International Journal of Computer Sciences and Engineering
Vol.**12**, Issue.**11**, pp.**21-35**, November **2024**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

Technological Evolution in Information Security: A Cryptographic Perspective

Sriramudu[1], G. Padmavathi[2], Nagendar Yerukala[3], Neelima Guntupalli[4]

[1]C R Rao AIMSCS, UoH Campus, Hyderabad, Telangana, India & Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
[2,3]C R Rao AIMSCS, UoH Campus, Hyderabad, Telangana, India
[4]Acharya Nagarjuna University, Guntur, Andhra Pradesh, India

**Corresponding Author: padmagvathi@gmail.com*

Received: 21/Sept/2024; **Accepted**: 23/Oct/2024; **Published**: 30/Nov/2024. **DOI**: https://doi.org/10.26438/ijcse/v12i11.2135

Abstract: This paper gives a critical review of the evolution of encryption methodologies with regard to their function within the technological field in ensuring cryptographic security. It starts with an overview of traditional methods of encryption, including character replacement methods, then classical encryption methods. It progresses through the electrical and electronic machine-based method of developing newer techniques up to the modern ones, such as digital machines, quantum machines, and post-quantum ciphers.
This is followed by simulations, software-based generation of cipher text, thus forming an overview of the cryptographic technologies in use. Examples of formats for ciphers are provided to show how, in practice these encryption methods apply to real-world-type situations or scenarios. Maybe, through such observation, the paper is trying to enlighten its audience with regard to the dynamic nature of cryptographic security and its place in modern technology.

Keywords: Classical encryption, electronic machine cipher, Digital Machines, Quantum machines.

1. Introduction

Cryptography is the art of secure communication, which has experienced tremendous change over its periods, each with a significant advancement. Classical cryptography started with simple substitution and transposition ciphers like the Caesar cipher and Vigenère cipher. Effective in their times, these techniques became weak as cryptanalysis improved with passing time.

Machine ciphers in the twentieth century, particularly rotor-based ciphers such as the Enigma machine, began mechanical methods of encryption with greatly increased complexity and security of encrypted messages. These developments were very critical in wartime communications and cryptographic progress.

With the advent of the digital age came the emergence of the remaining category, modern cryptography, relying on mathematically strong algorithms like AES and RSA to secure electronic communication and data storage, this can be said to make cryptographic techniques basically fundamental to today's security in the electronic world-from online banking to secure messaging.

Quantum Computing: The new challenges that arise with the advent of quantum computers are the breaking of the classical cryptographic algorithms. Quantum cryptology provides solutions, for example, in the form of Quantum Key Distribution (QKD) that utilizes quantum mechanics for secure communication.

To counter such quantum threats, current efforts are being made towards developing post-quantum cryptography which works towards designing encryption algorithms that would resist a quantum computer attack so that long-term data security is not affected.

This paper would briefly tell of the course of cryptography from its classical forms to modern days, including key developments and challenges brought about by quantum advances.

We have presented how technology evolution has played major role in designing secure and efficient crypto-algorithms from classical to modern, Quantum and post-Quantum days. The different transformation models has been discussed with transistors/devices technologies.

2. Transform Model

There are different ways to represent the ciphertext (encrypted text) based on that particular encryption procedure (Classical/ Machine based/ Modern/ Quantum/ Post-Quantum) such as Reversing the text, replacing the word, numerical representations, Bit representation, code-word representations etc. Some of them are discussed below.

2.1. Replace-encryption

Character substitution, sometimes referred to as "replace-encryption," is a very basic form of text obfuscation in which the characters in a message are replaced or substituted with other characters based on some predefined rule or key. Here, every character of the plaintext is substituted with another one following the key series for encryption. Although this technique seems to be a simple way for changing the apparent text of a message, it is not at all considered secure for protecting sensitive information, since the substitution patterns can be easily analysed and reversed. More advanced cryptographic techniques, like symmetric-key or asymmetric-key encryption, could be advised for stronger security.

Plain text: A DEFINITION OF A SECURE CHANNEL THAT REMAINS SECURE, EVEN WHEN USED IN ARBITRARY CRYPTOGRAPHIC PROTOCOLS IS AN IMPORTANT BUILDING BLOCK FOR UNIVERSALLY COMPOSABLE CRYPTOGRAPHY.

Cipher text: A DEFINITION OF A HARD CHANNEL THAT REMAINS SECURE, EVEN WHEN USED IN ARBITRARY CRYPTOGRAPHIC PROTOCOLS IS AN IMPORTANT BUILDING BLOCK FOR UNIVERSALLY COMPOSABLE CRYPTOGRAPHY.

2.2. Reverse encryption

Reverse, otherwise known as "reversal" or "mirror cipher," is a very basic text transformation technique where each character in the message gets reversed; that is, the first character becomes the last, the second becomes second-to-last, and so on. For example, "Hello" would be encrypted as "olleH.". Although it is easy to use reverse encryption, it is rather plain and not considered secure for the encryption of sensitive information. This, most of the time, will only be utilized either just for fun or as an educational tool and wouldn't be used with serious encryption, since it's easily reversible to obtain the original message. More advanced cryptographic methods should be used for secure communications.

Ciphertext: YHPARGOTPYRC ELBASOPMOC YLLASREVINU ROF KCOLB GNIDLIUB TNATROPMI NA SI SLOCOTORP CIHPARGOTPYRC YRARTIBRA NI DESU NEHW NEVE, ERUCES SNIAMER TAHT LENNAHC ERUCES A FO NOITINIFED A

2.3. Case Transform

Case transform encryption is the easiest text obfuscation, which is just a change in case. A predefined rule changes the case, either upper or lower, of letters in a message. All these transformations are not at all secure for sensitive information since they are readily reversible. The process usually consists of changes to the letter case, which proceed by some defined rule, such as alternating between upper and lower cases, or by some other rule. This technique has very low security compared with symmetric and asymmetric methods; hence, if one really wants to protect sensible information, it is advisable to use either symmetric or asymmetric cryptographic methods [1].

Cipher text: a dEfInItIoN Of a sEcUrE ChAnNeL ThAt rEmAiNs sEcUrE, eVeN WhEn uSeD In aRbItRaRy cRyPtOgRaPhIc pRoToCoLs iS An iMpOrTaNt bUiLdInG BlOcK FoR UnIvErSaLlY CoMpOsAbLe cRyPtOgRaPhY.

2.4. Numeral System

Cipher text (HEX): 41 20 64 65 66 69 6e 69 74 69 6f 6e 20 6f 66 20 61 20 73 65 63 75 72 65 20 63 68 61 6e 6e 65 6c 20 74 68 61 74 20 72 65 6d 61 69 6e 73 20 73 65 63 75 72 65 2c 20 65 76 65 6e 20 77 68 65 6e 20 75 73 65 64 20 69 6e 20 61 72 62 69 74 72 61 72 79 20 63 72 79 70 74 6f 67 72 61 70 68 69 63 20 70 72 6f 74 6f 63 6f 6c 73 20 69 73 20 61 6e 20 69 6d 70 6f 72 74 61 6e 74 20 62 75 69 6c 64 69 6e 67 20 62 6c 6f 63 6b 20 66 6f 72 20 75 6e 69 76 65 72 73 61 6c 6c 79 20 63 6f 6d 70 6f 73 61 62 6c 65 20 63 72 79 70 74 6f 67 72 61 70 68 79 2e 20 20

2.5. Bitwise operation

Bitwise operation encryption modifies each individual bit of a binary numeral with the help of the bitwise operators: AND, OR, XOR, and shifts. It is a very useful tool in low-level programming and for computer systems wherein simple encryption operations on binary data are performed. In this, bitwise operations are applied onto each bit of a message and a key such that the information in it may get modified. In the case of bitwise operations, they do hide information to a certain extent. But it's not very secure for secret information and definitely not adequate to endure complex attacks. So, some form of better confidentiality and integrity cryptographic algorithm should be used for safe encryption.

