. In this paper, we introduced two different schemes: A-Type and B-Type They have different system models, threat models and constructions. We analyzed the typos detecting accuracy and security for each scheme.	The A-type has several limitations which are solved by the B-type. But protects only from brute-force attack and hence is not a good technique by itself nut along with hashing it can solve majority password problems.

14.	**Modified honey encryption scheme for encoding natural language message** **Abiodun Esther Omolara, Aman Jantan**	Our approach leverages the power of deception to persuade and confuse the attacker that he has the original message. The decoy message will have a completely different message structure from the original message but will have a semantic and contextual meaning. Each message to be encoded is treated as a string of sentence and processed as a grammatical feature in the English Language. In the English Language, the main parts of speech are noun, pronoun, verb, adverb, adj ective, preposition, interjection, conjunction and determiner.	able to create a structure where messages are encoded in binary such that message recovery becomes impossible for an adversary that intercepts a ciphertext and tries to decrypt it using random keys. Our proposed approach is the first successful implementation of adapting the honey encryption scheme for supporting encoding of human-generated message. It produces a plausible message that is good enough to deceive the adversary. More importantly, the critical message that the sender might want to protect is completely concealed and cannot appear during decryption with incorrect keys, thereby, countering the CCA.	critical message (keywords) that the sender might want to protect is completely concealed and cannot appear during decryption with incorrect keys, thereby, countering the CCA. However, the approach impacts time when the message gets larger.
15.	**Honey Encryption for Language** **Marc Beunardeau, Houda Ferradi, R´emi G´eraud(B) , and David Naccache**	This is an encryption paradigm designed to produce ciphertexts yielding plausible-looking but bogus plaintexts upon decryption with wrong keys. Thus brute-force attackers need to use additional information to determine whether they indeed found the correct key.In this paper we give arguments why the approach of Chatterjee et al. does not extends, and give an alternative approach based on a corpus quotation distribution transforming encoding.	Scanning reveals one potential application of rule 1 (namely “his early youth”), two potential applications of rule 2 (“a skilled architect” and “the approximate age”) and one potential application of rule 2 (“by a linguist and by a skilled architect”). Hence 4 bits suffice to identify and remove the outgrowths.	HE security is threatened when A has some side information about the target message. This puts strong constraints on HE’s applicability to situations such as protecting RSA or HTTPS private keys. A second limitation is that the HE construction assumes that the key and message distributions are independent. When these distributions are correlated, A can identify a correct message by comparing that message with the decryption key that produced it.

