Review Article

The Future of Data Security: DNA Cryptography and Cryptosystems

Tanvay Jaithliya[*]

Department of Pharmacy, Mewar University, Gangrar (Chittorgarh), India

[*]**Corresponding author:** Jaithliya T, Department of Pharmacy, Mewar University, Gangrar (Chittorgarh), India; Tel: +91-01471-291148; E-mail: jtanvay@gmail.com

In simple terms DNA cryptography can be defined as a hiding data in terms of DNA Sequence. The world of digitalization is growing and becoming better day by day. In this league of advancement all the nations are in a hurry to launch their best technology, to get a huge amount of customers and in the return increase the numbers in their accounts. There is a huge profit of these advancement one can even now do any work by using his voice, gestures or on his fingertips there is a new world waiting for him. This advancements increase our knowledge by teaching us in various means but some people gets the wrong idea of this advancement. People of this kind use their knowledge and ability in the wrong direction and become cyber criminals. Due to increasing crime rates or we can security breaches in the year 2014, a survey said that it is around 32 records were breached in every single second. As the technology and computer world develops the security question also arises side by side in order to protect the data, intellectual property, personal or public records and to retain breaches. There is a need to arrest the criminals as well as increase the security procedures as well. A new era of security techniques started which has originated from pin number protection enhance to password, finger print, retina, blood test, picture password and so on and sometimes a mixture of two or three also used for extra protection. A individual wants to secure its data in any condition, she wants to be the owner of her work and without her permission no one can see it or get knowledge about it. Thus to increase security levels a new security techniques are used to get more security. In this article a new future data security technology is explained named as DNA cryptography.

Why DNA Cryptography and Which Are the Principal Benefits for its Adoption?

DNA Computing

Information Security is very vital in today's digital era of e-commerce and e-business. While 2014 was "The Year of Data Breach", 2015 is off to a fast start with several prominent data breaches. As per statistics gathered by *Breach Level Index*, there were more than 2 million records per day that were breached in the year 2014, which means, 32 records were breached each second. It's apparent that a new approach to data security is needed, if organizations are to stay ahead of the attackers and more effectively protect their intellectual property, data, customer information, employees. Security approaches must be good enough to tackle the ever-changing data breaches. This is where the data security, encryption of data at rest and in motion, implementing user access control come into play.

World of Cryptography

Multiple cryptographic techniques are used for securing the data over the network. Cryptography is the art of converting the original message into human unreadable code, which cannot be reversed to the original message. Cryptography plays a very important role in data integrity in the three components of the CIA triad (Confidentiality, Integrity, and Availability). CIA is the fundamental concept in security.

Why DNA cryptography?

DNA cryptography is one of the rapid emerging technology which works on concepts of DNA computing. A new technique for securing data was introduced using the biological structure of DNA called DNA Computing (aka molecular computing or biological computing). It was invented by Leonard Max Adleman in the year 1994, for solving the complex problems such as directed Hamilton path problem, NP-complete problem similar to The Travelling Salesman problem. Adleman is also known as the 'A' in the RSA algorithm – an algorithm that in some circles has become the de facto standard for industrial-strength encryption of data sent over the Web. The technique later on extended by various researchers for encrypting and reducing the storage size of data that made the data transmission over the network faster and secured.

DNA can be used to store and transmit data. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, a five carbon sugar and a phosphate group. The nucleotides that make up these polymers are named after the nitrogen base that it consists of;

► Adenine (A)

► Cytosine (C)

► Guanine (G)

► Thymine (T)

Advantages of DNA Computing

► **Speed:** Conventional computers can perform approximately 100 MIPS (millions of instruction per second). Combining DNA strands as demonstrated by Adleman, made computations equivalent to 10^9 or better, arguably over 100 times faster than the fastest computer.

► **Minimal Storage Requirements:** DNA stores memory at a density of about 1 bit per cubic nanometer where conventional storage media requires 10^12 cubic nanometers to store 1 bit.

► **Minimal Power Requirements:** There is no power required for DNA computing while the computation is taking place. The chemical bonds that are the building blocks of DNA happen without any outside power source. There is no comparison to the power requirements of conventional computers.

Traditional cryptography and its security are based on difficult mathematic problems which are mature both in theory and realization. Both the secret-key and public-key methods of cryptology have unique flaws. The keys used in modern cryptography are so large, in fact, that a billion computers working in conjunction with each processing a billion calculations per second would still take a trillion years to definitively crack a key. This isn't a problem now, but it soon will be, given the growth of the computing power and technologies.

Multiple DNA crypto algorithms has been researched and published like the Symmetric and Asymmetric Key crypto System using DNA, DNA Steganography Systems, Triple stage DNA cryptography, Encryption algorithm inspired by DNA and Chaotic computing.

DNA Cryptography can be defined as A Hiding Data in Terms of DNA Sequence

Cryptographic technique in which each letter of the alphabet is converted into a different combination of the four bases that makes up the human Deoxyribonucleic Acid (DNA).

Professor Shafi Goldwasser, winner of the 2012 Turing Award, told Asian Scientist Magazine at the Global Young Scientists Summit.

"Often people's gut instinct is that it is impossible to achieve privacy, so there is no point in trying, that is not a misunderstanding of what's currently going on, but it is a misunderstanding of what is possible. However, people may be unwilling to give their DNA if their genetic information is used against them. The idea is to encrypt the DNA such that you can recover what you are looking for, such as a particular gene, without revealing the entire sequence." Goldwasser also emphasizes that "There are many things we can do with the mathematics- it's just that they appear somewhat paradoxical if you think about them in the physical world. The idea that you can compute on the data without actually looking at it, or that you can actually verify something without looking at all the steps; it's a bit mind boggling".

Even today, people are not entirely sure what they expect a good encryption mechanism system to do. A simple mechanism of transmitting two related messages by hiding the message is not enough to prevent an attacker from breaking the code.

Traditional Cryptography can be traced back to Caesar Cipher 2000 years ago or even earlier. With time, it has evolved to provide an extremely high computational security. But an adversary with infinite computing power can break them theoretically. On the other hand DNA cryptography can have special advantage for secure data storage, authentication, digital signatures, steganography, and so on. DNA can also be used for producing identification cards, and tickets. Below is an Image Encryption using Chaotic Maps and DNA addition:-

"Trying to build security that will last 20 to 30 years for a defense program is very, very challenging,"

Benjamin Jun, Vice President and Chief Technology Officer at Cryptography Research

Multiple studies have been carried out on variety of bio-molecular methods for encrypting and decrypting data that is stored as a DNA.

Advantages of DNA Storage of Data

► Medium of Ultra-compact Information storage: Very large amounts of data that can be stored in compact volume

► A gram of DNA contains 1021 DNA bases = 108 Terabytes of data.

► A few grams of DNA may hold all data stored in the world.

Though DNA cryptography is in its infancy. Only in the last few years has work in DNA computing seen real progress. DNA cryptography is even less well studied, but ramped up work in cryptography over the past several years has laid good groundwork for applying DNA methodologies to cryptography and steganography. A number of schemes have been proposed that offer some level of DNA cryptography, and are being explored. At present, work in DNA cryptography is centered on using DNA sequences to encode binary data in some form or another. Though the field is extremely complex and current work is still in the developmental stages, there is a lot of hope that DNA computing will act as a good technique for information security.

Great SIM Heist-Documents Reveal Mass Cell Phone Hack by Five Eyes Intelligence

US and British intelligence services have stolen encryption keys of the major SIM card maker Gemalto to spy on mobile voice.

References

1. http://securityaffairs.co/wordpress/33879/security/dna-security-cryptography.html