Cipher text(NOT): be df 9b 9a 99 96 91 96 8b 96 90 91 df 90 99 df 9e df 8c 9a 9c 8a 8d 9a df 9c 97 9e 91 91 9a 93 df 8b 97 9e 8b df 8d 9a 92 9e 96 91 8c df 8c 9a 9c 8a 8d 9a d3 df 9a 89 9a 91 df 88 97 9a 91 df 8a 8c 9a 9b df 96 91 df 9e 8d 9d 96 8b 8d 9e 8d 86 df 9c 8d 86 8f 8b 90 98 8d 9e 8f 97 96 9c df 8f 8d 90 8b 90 9c 90 93 8c df 96 8c df 9e 91 df 96 92 8f 90 8d 8b 9e 91 8b df 9d 8a 96 93 9b 96 91 98 df 9d 93 90 9c 94 df 99 90 8d df 8a 91 96 89 9a 8d 8c 9e 93 93 86 df 9c 90 92 8f 90 8c 9e 9d 93 9a df 9c 8d 86 8f 8b 90 98 8d 9e 8f 97 86 d1 df df

2.6. Morse code

Basically, Morse code consists of short and long signals, usually notated as dots and dashes, that are transmitted by sound or light. Developed in the early years of the 19th century by Samuel Morse, it was a method of transmitting information over long distances using telegraph technology.

In the code, each letter and number is given a unique combination of dots and dashes. As an example, the letter "A" is represented by a single bit, followed by a single dah: ".-"; similarly, the number "5" would represent five bits, followed by a single dah: ".-".

In the past, Morse code was heavily used for communication over telegraph wires, radio waves, and other means of long-distance communication; today, it is still in use among amateur radio operators. Today, to some extent, it is also used in situations of low availability of equipment for communication, like in the military or even in survival

scenarios in the wilderness. One of the many merits of Morse code is the fact that it is capable of sending out a message using only simple equipment and language that may not even be shared between the sender and receiver.

Use of Morse code: Morse code was used, historically, in a vast number of purposes in communication, which includes:

1. Telegraphy: At the very beginning, morse code was developed to work with the technology of telegraphy-mid 19th century. The code was specifically put to use to make sure messages were transmitted over quite a long distance at a faster speed with reliability, hence revolutionizing communication at that time.

2. Aviation: Morse code was in use during the nascent days of aviation for communication between aircraft either in-air with the communication centres on the ground or between more than one aircraft in the sky.

3. Maritime: Morse code found extensive uses in the maritime industry for distress signalling, such as SOS, etc. Ships could send their signals to other ships or the shore station even a long way off. when other communication modes had failed.

4. Military: The use of morse code dates back with the military for utilities such as covert communication, encoding sensitive messages and also for signalling.

5. Amateur Radio: Even today, morse code remains in use by thousands of amateur radio operators to communicate over long distances using very simple equipment.

6. Wilderness survival: In cases of wilderness survival, morse code can come in use when it needs to be used for an SOS or another form of communication when all other forms of communication are not possible.

Even though Morse code in most practical situations has already been replaced with newer versions of communication technology, it still holds an important position in the pages of history and is preserved with many hobbyists and enthusiasts even today.

Cipher text:.- / -.. . ..-. .. -. .. - .. --- -. / --- ..-. / .- / ... . -.-. ..- .- . . / -.-. .... .- -. -. . .-.. / - .... .- - / .-. . -- .- .. -. ... / ... . -.-. ..- .-. . --..-- / . ...- . -. / .-- .... . -. / ..- ... . -.. / .. -. / .- .-. -... .. - .-. .- .-. - .-- / -.-. .-. -.-- .--. - --- --. .-. .- .--. .... .. -.-. / .--. .-. --- - --- -.-. - -- .-.. ... / .. ... / .- -. / .. -- .--. --- .-. - .- -. - / -... ..- .. .-.. -.. .. -. -- . / -... .-.. --- -.-. -.- / ..-. --- .-. / ..- -. .. ...- . .-. ... .- .-.. .-.. -.-- / -.-. --- -- .--. --- ... .- -... .-.. . / -.-. .-. -.-- .--. - --- --. .-. .- .--. .... -.-- .-.-.- / /

2.7. Spelling alphabet

The spelling alphabet cipher, also known as the phonetic alphabet or, more specifically, NATO phonetic alphabet, is a system of spelling letters or words over a communications channel of low intelligibility, like radio or phone. Each letter in the alphabet corresponds to a unique word to avoid confusion between similar sounding letters.

A = Alpha, B = Bravo, C = Charlie, D = Delta, E = Echo, F = Foxtrot, G = Golf, H = Hotel, I = India, J = Juliet, K = Kilo, L = Lima, M = Mike, N = November, O = Oscar, P = Papa, Q = Quebec, R = Romeo, S = Sierra, T = Tango, U = Uniform, V = Victor, W = Whiskey, X = X-ray, Y = Yankee, Z = Zulu

It would help this system to spell a message, "HELLO," as "Hotel Echo Lima Oscar." This brings out the clear message even under noisy or unclear conditions.

Cipher text: Alfa (space) Delta Echo Foxtrot India November India Tango India Oscar November (space) Oscar Foxtrot (space) Alfa (space) Sierra Echo Charlie Uniform Romeo Echo (space) Charlie Hotel Alfa November November Echo Lima (space) Tango Hotel Alfa Tango (space) Romeo Echo Mike Alfa India November Sierra (space) Sierra Echo Charlie Uniform Romeo Echo , (space) Echo Victor Echo November (space) Whiskey Hotel Echo November (space) Uniform Sierra Echo Delta (space) India November (space) Alfa Romeo Bravo India Tango Romeo Alfa Romeo Yankee (space) Charlie Romeo Yankee Papa Tango Oscar Golf Romeo Alfa Papa Hotel India Charlie (space) Papa Romeo Oscar Tango Oscar Charlie Oscar Lima Sierra (space) India Sierra (space) Alfa November (space) India Mike Papa Oscar Romeo Tango Alfa November Tango (space) Bravo Uniform India Lima Delta India November Golf (space) Bravo Lima Oscar Charlie Kilo (space) Foxtrot Oscar Romeo (space) Uniform November India Victor Echo Romeo Sierra Alfa Lima Lima Yankee (space) Charlie Oscar Mike Papa Oscar Sierra Alfa Bravo Lima Echo (space) Charlie Romeo Yankee Papa Tango Oscar Golf Romeo Alfa Papa Hotel Yankee Stop (space) (space).

The evolution of cryptosystems based on the evolving technologies is categorized into classical, Machine, electronic-machines, modern, Qunatum and Post-Quantum as discussed below.

3. Classical Cryptology

3.1. Caesar cipher

The Caesar cipher is the classic, simplest substitution encryption method. It is named after Julius Caesar, said to have used it with his private messages. In this system, each letter of the plaintext is shifted by some places either downwards or upwards in the alphabet. For example, the shift of 3 moves 'A' to 'D', 'B' to 'E', and so on. While quite easily thought out and implemented, the Caesar cipher is nonetheless considered comparatively weak by modern standards. The method employed here is, in essence, what was known as a substitution cipher; in consequence, it is relatively insecure against brute-force attacks because there are only twenty-six possible keys to be tried. Again, while this does not yield much in terms of security, the Caesar cipher provides an extremely good way of introducing students to some basic ideas behind cryptography [1].

CipherText:HKLMPUPAPVUVMHZLJBYLJOHUULSAO HAYLTHPUZZLJBYLLCLUDOLUBZLKPUHYIPAYHYF JYFWAVNYHWOPJWYVAVJVSZPZHUPTWVYAHUAI BPSKPUNISVJRMVYBUPCLYZHSSFJVTWVZHISLJYF WAVNYHWOF AFFINE CIPHER

3.2. ROT13

Well, then, the really easy and very popular technique of obfuscating text is a kind of ROT13 encryption, rotating

every letter in the alphabet by 13 places. As is visible from the name itself, this is a kind of a Caesar cipher; to be more exact, a shift of half the alphabet in a Caesar cipher is performed. With ROT13, every letter is substituted with the one standing 13 places forward or backward from it in the alphabet. The process is its own inverse, meaning applying this a second time to the encrypted text basic restores the original message. ROT13 is often used for casual data obfuscation. It helps in hiding the spoilers or obscuring text in online forums based on its simple substitution method. Such a method provides minimum security and no protection for sensitive data [2].