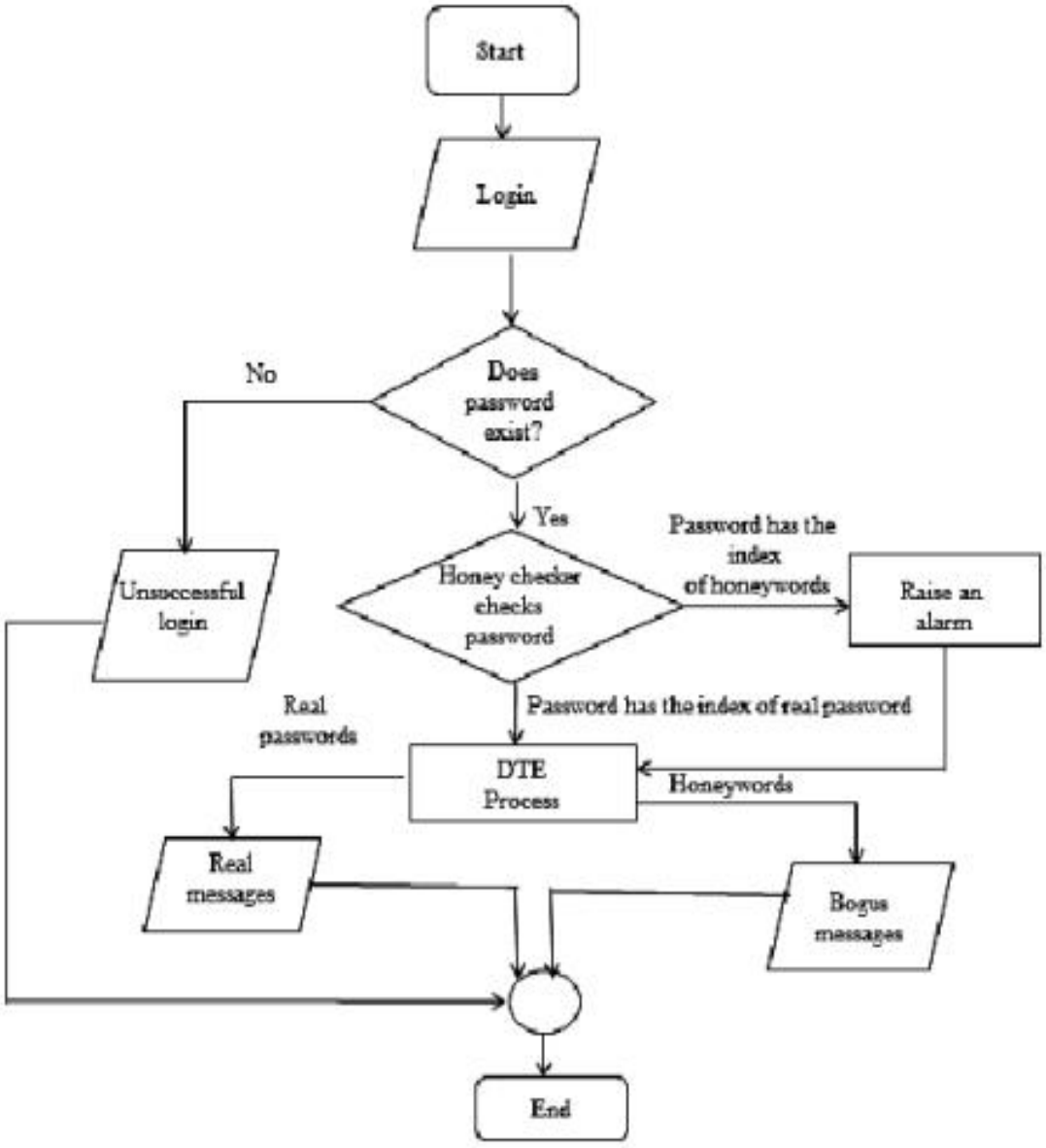
16.	**Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps.** **Jian Zhang, DongXin Fang, and Honge Ren**	For image encryption, the authors suggest an unique confusion/diffusion technique. To confuse the picture pixels, they first exchanged the pixel locations of the digital image's rows and columns as per a chaotic approach focusing on the logistic chaotic map. Following a series of repeated computations based on Chebyshev's chaotic map, they encoded each of the confused pixels into four nucleotides and generated a one-dimensional nucleotide sequence. Then, using the complementary rule, we turned each nucleotide into its matching base pair a random number of times. Finally, they turn the resultant two-dimensional matrix into an encrypted photograph.	This work effectively integrates chaotic encryption technology with DNA coding techniques in a manner that has been validated by a significant number of trials and security evaluations to demonstrate the algorithm's security and logic. The experimental findings and security analysis reveal that the system not only achieves strong encryption results, but also has a sufficiently large key space to reject typical assaults. As a result, the system is trustworthy enough to be used in image encryption.	The authors state that they have no competing interests in the publication of this research.
17.	**A Novel Audio Cryptosystem Using Chaotic Maps and DNA Encoding.** **S. J. Sheela, K. V. Suresh, and Deepaknath Tandur**	It is suggested to develop a new voice encryption technique based on chaotic maps and DNA encoding. The method employs chaotic maps such as 2D-MHM and SM, as well as HCST. When compared to the seed map, the modified Henon map has a large chaotic range over a wide range of system characteristics. Furthermore, DNA encoding technology is included to improve the security of the cryptosystem. The cryptosystem's performance is assessed and compared to that of current algorithms.	Analytical and simulation results demonstrate that the proposed technique can encrypt many types of voice signals with a high level of security and withstand a variety of assaults. When compared to the previous approach, the new algorithm provides more security. Furthermore, the method can handle many forms of noise while maintaining a high SNR. As a result, the suggested approach is applicable to real-time voice encryption technologies, secured telephone communication, and narrow spectrum radio communication.	The attacker can simply access the chaotic map's initial states and/or system settings. Furthermore, one-dimensional chaotic maps have a limited key space and poor security. Furthermore, it has been demonstrated that encryption systems based only on chaos are less safe, necessitating the adoption of other mechanisms to improve the security of the cryptosystem.
18.	**Research on Image Encryption Based on DNA Sequence and Chaos Theory.** **Tian Tian Zhang, J. Phys.**	The algorithm proposed in this study combines DNA and Logistic chaotic mapping. The research initially demonstrates how to include the genuine DNA chain into the image before introducing logistic chaotic mapping, which is utilized for image encryption. Then, to encrypt the grayscale image, a novel approach is given that combines the logistic method with the DNA sequence. On the basis of logistic chaotic mapping and DNA sequence, a random matrix is constructed, and addition and complement operations are conducted on it.	This method overcomes irreversible issues and broadens the key space. It can withstand certain plaintext assaults, brute force attacks, and statistical attacks.	In the worst-case scenario, the attacker can immediately obtain the key for decryption. We examine a specific plaintext assault known as the differential attack. The difference analysis entails comparing ciphertext pairs and plaintext with some features. We know that if an image encryption method is to be secure, it must be both exquisite and sensible. In this section, the algorithm is subjected to a slew of assaults in order to assess its security.