Cipher Text: N QRSVAVGVBA BS N FRPHER PUNAARY GUNG ERZNVAF FRPHER, RIRA JURA HFRQ VA NEOVGENEL PELCGBTENCUVP CEBGBPBYF VF NA VZCBEGNAG OHVYQVAT OYBPX SBE HAVIREFNYYL PBZCBFNOYR PELCGBTENCUL.

3.3. A1Z26

A1Z26 is a rather basic form of text encryption whereby each letter is replaced by its corresponding alphabetical position. In this scheme, 'A' is 1, 'B' stands for the number 2, and so forth, up to 'Z' being 26. Usually, numeric characters and spaces are not changed. A1Z26 is very easy to both teach and learn; therefore, it would be suitable for use in schools or personally [3]. This technique, however, cannot be adjudged secure for sensitive information since it lacks adequate complexity and cryptographic strength compared with other kinds of encryption.

Cipher Text: 1 4 5 6 9 14 9 20 9 15 14 15 6 1 19 5 3 21 18 5 3 8 1 14 14 5 12 20 8 1 20 18 5 13 1 9 14 19 19 5 3 21 18 5 5 22 5 14 23 8 5 14 21 19 5 4 9 14 1 18 2 9 20 18 1 18 25 3 18 25 16 20 15 7 18 1 16 8 9 3 16 18 15 20 15 3 15 12 19 9 19 1 14 9 13 16 15 18 20 1 14 20 2 21 9 12 4 9 14 7 2 12 15 3 11 6 15 18 21 14 9 22 5 18 19 1 12 12 25 3 15 13 16 15 19 1 2 12 5 3 18 25 16 20 15 7 18 1 16 8 25

3.4. Vigenere cipher

The Vigenere cipher is a classical text-encryption technique developed by Blaise de Vigenere in the 16th century. It is a polyalphabetic substitution cipher; that is, it uses several substitution alphabets. The keyword or phrase for the Vigenere cipher is a key that determines the shifting of the alphabets. Surprisingly, until the 19th century, the Vigenere cipher remained unbroken for centuries and was considered totally unbreakable [4]. It gives a much higher level of security compared to a lot of the simple substitution ciphers because of key-dependent shifting. Nevertheless, in this day and age, it succumbs to modern cryptographic analysis techniques, and currently it is primarily of interest only in history.

CipherText:CUCUBVQVZMCHNIUVAJKMKJRLCXTBJ RRGXUIKEQHXKCTV,CKXVEJVLJLMLKEYGUQBTRP NVZGRKMVKIXJZAEKWBQTMALQACEGBIWZVRLIU CQNUGCZJTQTIUHZCPZTTKAINCWRHUXQJYQEMK TPNIHOZCGFN.

3.5. Baconcipher

This is often referred to as the Bacon cipher, although it is sometimes referred to by the alternative name, Baconian cipher [5]. This is actually a steganographic way of encoding the message in a binary system. The writer Sir Francis Bacon is credited for developing this cipher during the late 16th century. Each letter of the alphabet in the message is replaced by a string of five binary digits, normally represented as a change of capitalization between two different letters, such as 'A' and 'B'. This cipher can be implemented in a variety of schemes, like uppercase and lowercase letters or even specific fonts. Technically, users do not employ the Bacon cipher for the purpose of security, but it was designed to conceal communication in quite plain sight. It is a bit simplistic, but if implemented with some other scheme for encryption, it can provide minimal security.

Cipher Text: aaaaa aaabb aabaa aabab abaaa abbaa abaaa baaba abaaa abbab abbaa abbab aabab aaaaa baaab aabaa aaaba baabb baaaa aabaa aaaba aabbb aaaaa abbaa abbaa aabaa ababa baaba aabbb aaaaa baaba baaaa aabaa ababb aaaaa abaaa abbaa baaab baaab aabaa aaaba baabb baaaa aabaa aabaa baabb aabaa abbaa babaa aabbb aabaa abbaa baabb baaab aabaa aaabb abaaa abbaa aaaaa baaaa aaaab abaaa baaba baaaa aaaaa baaaa babba aaaba baaaa babba abbba baaba abbab aabba baaaa aaaaa abbba aabbb abaaa aaaba abbba baaaa abbab baaba abbab aaaba abbab ababa baaab abaaa baaab aaaaa abbaa abaaa ababb abbba abbab baaaa baaba aaaaa abbaa baaba aaaab baabb abaaa ababa aaabb abaaa abbaa aabba aaaab ababa abbab aaaba abaab aabab abbab baaaa baabb abbaa abaaa baabb aabaa baaaa baaab aaaaa ababa ababa babba aaaba abbab ababb abbba abbab baaab aaaaa aaaab ababa aabaa aaaba baaaa babba abbba baaba abbab aabba baaaa aaaaa abbba aabbb babba

3.6. Alphabetical substitution

Alphabetical substitution, otherwise known as mono-alphabetic substitution, is the easiest concept in encryption. In this technique, the letters of plaintext get substituted by corresponding letters from the shifted alphabet. For instance, since it is a simple alphabetic substitution technique, in the case of the Caesar cipher, each letter is replaced by a letter some fixed places down the alphabet [6]. Though simple, monoalphabetic substitution ciphers are susceptible to attack by letter frequency analysis, which is basically an inference of the probable letters used in the cipher text to decrypt a message. Simple alphabetical substitution, though a minor step in the development of cryptography, played a big role in the history of this discipline and therefore provided a foundation for more complex encryption techniques.

CipherText:ZWVURMRGRLMLUZHVXFIVXSZMMVO GSZGIVNZRMHHVXFIV,VEVMDSVMFHVWRMZIYRG IZIBXIBKGLTIZKSRXKILGLXLOHRHZMRNKLIGZMG YFROWRMTYOLXPULIFMREVIHZOOBXLNKLHZYOV XIBKGLTIZKSB.

3.7. Rail fence cipher

The Rail Fence cipher is one of the easiest transposition ciphers, rearranging simply the characters of a message. The

process works T by writing a plaintext in a zigzag pattern over a number of lines or "rails" and then reading off in linear manner to form the cipher text. The number of rails is the key for the cipher [7].

CipherText:AEIIINFSCRCANLHTEANSCR,VNHNSDNR IRRCYTGAHCRTCLIAIPRATULIGLCFRNVRALCMOA LCYTGAH.DFNTOOAEUEHNETARMISEUEEEWEUEIA BTAYRPORPIPOOOSSNMOTNBIDNBOKOUIESLYOPS BERPORPY

3.8. Polybius Square ciphers

The most basic type of encryption is called Polybius Square, after the well-known Greek historian of antiquity by the same name [8]. It works by simply mapping each letter of the alphabet onto a grid's coordinates. primarily utilized for plaintext communication encryption.

CipherText:11141521243324442434333421114315134542151323113333153144231144421532112433434315134542151551153352231533454315142433114212244442114254134254354434224211352324133542344434133431432443113324323534424411334412452431142433221231341325213442453324511542431131315413343235344311123115134254354434224211352354

3.8.2.ADFGX cipher

ADFGX cipher is one of the methods of cryptography used during World War I by the German military. It is basically the variant of both transposition and substitution ciphers whose principles of columnar transposition are combined and interwoven with those of a Polybius square [9].

In the ADFGX cipher, the letters of the alphabet get encrypted to two different ciphertext characters—'A', 'D', 'F', 'G', and 'X"—via a Polybius square, the characters forming a fractionated key square arranged in a grid. The rows are filled column-wise with a plaintext transposition, and the resulting cipher is then read off row by row.

The name "ADFGX" comes from the fact that in ciphertext, only these letters were used. Due to its high complexity, the ADFGX cipher was considered secure, but after deciphering by French cryptanalysts, the property is not held any more, like the evolution of cryptographic techniques to create more secure systems.

CipherText: adfdf axgff xdgfg gfaax xggad gdgxd adxgf gfdxg fgafd aaggg axgfa adgdf gaxfg faaxa aaggx dfadx faxaf aggff gaffg aagff dfdfg agddd xaafx aagxd axgdg fggfa ffaad afaxa xdfag ggagx ggxad fgdaf gagdg dadgf agaad gdagf ddagg gdfgx afgaa agxgx ffgxf dgaag fddff gfgfd gaagd dfxgf affff ffffg afaad gfaad dfffg dffgx adffd addxd gdfgg gffag fggxa ffffx xdfgf gaxxg gx

3.8.3. Bifid cipher

The Bifid cipher was invented in the year 1901 by Félix Delastelle, a French cryptographer. Being a mix of both a transposition and substitution cipher, it offers greater security compared to monoalphabetic substitution ciphers.

First of all, in Bifid, plaintext is converted into numbers with a Polybius square, where every letter designates its coordinates: column and line. Afterwards | the numbers were arranged in a grid. Later, the numbers are read out in another order. Normally, this would be done row after row or column after column. A transposed sequence of numbers comes out. Later, the transposed numbers are rewritten as letters [10].

The Bifid cipher is incomparably more secure than many others, due to the presence of the features of transposition and substitution, which make the cipher resistant to frequency analysis. Still, it might be quite vulnerable to the most modern methods of cryptanalysis. Although it played a very significant role historically, it is almost never used in modern cryptography nowadays, though it's interesting for studying classical ciphers and the history of cryptography.

CipherText:abhihnfqdqbcloftcboqdqecwctahdbtdvuomqmfo olnrqmnoqodhbmclgoskdqnvnnqcauomqmvudotsqcxwxlnvsd kfsnxwzemppptlgtfimutgeopitocscryicrydsgdpdkoehadoksbe mutgeo

3.8.4 .Nihilist cipher

The Nihilist cipher is a method that employs a Polybius square with a numerical key. This method was in use during the late 19th century among revolutionary Russian nihilists and anarchists. The application is considered that type of fractionation cipher which transforms plain text into its numeric equivalent and then encrypts such values through the use of a Polybius square [11].

Cipher Text: 24 56 69 56 68 57 48 57 66 88 68 78 45 35 56 57 67 80 86 39 37 36 53 87 68 59 55 68 36 53 98 77 59 56 35 37 75 97 78 59 37 69 55 57 69 86 59 57 76 36 57 87 80 87 39 38 37 75 65 77 56 48 68 55 53 96 89 57 66 78 48 86 88 57 86 35 59 36 66 67 70 86 58 68 47 55 88 66 87 48 67 24 75 78 67 79 58 66 57 53 87 79 56 69 48 44 56 78 68 66 36 55 47 55 79 56 78 66 69 46 66 105 50 86 67 35 44 73 108 48 78 56 59 47 85 65 47 75 39 37 55 96 89 79 78 46 66 24 77 77 89

3.8.5. Tapcode

The Tap Code is a simple, ingenious way to encode and send messages using a grid of tapping sounds. Notably, it has been in use among prisoners, more so during the Vietnam War period, as a secret means of communication. Basically, the Tap Code is a substitution cipher based on a 5 × 5 grid where every letter of the alphabet, excluding 'K', gets represented by two different taps: one for the line and another for the column [12].

Cipher Text:. . . ..

3.8.6. Trifid cipher

A well-known cryptography algorithm, the Trifid cipher is a combination of substitution and transposition ciphers. The Trifid cipher was devised by Félix Delastelle in 1895. It can be regarded as an extension to the Bifid cipher [13]. In essence, the Trifid cipher looks each character of plaintext up in a three-dimensional grid and represents it as three sets of coordinates and then encrypts them.

CipherText:aansrleuormhmfsckcozamtqefbcfmvjwfjfujqbhah rwttntnftjntbevulcjufppruyyqfftuda+arnxvlxesj+utdfjpnupcvp tawrjjqyveddfzewprzgrogpesccunqqggbabbxqxypfdluuby

4. Machines based Cryptology

4.1. Enigma

Probably the most compulsorily electromechanical cryptography device tasked for the German military during World War II, the Enigma was a device by a German engineer known as Arthur Scherbius in the early twentieth century. It played a very integral part in securing communications within the Axis forces. This device is notorious for its high level of complication; it was first considered a very strong encryption [14].

This was the Enigma machine, and it did this through a series of rotors, plugboards, and reflectors. And each time you hammered a key on the keyboard had quite complicated electrical connection series to substitute a letter. Rotors and the settings of the plugboard changed very frequently to add security to the process.

Among all that security, Enigma in encrypted communications was broken by the Allies, one major contributing factor being British mathematician Alan Turing and his colleagues working at Bletchley Park, that proved to be very instrumental in ending victory by the Allies during the war. Cryptographically, Enigma's weak spots and the achievements of these decryption activities marked a turning point within the history of cryptanalysis.

A tool such as Enigma is a symbol of issues and victories that the 20th century faced regarding cryptography-the sign of innovation and resilience against cryptographic threats.

CipherText: uuiis euxox fgslp ohmtk ravud ogfvj qujlz mabmt zvgjn wbdiw lqjac avici qsidq chybz vpsrz lwuzu gzcux tradr jvyff mbesz wqfnq dgokx qvmqh semrx fwoll duhaj clzwv uitdx afwuf pqjaw i

4.2. Hagelin

One of the most famous Swedish inventors and entrepreneurs in modern times is Boris Hagelin, leaving his mark on cryptography by developing cryptographic machines. Born on July 2, 1892, he founded what is now Crypto AG, in Switzerland, in 1952. Crypto AG has become huge in manufacturing cipher machines during the Cold War years.

Hagelin's most famous cryptographic machine was the M-209, a portable mechanical cipher machine that saw wide use with the United States and its allies during World War II and the Korean War. The M-209 gained a reputation in the field for being simple, reliable, and easy to operate [15].

Other than the M-209, Hagelin's company produced a range of cryptographical machines for different governments, military, and intelligence organizations across the globe. The machines he designed at Crypto AG made news without exception for their superior functionality and served adequately in secret communications in the decade of geopolitical tension.

It was revealed in 2020 that Crypto AG had secretly been rigged under Hagelin's leadership, and for decades, the CIA and West German intelligence had the ability to wiretap thumb-encoded, inked, and lined-up communications. This fact has added an extremely complex layer to the history of Crypto AG and grounded the legacy of Boris Hagelin in world cryptography.

4.3. Hagelin BC-52

Hagelin BC-52 is one of the series of mechanical cipher machines invented and developed by Swedish inventor and entrepreneur Boris Hagelin mid-century. Hagelin BC-52 is a member of the legendary M-209 [16].

BC-52 is a portable encryption device: essentially in service with military and diplomatic services during years of the Cold War. It has therefore developed safe encoding and decoding of messages due to its rotating cipher wheels and mechanisms found inside the device that ensure cryptographic security.

As with most cipher machines of this era, the BC-52 is a hand machine; plaintext messages are typed in, and the various settings on the machine are set such that an enciphered ciphertext is produced. Its compactness makes it ideal for field use and satisfies all the requirements of communications in remote or hostile environments.

In the operational life of the Hagelin BC-52, it served at the center of secure communication and helped further the encryption effort in many government and military organizations. Even though the BC-52 has been replaced by much more advanced electronic methods of encryption, it remains an illustration of the ingenuity of Hagelin and the advancement in cryptographic methods over the twentieth century.

Cipher Text (BC52): FUYBA JEDKJ YOYGH ZHKJR CDMEA VVISE IOPYV RDRNT ANSQJ IKFOJ SPNSM XWLBM QADVO EQFCI BEMYJ QRTFZ YCRDP VCVYQ FQBWK SSZOT SRTEN FQFDS YLUUL CVLCT AZGLQ PMAUO CRHYY MMEGH EVBFF YBNMP IG

5. Electronic Machine based Cryptology

5.1. SIGABA

SIGABA, otherwise known as the M-134-C, was a highly advanced electro-mechanical rotor machine for secure communications during World War II. Having been invented in the United States, it was surely among the most secure encryption devices available at this time with its cynically

complicated system of rotors, cams, and switches that encrypted and decrypted messages [17].

What set SIGABA apart was that it could generate several layers of encryption simultaneously, which gave it a huge security value against cryptographic attack. No enemy forces could break the machine during its operational use, thus maintaining very secure channels for communication work on the Allied side.

This was such a good security that SIGABA remained classified for many years after World War II. The design of this machine clearly became very complex and powerful; therefore, it represents a genuinely important contribution to the history of cryptographic machines.