19.	**Protecting Private Data using Improved Honey Encryption and Honeywords Generation Algorithm.** **Thanda Win , Khin Su Myat Moe**	The honeywords generating process might confuse attackers by keeping the true password alongside the bogus passwords or honeywords in password files. However, if a large number of people utilise this programme, the honeywords generation process can address the storage cost issue. If the attackers utilise honeywords, the honey encryption technique can guard against brute force attacks by creating honey messages.	Our suggested honeywords generation technique and honey encryption algorithm can tackle the storage overhead and message encryption problems. The issue of limited space. Furthermore, we presented a novel hashing algorithm. method for safeguarding our system and increasing speed processing time as compared to the current MD5 hashing system. Our proposed solution overcomes the shortcomings of Honey encryption and honeywords generating algorithms that are currently in use.	The present honey encryption scheme has a message space constraint and can only deliver four messages at a time using the probability distribution function.
20.	**A Review on Multiple Chaotic Maps for Image Encryption with Cryptographic Technique.** **Govind Chandra, Naveen Chandra, Swati Verma**	Many key encryption approaches have been discussed and evaluated in order to become acquainted with the various encryption algorithms utilised in picture encryption that has been transmitted over the network. The simulation results reveal that each method has benefits and drawbacks dependent on the approaches used to process photos.	Following a careful examination of all of the above-mentioned research studies, the following recommendations may be made: A Chaos-based algorithm should be used to safeguard multimedia assets. To give great speed and security to the system, a more complicated and compressed algorithm should be implemented. To raise the security level, modified versions of several algorithms are utilised. To achieve considerable security, we can use current picture encryption techniques, but only a few existing image encryption approaches meet this need.	The security analysis parameter revealed that present picture encryption solutions are resistant to various assaults such as statistical attacks, key sensitivity analysis attacks, and so on.

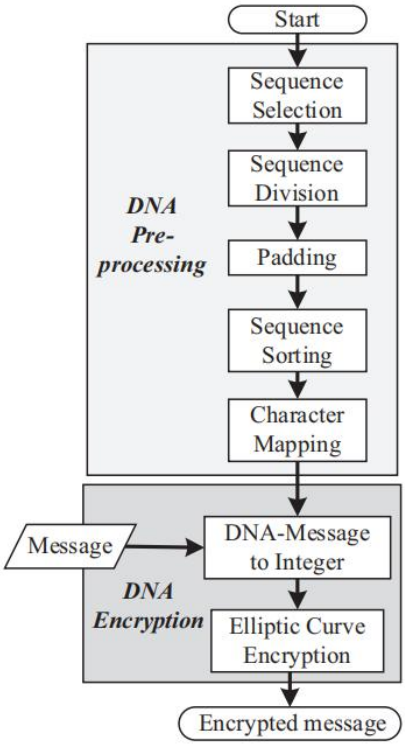
OVERALL ARCHITECTURE:

1. The overall architecture (diagrammatic representation):

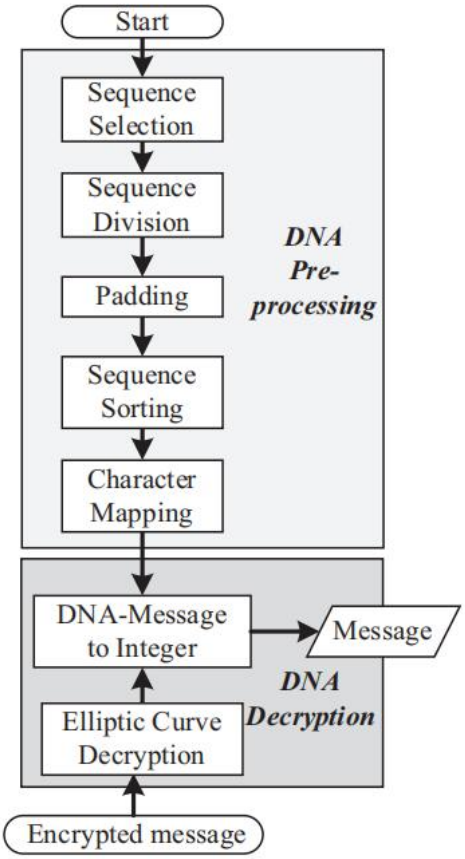
HONEY ENCRYPTION:



DNA-based encryption:



DNA-based decryption:



2. The flow of the architecture in detail:

HONEY ENCRYPTION:

In honey encryption as illustrated in the process flow diagram above it is used for password protection. For the login, whenever the user tries to enter the password for the particular username, 3 cases might occur:

1. The username and password match: The user gets logged in successfully.
2. The password entered is wrong:
   2.1 The password entered is not one of the honey words: The user would be asked to try login again and invalid authentication would be generated.
   2.2 The password entered is one of the honey words: alerts to the associated authorities will be issued and they can take the appropriate actions.