Cipher Text: SAGUC XMYTL KUWWF OXQRL MXOHI WTLAM RPFQW FNNVK JLVGI OTCYO BNFMB WMQVZ MBVHI SRYHK JSOIA CIMAD KWKUK YUCCN LXVJI IUDTJ YOJXU WGTSR MKBHX GRFIB ADCMP JQUJZ LDBLY KBYQI VKAFP WFHZR W
Rotor settings:
cipher rotor = ASDFG control rotor = LKJHG index rotor = 967664

5.2. Lorenz

Lorenz cipher was one of the most complex cryptosystems, or high-order encryption systems, which the German army used to ensure safe communication during World War II. It is believed to be mainly used for strategic purposes in communication between senior officers and commands [18].
Key features of the Lorenz cipher can be stated in the following points:

Teleprinter Encryption: The Lorenz Cipher used with teleprinter machines, which were electro-mechanical contraptions for sending and receiving messages over long distances, contained inside it five binary, or "sprockets," wheels which powered the machine for encrypting.

The complexity and security were much greater than for the better-known Enigma cipher. This had been due to synergy of principles from the Vernam cipher-a type of XOR operation-with a machine-wheel technique for generating a pseudorandom key stream. It made it far harder for Allied codebreakers to break.

Codebreaking Success: Breaking the Lorenz cipher had to be crucial for Allied intelligence. It was British mathematician and computer scientist Bill Tutte, along with his Bletchley Park team, who succeeded in cracking this system. Known as the "Tunny" cryptanalysis, this furnished the Allies with much-needed assistance in issuing intercepts on the high level of German military communications.

The Lorenz cipher is a prime example of an extremely secure, or at least at its time, state-of-the-art system, where the depth of effort put forward by Allied cryptanalysts won attempts to break its code. Indeed, the Lorenz-encrypted messages were mainly decrypted because of work done at Bletchley Park, including the development of the Colossus computer, and contributed to the Allied victory in World War II [4].

CipherText:AWPX94SXATGWLN8EAFLYQAMV/TQSH BUGAL/JDFWRZ3TENHBORAVVJH9MIPHG+3WUI4AS YGNTYTLQKABMG+XSOHK4U3ICDCRXUSRAEGEW8 SPH/JMUOHOXG99EAPQEGN3LO9/3KKGZYA9+RKE/G HDCWMA
Key wheel settings:
K-Wheel start position=1
S-Wheel start position=1

5.3. KL-7

The KL-7, otherwise known as ADONIS, was a rotor-based cipher machine in use by the United States military forces and its allies during the Cold War era. It was designed to organize secure communication through the encryption and decryption of messages in the 1950s by the U. S. National Security Agency.

The KL-7 used a set of rotors like those of the Enigma machine, a German cryptographic MONTH machinery, to transform plaintext into ciphertext. It had a highly complex rotor system with several layers of encipherment and afforded a very high degree of cryptographic security [19].

Although very effective, the KL-7 was finally replaced by more advanced electronic encryption technologies like KW-26 and later by computer-based encryption systems. However, the KL-7 played an important role in encrypting military communications throughout the Cold War years and became one of the means toward the goal of safeguarding national security and diplomatic secrecy.

Rotor Settings:
Key: EHFLIAGB
0428041609320811
05100607010803
04342509032714

Cipher Text: TLVVG OWQUK JNVGD IQCWQ KRPXZ MSIQI BBMKC ZNYMW UMCHX CDLBM UOIPC IOMRL OCEXE BOYBL YIIAT EXWTR NMHDZ GGHKR GRHVW FBNCS EBMFZ XBVAQ MJEVZ WKOTB IUMJX RDXVT EHRQJ RNKHG LJYCB UOUWV KSBL

6. Modern Cryptology

6.1. Public Key encryption

In this scenario, there are two different keys for encryption and decryption. Encryption key is public and everybody can access where as decryption key is kept secret and only intended person uses this for decrypting the key.

Public Key: The very term says that this key has to be public. The public key is accessible to all and thus can be further used.
Use in Encryption: The basic usage of the public key is encryption of data. If a sender wishes to convey confidential

information to the receiver, he/ she applies the public key of the receiver to encrypt his message [20].

Use in Digital Signature Verification: The public key also is used for verifying whether a message or document has originated from a particular sender. If the sender digitally signs a document with his private key, then it is easily verifiable with the sender's public key that indeed it has come from him and also that it remains unchanged.

Private Key: This password must be private and known only to the owner. It has to be very cautiously guarded since it is the lifeline to the security of the system [21].

Decryption: When encrypting using a receiver's public key to encipher a message, it could only be deciphered using a receiver's private key. This would mean that if someone interceded and intercepted the encrypted message, he could not read the message without using his private key.

Digital signatures: The digital signature is also produced with a private key. If the owner of the private key has signed the message or document, then authenticity of that message is proved. Anyone can validate the signature utilizing the corresponding public key linked with it that it is original and, at no point of time, has got manipulated.

6.2. Private Key encryption

In this scenario, only one secret key will be used for encryption and decryption. There are two types of ciphers: stream cipher and block ciphers. There are different approaches for designing block ciphers like Substitution-Permutation-Network, Fiestel Structure [25, 26], etc.

Examples for private key encryption: The Data Encryption Standard, popularly known as DES, 2DES and Triple DES, also known as 3DES, AES, RC4.

6.3. Light weight Cryptology

ARX: They belong to a family of encryption algorithms, which-as their name indicates-use "Addition, Rotation, and XOR" in different combinations to generate encryption or hashing. In contrast, the classic block ciphers based on substitution-permutation networks are made much simpler in ARX ciphers [22].

The design philosophy of ARX focuses on efficiency, simplicity, and strength against some forms of cryptanalytic attacks. ARX ciphers use only three addition, rotation, and XOR operations, trying to strike a balance between security and performance. Being bit-wise, these operations are pretty suitable for implementation in either hardware or software under simple logic.

One of those ARX ciphers is Salsa20-a stream cipher that generates a stream of pseudo-random bits by successions of addition, rotation, and XOR. Generally, ARX ciphers are particularly applied in situations requiring lightweight, efficient cryptographic solutions such as in resource-constrained or embedded systems.

7. Quantum Cryptology

Quantum Cryptology is also sometimes called Quantum Cryptography or Quantum Key Distribution (QKD) and it is a sub-branch of quantum information science that studies how quantum mechanics can potentially be applied to improve the security of cryptographic systems [27]. Aerial overview:

Principles of Quantum Mechanics: Such wellsprings of quantum mechanics are harnessed by quantum cryptology to provide cryptographic protocols resistant in theory to attack, in particular, classical computing-based.
Quantum Key Distribution (QKD): Quantum key distribution is the primary application of quantum cryptology. Two users can share a common secret key with the security absolutely assured by quantum mechanics. Since any eavesdropping with a quantum communication will necessarily introduce detectable disturbances, the parties will become alerted at the possible compromise [28].
Entanglement-based protocols: Some quantum cryptographic protocols are based on the phenomenon of entangled particles, wherein two or more quantum particles become interconnected in such a way that the state of one particle is instantly influenced by the state of the other, however far apart they are. Any change effected within an entangled particle would be noticed by the two communicating parties; hence, this forms the basis of eavesdropping detection [29].
Quantum-Secure Algorithms: Among the central goals of quantum cryptology is to come up with cryptographic algorithms that are both secure against classical as well as quantum attacks irrespective. Post-quantum cryptography has been defined as the branch of classical cryptographic algorithms that are largely safe even against very powerful quantum computers [30].

Some of the issues to be addressed for practical quantum cryptosystems are maintaining quantum coherence over large distances, dealing with noise in the quantum channels, and finally, some may be the limit of technology. Many researchers continue studies on how to overcome these bottlenecks and further advance the field of study.

In fact, up to now, quantum cryptography is still in the development and research phase. But even now, recently, there is some form of substantive progress in the development of the first small-scale quantum key distribution networks that have been put in place. These may serve as a new tier in secure communication for very sensible fields that require integrity and confidentiality.

Quantum cryptology stands at the research frontier that may revolutionize secure communication in the future, especially in an era dominated by quantum computing. It exploits the strange, unique aspects of quantum mechanics for cryptographic systems with advanced guarantee security properties.

8. Post Quantum Cryptology

Post-quantum cryptography, or PQC, are the cryptographic algorithms that promise to be secure even against attacks from quantum computers. Quantum computers differ from classical computers in the respect that they are currently made to perform calculations much more efficiently by using quantum phenomena such as superposition and entanglement from quantum mechanics on specially chosen types of problems. Thus, many of the cryptosystems now in use threaten to be broken, especially those based on public-key cryptography [31].

Below is the explanation of post-quantum cryptography and why it is necessary:
post-quantum cryptography required:
They depend on problems proven to be hard for a classical computer, like integer factorization and discrete logarithms, although quantum algorithms like Shor's algorithm can compute these in polynomial time; therefore, such cryptosystems are also vulnerable.

Quantum Risk: Once it is feasible to build large-scale quantum computers, nothing prevents such computers from breaking current classical systems. Any data encrypted today using RSA or ECC, for example, if captured and stored, can be broken in the future when a quantum computer exists.

Post-Quantum Cryptographic Algorithms: The future-proofing of cryptography is achieved by coming up with new algorithms that resist quantum attacks. Thus, the data will be secure even with future developments in quantum computing.
Post-quantum cryptography is the area of several types of cryptographic algorithms intended to be secure against quantum computers. The major variants include the following:

Lattice-Based Cryptography: It deals with the hardness of lattice problems, such as the Shortest Vector Problem or Learning with Errors, to construct secure schemes of encryption. Examples involve the NTRU encryption algorithm and LWE-based cryptographic constructions [32].
Code-Based Cryptography: Its turnstile based on the hardness of decoding random linear codes. Among the most representative examples are the McEliece cryptosystem and its various variants [33].
Multivariate Quadratic Equations: This one is based on the hardness of solving systems of multivariate quadratic equations over finite fields. One of the most prominent examples is HFE, Hidden Field Equations, and Rainbow [34].
Hash-Based Cryptography: It is based on cryptographic hash functions and provides security. The schemes belonging to this are the one-time signature schemes, the Lamport signature, stateful schemes, and the Merkle signature scheme [35].

Isogeny-Based Cryptography: It is based upon the hardness of computing isogenies between elliptic curves. One of its popular representatives is called the Super singular Isogeny Key Exchange or SIKE [36].

Symmetric-Key Cryptography: Not strictly post-quantum, symmetric-key cryptographic algorithms, like AES, are expected to withstand a quantum attack if the key sizes are large enough. In any event, even the best Grover's algorithm can provide a quadratic speedup; hence, doubling the length of the key should be sufficient to withstand quantum threats [37].
Hybrid Schemes: Proper pairing of the classical cryptographic methods with the post-quantum algorithms gives a way to transition, and security against both the classical and the quantum threats is assured [38].

All these types use various problems and mathematical principles to find their quantum resistance, hence offering a variety of tools in the digital information safeguarding pursuit from quantum computing.

Applications of Post-Quantum Cryptography
Any region where long-term security is a concern will require post-quantum cryptography, including but not limited to:
Internet communications (HTTPS, VPNs): Current internet encryption uses public-key cryptography, and all of them will be broken by quantum attacks.

Digital signatures will prove the authenticity and integrity of updated software, documents and communications. These should be quantum-safe against tampering.

Blockchain: Most blockchain-based solutions, including Bitcoin and Ethereum, depend on the security offered by ECC. To maintain the security of blockchain technologies after the advent of quantum computers, post-quantum alternatives of ECC will be needed [39].

IoT: The devices in this category have very limited computational capabilities and, thus need more effective quantum-resistant algorithms to secure their data [40].

Challenges in Adopting Post-Quantum Cryptography
Performance: Most post-quantum algorithms require more computational resources compared to their classical counterparts. For example, public key operations in post-quantum algorithms may be slower or more expansive in terms of keys, which would pose a non-friendly user interface for devices as minimalist as IoT.

Transition: The transition from a classical cryptography system to a post-quantum cryptography system will be an infrastructure and protocol-to-protocol changeover. Hence, the transition should be planned with utmost care to ensure both compatibility and security of the network.

Hybrid Cryptosystems: Most of the systems will be hybrid systems, where both classical and post-quantum algorithms are merged together that assure if one is broken with the advent of a future quantum computer, the other is still secure.

9. Technology based Evaluation

Spy radio sets: Spy radio sets or clandestine or covert radio transmitters have been an essential tool for intelligence

operations over the course of the 20th century and up to present times. Such devices allowed spies and resistance fighters to secretly communicate with their handlers or headquarters, often from behind enemy lines. Here's a summary of spy radio sets and their technological evolution:
Historical Context-World War II

Well post-World War II, the spy radio sets were in widespread use in espionage agencies of both sides of the Iron Curtain - British Special Operations Executive (SOE) type, the American Office of Strategic Services (OSS) type, and the Soviet NKVD.
Well-known models are the British B2 radio set, the American SSTR-1, and the German Enigma, though the latter was more of a cipher gadget than an example of a spy radio.
Cold War: In the Cold War era, however, these were still considered very important tools in espionage work, particularly within agencies such as CIA and the KGB.
Technology: These were now available in compact forms, more sophisticated, and harder to detect. Miniaturization and encryption allowed improvement of security and efficiency.
Key Features and Technologies-Compact Design: These spy radio sets were highly convenient in design and easy to conceal. As a matter of fact, for it to not fall into capture, it was often stashed in one's everyday object like suitcases, typewriters, or household appliances.

Encryption and Coding: The communications broadcast by spy radios were typically encrypted, so their contents could not fall into enemy hands. A wide variety of cipher techniques were used to encode these communications, including one-time pads and mechanical machines such as the Enigma.
Frequency Agility: Another typical feature mounted on these spy radios was frequency agility, which allowed operators to switch between frequencies to avoid enemy detection and jamming.
Power Sources: Early models were powered by battery packs; later models made use of more efficient power sources, such as rechargeable batteries and portable generators.
Transmission and Reception: Most spy radio sets broadcasted on short wave frequencies, which allowed waves to cover vast areas. This made it possible for agents to transmit signals to their control from anywhere in the world-even a place that would be considered remote or hostile.
Legendary Spy Radio Sets
B2 (British): The B2 was used by SOE agents during the Second World War. The B2 was small and compact enough to fit inside a small suitcase. It played a critical role in coordinating resistance efforts against the Axis occupation of Europe.

SSTR-1 (American): The OSS designed the portable, shortwave transmitter-receiver SSTR-1 for secret communications in several theatres of operation.
American: The RS-6 miniaturized, portable radio set during the Cold War contained an easy disguise and minimalistic setup to prepare for operation.
Soviet: The R-350M is a radio set designed during the Cold War by the KGB and other Soviet intelligence organizations. It is well known for its reliability and compactness.

Modern Use and Evolution
Digital Technology: Digital technology has transformed the spy radios into ones that are constantly updating sophisticated devices able to accept secure digital communications. Some of these features include satellite phones and encrypted digital radios.
Steganography: Most of the modern devices use steganography, which is the secret writes of a message within another type of digital file not to be noticed.
Cyber Espionage: Following the rising of cyber espionage techniques, modem spy radio sets have been kicked out by encrypted e-mails, secure messaging applications, among other high-level hacking capabilities.
Impact and Legacy: Historical Influence: Spy radio sets were heavily involved in many intelligences works, contributing to the successes of a number of military and political efforts.
Technological Advancement: The invention of the devices spurred the development of radio technology, encryption, as well as portable electronic breakthroughs.
Modern Spying: The idea of spy radio sets influences modern spying tools and techniques as it proposes the requirement for security of communication in intelligence affairs.
Spy radio transmitters have been a cornerstone part of spy history, progressing through the years from very simple transmitters to those developed, secure communicating devices that have shaped the field of intelligence and still influence modern spy craft.

However, in order to assess all the classical, machine-based, modern, quantum, and post-quantum cryptography along with the transistor technology, it is indeed important to understand the dynamics of how the association between the cryptographic method and the hardware advancement goes along with time. It is, indeed, transistor technology that made very complex algorithms operational on these modern devices quite efficiently. This shall study the association of such cryptographic paradigms with the physical implementations over a wide range of transistor technologies starting from traditional silicon-based to Fin-FETs and even stretching on to quantum transistors.