The strength of honey encryption depends on how much the honey words are indistinguishable from the real password, and the better the password generator, the better the security.

DNA ENCRYPTION:

The DNA encryption and decryption depicted in the above flowcharts are representation of how the process flows in order to successfully encrypt an image and also to decrypt the same image. Here is the step-wise description of the flowchart:

1) Step 1: Sequence Selection: The sender begins by selecting a DNA stream from a recognized organism from the worldwide database.
2) Step 2: Sequence Division: The sequencing is then subdivided into S size categories.
3) Step 3: Padding: If the last element post-division contains less components than the beginning, the beginning is padded onto the end.
4) Step 4: Sequence Sorting: The sequence is then divided into non-repeated subgroups. To do this, each subset must first be transformed into integer numbers. A, C, G, and T are denoted by the numbers 00, 01, 10, and 11, respectively.
5) Step 5: Character Mapping: Each character in cryptology is expressed by a DNAseq equivalent. Its binary equivalent is utilized for execution. Then, using a DNAseq stream, each set of MESSAGE strings is translated to an equivalent "DNAmess."
6) Step 6: Converting the DNA-Message to an Integer for Encryption: The bitstream is then separated into n bits. These n-bits are then expressed as integers and ECC is used to encrypt them.
7) Step 7: Decryption to DNA-Message: ECC decryption is used to decrypt the collected information.
8) Step 8: From message to message: the receiver will choose the same DNA sequence and use the sorting algorithm. The message bits are separated into DNA subsets of S and translated to integer equivalents.
9) Step 9: Converting the DNA-Message to an Integer for Encryption: The bitstream is then separated into n-bits. These n-bits are then converted to integers and encrypted with the ECC.
10) Step 10: Decryption to DNA-Message: ECC decryption is used to decrypt the data received.
11) Step 11: From message to message: the receiver will choose the same DNA sequence and use the sorting algorithm. The message bits are separated into DNA subsets of S and translated to integer equivalents. These integer variables will be used to remap the characters and build the decrypted message string using the "DNApos" array.

PROPOSED METHODOLOGY:

HONEY ENCRYPTION

1. Detailed explanation of the methods used in the diagrammatic representation:

We use the methods of seeds which are nothing but a numerical value that simply points to the secret message. So in honey encryption using the password, we are pointing to a secret message. We use a simple XOR algorithm for encryption but since all the inputs are strings only, we need to convert the strings to numericals and then do the same for both the secret message and the password, and with the help of a predefined dictionary of Indian states, we assign values to the rest of the passwords.

For encryption we use the simple formula of XOR :
ENCRYPTION: sk $\oplus$ sm
Where sk → seed for the key
Sm → seed for the message
DECRYPTION: sk $\oplus$ cipher
Where sk → seed for the key
cipher→ encrypted message only

2. Advantages and disadvantages of the methods used:
ADVANTAGES:

- ✓ This method depicts the workings of honey encryption quite well.
- ✓ The encryption and decryption techniques of honey encryption are implemented correctly and perform as expected.
- ✓ Gives the best user experience and makes it easier to understand how the honey encryption works.

DISADVANTAGES:

- ✓ Using NLP to make a proper generator function for the passwords can make the bogus passwords look even more deceivable as in our case the system doesn't recognize if the password has some hidden date or number representing something that corresponds to the user.

3. Justification on why you have chosen this particular method:
We chose this method as it was easier to implement and makes it really easy for the user to understand the concepts illustrated based on honey encryption. This method works moderately with the passwords generated and most of the time it is impossible to find the correct passwords from the ones generated. It also shows how difficult it is for an adversary to guess multiple passwords at a time. Therefore, depicting the use cases of honey encryption quite well and the best scenarios to use honey encryption.