9.1. Classical Cryptography and Transistor Technology
Classical Cryptography: Based on elementary forms of cryptography, such as the Caesar cipher, Vigenère cipher, and the Enigma machine developed during World War II. These were not transistor-based computer-based implementations but hand- or electromechanical-based.
Relation with Transistor Technology: Minimum Number of Transistors: Majority of the classical cryptographic algorithms were developed well before the contemporary computation. Their construction was not inherently dependent on the number of transistors but easily implemented in early computers when transistor technology emerged.
Vacuum Tubes to Transistors: Transistor technology began to materialize in the 1950s and 1960s, which considerably

boosted the computing power. This improved the automation and perfection of classical ciphers.
Hardware: Classical encryption schemes that result in machine-based cryptography were implemented on early transistor-based computers, such as the IBM 1401.
Performance: Classical ciphers are relatively lightweight, and they can even be implemented on primitive transistor-based systems due to their low computational complexity.
Security: At present, classical ciphers are insecure against modern computers and cryptanalysis methods.

9.2. Machine-Based Cryptography and Transistor Technology

This involves machine-based cryptography, which is the development of algorithms based on electronic machinery from the early 20th century: mechanical developments of ciphers like the Enigma machine and early computation algorithms. Link with transistor technology
Transistorized Computing: It was quite feasible to design complex encryption algorithms and machines, which would enable calculations at highly rapid speeds, with the advent of transistors. With transistor technology and integration of circuits in almost gigantic dimensions came the possibility of computational cryptography.
Hardware Acceleration: The outcomes of advanced improvements in transistor density besides the development of integrated circuits were the cryptographic co-processors in which these cryptographic computations were made independent by the computer's processor.
Transistor Scaling: As per the Moore's Law, the size of the transistors was scaled down; cryptographic algorithms are much complex but at higher speeds due to an increased speed and low power dissipation of the contemporary processors.
Cryptographic Innovations: As a result of the improved computing abilities because of the transistor-based hardware, DES-like algorithms have become feasible.

9.3. Modern Cryptography and Transistor Design

Modern Cryptography This includes the cryptosystems designed during the period following the 1970s. It is broadly encompassing AES, DES, RSA, ECC, hash functions [41].
Correlation with Transistor Technology: Microprocessors and ICs: Transistor scaling of microprocessors has been continued since their invention. It is now taking a microprocessor from tens of thousands in early microprocessors to billions in modern microprocessors. This means modern cryptographic algorithms can be implemented very efficiently on general-purpose CPUs, GPUs, and specialized cryptographic hardware.
Hardware Security Modules (HSMs): Modern transistors were allowed to implement HSMs for safe storage of keys and other cryptographic operation [42]

9.3.1. Hardware Implementations

AES (Advanced Encryption Standard): The algorithm has been largely implemented in the processors with dedicated instructions, such as AES-NI within Intel processors. There is much hardware acceleration of the AES performance due to strong dependence on S-box lookups and bitwise operations [43].
ECC: Efficiently with regard to key size versus RSA and consumes fewer computational resources, which bestows great importance for IoT and low power devices.
TPMs: Makes use of fresh transistor technology; because of this, it becomes possible to implement cryptography functions directly in hardware design for securing key storage and operations.
Evaluation:
Transistor Scaling: Actually, this was one of the primary motivators for high performance crypto operations with very low power usage and enabled modern crypto algorithms to be everywhere applied in all embedded systems, mobile devices, and data centres.
Security: Modern cryptography is resistant to all known classical attacks, but is susceptible to quantum attacks. This resulted in the emerging post-quantum cryptographic solutions.

9.4. Quantum Cryptography and Transistor Technology

Quantum Cryptography: Principles for secure communication borrowed from quantum mechanics. Quantum key distribution, the most promising application, is one where any attempt to intercept the channel of communication itself will reveal it [44]. Relation with Transistor Technology:
Quantum vs. Classical Transistors: The quantum cryptography, specifically QKD, functions in an entirely different plane compared to the classical transistor technology. Of course, with absolutely no classical transistors at all, QKD uses quantum devices made of quantum optical systems and single-photon detectors.
Quantum Processors: For quantum cryptography future applications, we will have to face the fact of using quantum transistors or qubits-quantum bits-for secure operations against both the classical and quantum attacks [45].
Analysis: Transistor Incompatibility: Standard silicon-based transistors cannot be directly applied in quantum cryptographic protocols since the latter operates on a completely different level of principles and principals involved, which include entanglement and superposition.
QKD Application: QKD devices lack most of the characteristics of standard transistor-based systems, though new research into semiconductors and materials may help bridge this difference.

9.5. Post-Quantum Cryptography and Transistor Technology

Post-Quantum Cryptography: Cryptographic algorithms designed to be post-quantum secure, yet they keep running efficiently on classical computing hardware. Examples include lattice-based cryptography, hash-based signatures, code-based cryptography, and many more [46].
Association with Transistor Technologies: Classical Hardware Compatibility: Contrary to quantum cryptography, PQC algorithms do not need quantum processors but can run on classical transistor-based hardware like modern microprocessors and FPGAs.

Performance on Advanced Processors: Most PQC algorithms require larger keys and more complex computations in many cases, say matrix multiplications. This

may further increase the demand for more powerful transistor-based hardware like multi-core CPUs, GPUs, or ASICs tailored for these particular operations.
Examples of Hardware Instantiations: Lattice-Based Cryptography: These are algorithms including Kyber and Di lithium that involve immense quantities of matrix computations. It uses SIMD capabilities from modern processors to allow parallel computation.
FPGA Implementations: Using the cutting-edge transistor technology, the FPGAs have been utilized as the means for prototyping post-quantum algorithms. For high-performance operation in IoT as well as embedded systems, the PQC algorithms such as McEliece have been implemented on the FPGAs.
Transistor Efficiency: Even though PQC can be implemented on the present transistor-based technology, the higher sizes of the keys and the increased complexity impose greater demands on processing power, memory, and energy efficiency. Therefore, further optimization of these algorithms will be highly dependent on future transistor technologies like FinFETs and nano-transistors.
Scalability: If quantum computing becomes more dangerous, then people would look into post-quantum-efficient solutions that could practically implement PQC algorithms within constrained environments, thereby propelling semiconductor technologies forward.

10. Devices based evaluation

Analyzing classical cryptography, machine-based cryptography, modern cryptography, quantum cryptography, and post-quantum cryptography through the lens of devices charts the course along which cryptographic methods developed in step with developing technology by using various devices that implement these cryptosystems.
The next section provides an overview of various implementations of different cryptographic paradigms by devices and continues to late-stage quantum devices and post-quantum secure hardware.

10.1. Classical Cryptography and Devices

Classical Cryptography This is the form of the cryptographic systems used before the time computers came into existence, traditionally hand or mechanical. Among the most famous ciphers are Caesar cipher, Vigenère cipher, and the Enigma machine [47].

Example ciphers like the Caesar were performed manually or with simple mechanical tools, such as cipher wheels or books.
Enigma Machine: The most classic example for the machines of cryptography in classical cryptography is the Enigma machine, which was a machine concerning a mechanical cipher used by the Germans during WWII. The rotating rotors and plugboards carried out very complex encryption in the Enigma machine.
Lorenz Cipher: Another electrical circuit-based cryptography machine used during WWII, employing rotors, for encrypting messages.

10.2. Machine-Based Cryptography and Devices

Machine-Based Cryptography: This was an era of cryptographic algorithms which started becoming automatic and processed on electronic computing machines. In this era of machine-based cryptography, the following equipment was used,

Equipment:
IBM 1401 : It was one of the earliest general-purpose computers and was used in initial machine-based cryptographic operations. It automated the processes of encryption and decryption.
Colossus: One of the earliest electronic computers ever constructed; a machine that the British code breakers used during World War II to crack the Lorenz cipher. Colossus is one of the first vacuum tube devices, precursors to the transistors.
SIGABA: It was an American cipher machine that encrypted military communications using electrical components.
Appraisal:
Speed: Electronic machines made processes much faster in encrypting and decrypting than when mechanical machines were used.
Security: Much more secure than the classical cryptographic devices, though early computers were not powerful enough in their first phases, so that complexity of algorithms was limited by them.