DNA ENCRYPTION

1. Detailed explanation of the methods used in the diagrammatic representation:

General Elipical Curve Cryptography(ECC) scheme:

Process	Description
Domain parameter generation	Elliptic curve domain parameters over F_p are defined by the sextuple $T = (p, A, B, G_E, N_G, h)$
Key generation	Private key: V = Random number (1 to N_G) Public key: $\beta = V \cdot G_E$
Message representation on elliptic curve Point	Message as number, m such that $mr < p$ Representing X-coordinate, $x_j = m \cdot r + j$ such that $j \in [0, \omega - 1]$ Calculate $s_j = x^3_j + Ax_j + B$, such that $s_j^{(p-1)/2} = 1 (\text{mod}\, p)$ y_i = Quadratic residual of s_j Message will be represented as $P_M = (x_j, y_j)$
Encryption	Transmitter uses the public key, β Select k = Random number (1 to $N_G - 1$) Calculate $P_1 = k \cdot G_E$ and $P_2 = P_M + k_\beta$ Encrypted text $P_C = (P_1, P_2)$
Decryption	Calculate $M_1 = V \cdot P_1$, using receiver's private key V Calculate $P_M = P_2 - M_1$ Message, m, is represented by P_M
Representation of elliptic curve point into message	Calculate $m = ceil(x_j/r)$ Converting m back to message

In general, three DNA cryptography techniques are being used:

a) Insertion technique.
b) Substitution method
c) The complementary pair method.

A similar method of encoding and decoding is employed in all of the following systems. The plaintext is transformed to binary integers. These binary integers are then translated to an analogous DNA nucleotide sequence.

Now, one of the DNA-cryptographic techniques is employed for encryption or decryption. For DNA the encoding and decoding procedures are based on the following four fundamental units that are binary encoded as:

- ✓ Adenine (A): 00,
- ✓ Thymine (T): 01,
- ✓ Guanine (G): 10,
- ✓ Cytosine (C): 11.

A DNA sequence is derived from a publically accessible sequence. As previously explained, convert the DNA sequence into binary. Divide the binary DNA sequence into segments, with each segment containing a randomly chosen number of bits larger than 2.

2. Advantages and disadvantages of the methods used:

Advantages:

- ✓ Even though this approach needs more memory, it has been demonstrated to be quicker than traditional methods.
- ✓ Thee same procedure may be used to decrypt the message.
- ✓ The proposed DNA mapping enhances the resilience of elliptical cryptography-based applications against unwanted assaults greatly.

- ✓ The proposed technique has a lot of promise for future of IoT devices that require a compact but effective security mechanism.
- ✓ Fewer power and processing time than that of other systems, faster than other ways.

Disadvantages:

- ✓ The brute-force method is a very time-consuming method.
- ✓ This approach needs additional memory.
- ✓ DNA strands investigate increased danger in the intentional destruction of biological equipment and the development of hazardous biological products.

3. Justification on why you have chosen this particular method:

We have chosen this method as it has plenty of advantages and its easy to implement for any person with little of the encryption and decryption. It helps in encryption of any image that is private/secretive for the user, this technique generates an unbreakable DNA-sequence. Its flexibility for decryption which allows the user to use the same method in reversed order to get the real image is also very exceptional.
The envisioned scheme's energy usage is comparable to that of existing systems without DNA mapping and remapping. As a result, the suggested DNA mapping and remapping method increases the strength of existing elliptical cryptosystems while consuming little energy and time. The suggested system has a high potential for usage in mobile and cloud-based applications due to its low energy consumption and confirmed implementation in an IoT context.

RESULTS:

HONEY ENCRYPTION:

1. Results obtained:

```
Please enter a password: ism
Please enter a secret message to store (one word): vitvellore
Your password is ism, your seed value is 16, and your secret message is vitvellore
====================================
['ISM185', 'ism173', 'ism15', 'ISM', 'ism', 'ism141']
Enter a password to crack: ism15
Intruder! SOUNDING ALARM!
'Bihar'
Would you like to enter another inquiry (Y/N):  y
Please enter a password: ism
Please enter a secret message to store (one word): vit
Your password is ism, your seed value is 24, and your secret message is vit
====================================
['ISM', 'ism23', 'ISM265', 'ism221', 'ism', 'ism253']
Enter a password to crack: ism
'vit'
Would you like to enter another inquiry (Y/N):  n

Thank you for testing Honey Encryption
```

2. *Interpretation of the obtained results.*

Here we have implemented all the three possible cases available:

- ✓ For the first image we entered the password 'ism'. Then we give it the value to store 'vitvellore' and when we have to guess out of all the given passwords we give the correct value which allows the user to login and returns back the value vitvellore.
- ✓ For this case again we have the same password and the same value but this time when we have to enter the password, we enter one of the honey words generated which raises an intrusion alert and returns the invalid message.
- ✓ For this case again if we enter the same password with the same value and this time enter a password which matches none of the honey words; in this case the authorization simply fails.

DNA ENCRYPTION:

1. *Results obtained:*

Image 1:

Uploading the image and saving an encrypted image, then decrypting the same image.

```
Image loaded!
D:/Sem 5/Information Security Analysis and Audit/Project/Encryption-Techniques-main/Images/us.jpg
pixels: 409600  width: 640 height: 640
saved ecrypted image as enc.jpg
decrypting...
Image Decrypted and saved as Recovered.jpg
```

Image 2:

Uploaded image as us.jpeg. This is our base image.

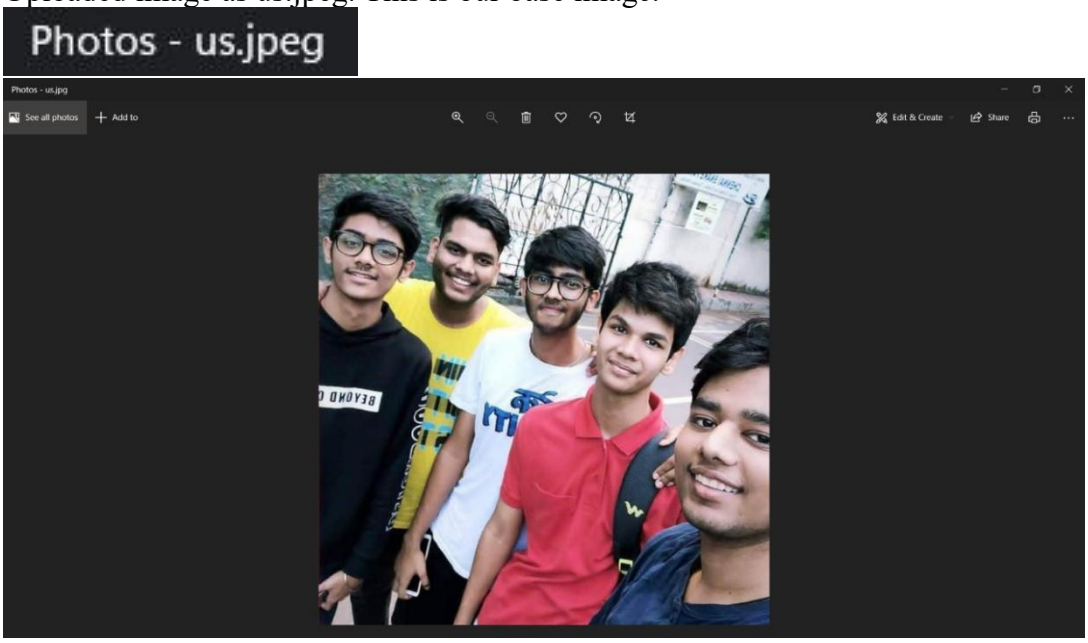


Image 3:
Encrypted image(enc.jpeg) obtained after encryption of uploaded image us.jpeg.

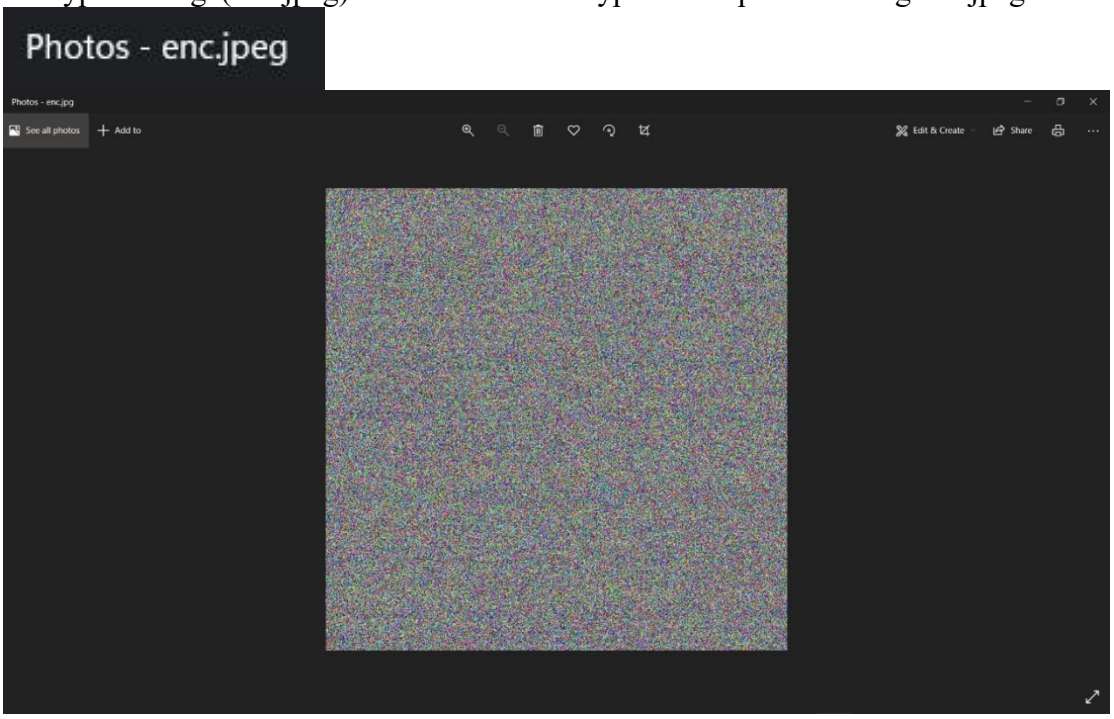
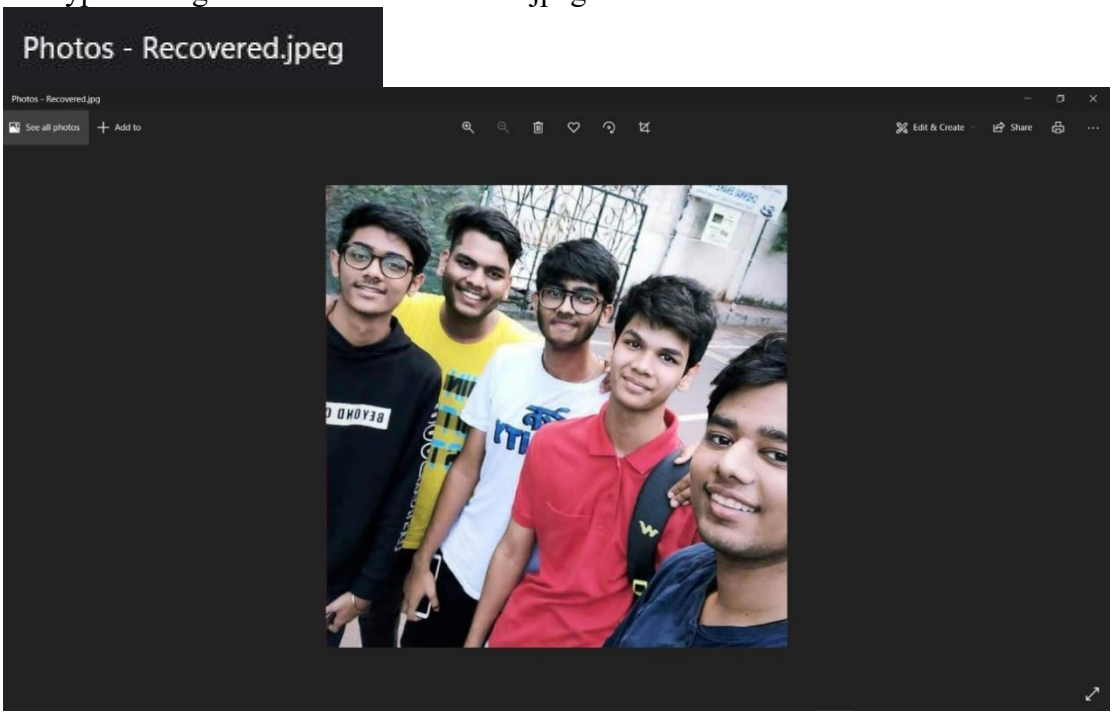


Image 4:
Decrypted image retrieved as Recovered.jpeg.



2. Interpretation of the obtained results:
In this well defined process as we observe from the above screenshots that the image uploaded at the beginning has been exactly retrieved the same from the executed DNA encryption code which depicts healthy implementation of designed code.

Firstly when us.jpeg is uploaded it soon gets encrypted and becomes a well protected image that is, enc.jpeg. Then decryption of enc.jpeg is initiated in order to recover the same image which was uploaded before and hence we get the desired image as a result of decryption which is saved in the system as Recovered.jpeg.

ANALYSIS:

HONEY ENCRYPTION:

1. Analysis of the results obtained:

From the results we can clearly observe how systems can be protected against brute force attacks on passwords by just adding honey words. Using honey encryption, we can also hide a secret message in these passwords.

2. Comparison of the obtained results with the already existing results:

Earlier there was no protection against brute force attacks which are a major threat as hashing and salting can't prevent it. Using honey words, we can increase the security of the system exponentially.

3. Efficiency obtained:

We have successfully hidden a secret message in these passwords generated through code of honey encryption.

DNA ENCRYPTION:

1. Analysis of the results obtained:

It is suggested from the results of DNA encryption and decryption that the processed image is perfectly encrypted and decrypted with the help of same algorithm and we can retrieve the decrypted image without any involvement of third-party medium.

2. Comparison of the obtained results with the already existing results:

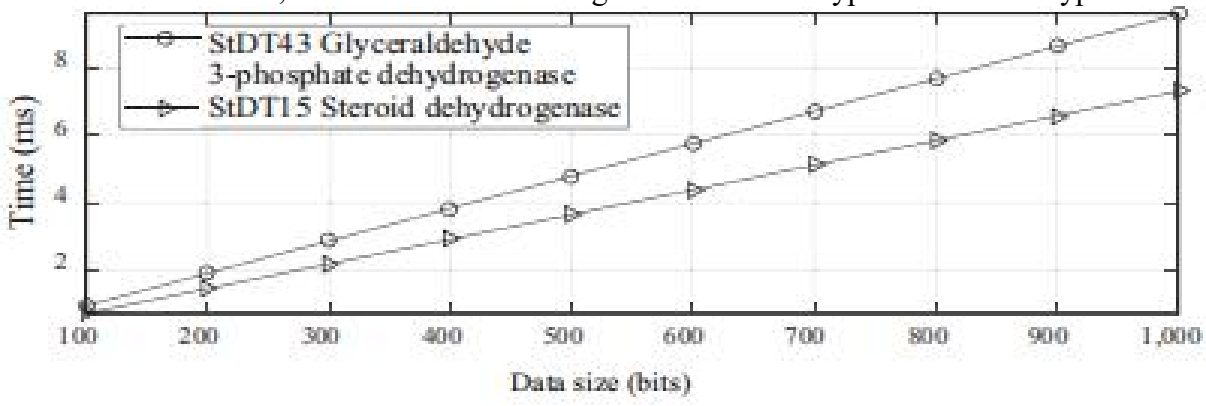
The current technique combines RSA public key cryptography with DNA computing to improve security. This procedure is quite simple, but the true issue is in selecting and generating public and private key pairs for RSA. It takes more bandwidth and electricity to convey data. For the modular exponential approach, RSA has a higher calculation cost.

3. Efficiency obtained:

The proposed method was significantly efficient in order to get perfectly encrypted image as tested by us. The decryption process was also personified with the result obtained of recovered image.

4. Graphs along with its interpretation:

For various data sizes, the execution time using DNA-based encryption-based encryption:



CONCLUSION AND FUTURE WORK:

1. Significance of the project:

From this project we studied the latest unpopular encryption techniques like Honey Encryption and DNA-based image encryption. We were able to recognize their advantages in real time scenarios and believe that honey encryption can be used in the password sector to protect them against brute force attacks.

2. Difficulties faced in performing these projects:

There were some key problems faced during the course of this project. As we know that DNA encryption and Honey encryption are not well known methods of encryption the field of cryptography due to which there were many intervals where we not able to find relevant papers. Compilation of code was also a tricky and lengthy process.

3. What could be done in the future? (Can it be improvised or not?):

For honey encryption using a proper NLP-based model for generating honey words, we can make the honey words generated even more deceptive and harder for the adversary to identify the real password. We can come up with a way to make sure that the honey maker is not exposed to the adversary ever as that would make the system the most secure. In the view of DNA encryption the time consumption of the process could be reduced in the future.

REFERENCES:

Journals:

- ✓ Jian Zhang, DongXin Fang, and Honge Ren, 31/12/2014, *Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps,* College of Information and Computer Engineering, Northeast Forestry University, Harbin 150040, China.
- ✓ Mousomi Roy, Shouvik Chakraborty, Kalyani Mali, Raja Swarnakar, Kushankur Ghosh, Arghasree Banerjee and Sankhadeep Chatterjee, May 2020,*Data Security Techniques Based on DNA Encryption,* Department of Computer Science & Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India.
- ✓ Vijay Choudhary, Tushar Mandge, 21-22 Feb. 2013, *A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme,* 2013 International Conference on Information Communication and Embedded Systems (ICICES), IEEE.
- ✓ Hoyul Choi, Hyunjae Nam, Junbeom Hur, October 2011, *Password Typos Resilience in Honey Encryption,* Department of Computer Science and Engineering Korea University Seoul, 136-701, Republic of Korea.
- ✓ Nahri Syeda Noorunnisa, Dr. Khan Rahat Afreen, 02/02/2016, *Review on Honey Encryption Technique*, Department of Computer Science and Engineering, Marthawada Shikshan Prasark Mandal‟s Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India.

Book Chapters:

- ✓ *Proceedings of The Eighth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), 2013* Zhixiang Yin Linqiang Pan Xianwen Fang (Eds.) Volume 1. The Advantages and Disadvantages of DNA Password in the Contrast to the Traditional Cryptography and Quantum Cryptography.

APPENDIX:

Work done by each individual student:

Maurya Goyal: Analyzed Honey encryption and performed coding.
Shivam Bansal: Analyzed DNA encryption compared and did image processing coding.
Saumitra Pathak: Analyzed DNA encryption compared and did encryption and decryption coding.

~~~~~THANK YOU~~~~~