10.3. Introduction of Cryptography and Computers

Introductory Cryptography: This one relates to the crypto systems that were invented in the later half of the 20th century. It contains symmetric-key algorithms, that is, AES and DES, and public key cryptography, such as RSA and ECC. All these might not have been possible without the innovation that created the transistor-based computing devices.

Devices:
Microprocessors: The invention of silicon-based transistors led to the embedding of encryption algorithms like AES and RSA within general-purpose CPUs. These processors contained millions of transistors and used complex mathematical functions for encryption and decryption [48].
Smartcards: Applications, such as credit cards and ID cards, make use of the device smartcard and comprise in-built microcontrollers which perform operations as cryptographic algorithms like RSA for digital signatures or AES for secure transactions [49]
Hardware Security Module: This module securely generates, stores, and manages cryptographic keys and carries out other kinds of cryptographic operations. It is something large industries such as the financial and government sectors have as staple for cryptographic processes [50].
TPMs (Trusted Platform Modules): TPMs are hardware-based cryptographic modules embedded in the modern computers; hence, this allows for secure storage of the key and maintains the system in integrity [51].
Performance: Modern algorithms are computed very efficiently on today's processors and hardware accelerators. For instance, AES-NI enabled processors can include cryptographic functions that are hardware-accelerated and therefore offer much better performance.

Security: Modern cryptography like RSA and ECC has been proven to be robust against classical computing threats. However, with the approach of quantum computing, modern cryptographic methods, especially public-key algorithms, face vulnerability to quantum attacks.

10.4. Quantum Cryptography and Devices

Quantum Cryptography: It uses principles from quantum mechanics for secure communication. The best example is Quantum Key Distribution, meaning any form of eavesdropping over the communication channel would be detectable [52].

Quantum key devices: ID Qu antique's Cerberis^3 and Toshiba's QKD system, both are quantum optical systems that allow secure photonic transfer of encryption keys with embedded in-built single-photon detectors and quantum random number generators [53].

QRNGs: These are appliances that generate random numbers based on the effect of quantum, for example, the quantum random number generator module by ID Quantique [54]. Cryptography fundamentally relies on randomness and devices based on quantum ensure highly entropy-rich keys.

Quantum Networks: Quantum cryptography is usually applied in dedicated networks for fiber optics. An example is China's quantum satellite Micius that so far has provided evidence of secure communication based on QKD over long distances [55].

Quantum computers: It will definitely compromise classical cryptography but is eventually going to be used for quantum cryptography. IBM and Google are manufacturing quantum processors in which one day, secure quantum algorithms will be placed. Meanwhile, compact quantum computers are being developed by D-Wave Systems, Inc. for practical purposes [56].

Efficiency: Quantum cryptographic devices are several orders slower and more resource-intensive than classical cryptographic devices. However, they offer security guarantees no technology based on laws of physics could violate.

Security: QKD is theoretically unbreakable because any attempt at eavesdropping would disturb the quantum state and alert the parties to the fact that an interception was taking place. However, distance and speed are a problem in practical implementations.

10.5. Post-Quantum Cryptography and Devices

Post-Quantum Cryptography (PQC): Normally refers to those cryptographic algorithms which are quantum computer attack-resistant. The known schemes include lattice-based, hash-based, and multivariate polynomial schemes that could be designed to operate efficiently on classical computers but resist the quantum attacks [57].

Devices:

Classical Microprocessors and FPGAs: Most post-quantum cryptographic algorithms can be mapped on today's chips, including the highest-end Intel processors, and FPGA-based cryptographic accelerators. For instance, lattice-based cryptography already runs on FPGAs. Their flexibility and hardware performance make them very efficient for such applications [58].

Internet of Things devices: This is likely to be one of the favourite honeypots for quantum-based attacks in the near future. Hence, tremendous focus is given today toward the development of lightweight post-quantum cryptographic solutions meant for resource-constrained devices such as sensors, smart devices, and embedded systems.

Cryptographic Hardware: The cryptographic hardware available already has post-quantum algorithms implemented. Examples of updated hardware that support the post-quantum algorithm are HSMs and TPMs. For instance, YubiHSM 2 is hardware whose PQC algorithms will be upgraded when standardized [59].

Hybrid Cryptosystems: Most of the communication devices have hybrid cryptosystems. Hybrid cryptosystems are applied such that the security is ensured based on the existing standards until the widespread adoption of quantum-proof standards.

Efficiency: In general, the post-quantum cryptographic algorithms and schemes have been designed to resist quantum attacks, while in most cases they produce longer keys and increase the complexity of computations much more dramatically than the classical counterparts. Probably, to achieve the efficiency of implementing such PQC algorithms, even stronger processors or a use of specialized hardware accelerators will be required.

Security: Post-quantum cryptography aims at mitigating the threats arising from quantum computers and therefore guarantees security for long-term digitized communication. The appliances that adopt PQC in addition turn out to become quantum attack-proofed, hence imperative in securing the post-quantum era.

11. Conclusion

This paper briefly indicates how technology is assessed, and in security devices, the assessment also happens through cipher text generation with a key. Classical cryptography to the quantum machine to post-quantum algorithm cryptography with technology, mechanical rotor machines, electrical rotor machines, microprocessors, microcontrollers, FPGAs, SoCs-all embedded boards, and quantum machines. Evaluation with all crypto evaluation.

Classical Cryptography was applied on manual and mechanical appliances such as the Enigma machine which was non-computational but set the ground for the applications that are currently in use of cryptography. Machine-Based Cryptography introduced devices such as Colossus and the

early IBM computers, which mechanized cryptographic operations and accelerated the process of encrypting, Modern Cryptography depends on microprocessors, HSMs, TPMs, and smartcards where the exponential increase in the number of transistors with processing is used to realize comprehensive secure communications. Quantum Cryptography uses specific quantum devices such as QKD systems and quantum random number generators almost much earlier than what technology would have been able to provide in the previous past. This post-quantum cryptography can be executed on classical computing platforms but is limited when trying to optimize performance on CPUs, FPGAs, even more embedded devices due to the size and complexity of keys for quantum-resistant security. Cryptography has evolved along with devices and technology; hence, in the quantum computing world, the future of cryptography will be in an efficient hybrid approach between the classical and the post-quantum approaches for guaranteed security.

In future, one can focus on design and development of cryptographic algorithms be implemented on Quantum computers. Cryptanalysis of quantum crypto-algorithms using emerging technologies like Artificial Intelligence and Machine Learning.

Conflict of Interest

Authors have NO affiliations with or involvement in any organization or entity with any financial interest, or non-financial interest in the subject matter or materials discussed in this manuscript.

Funding source: This research work was conducted without any external funding.

Author's contribution: Conceptualization, resources gathering, methodology done by Sriramudu, Writing, modifying, reviewing done by Nagendar Yerukala, Validation and formatting done by G Padmavathi, and over all support for article is done by Neelima Guntupalli.

Acknowledgment: We acknowledge Dr. Vankataraman, Director of AIMSCS, Dr. U Yugandhar, CE(BD), AIMSCS and Prof. Gangadhar, ANU, GUNTUR for their support and encouragement towards completion of this PhD work.

References

[1] Dooley, John F. "History of cryptography and cryptanalysis." History of Computing, **2018.**

[2] Risman, Risman. "*Comparison of Performance Rot13 and Caesar Cipher Method for Registration Database of Vessels Berthed at PT Samudera Indonesia*." International Journal of Basic and Applied Science Vol.**10**, Issue.**3**, pp.**91-98, 2021.**

[3] Balamurugan, Chithralekha, et al. "*post-quantum and code-based cryptography—some prospective research directions.*" Cryptography Vol. **5**, Issue.**4**, pp.**38, 2021.**

[4] Soofi, Aized Amin, Irfan Riaz, and Umair Rasheed. "*An enhanced Vigenere cipher for data security.*" Int. J. Sci. Technol. Res Vol. **5**, Issue.**3**, pp.**141-145, 2016.**

[5] Clody, Michael C. "*Deciphering the language of nature: Cryptography, secrecy, and alterity in Francis Bacon*." Configurations Vol. **19**, Issue.**1**, pp.**117-142, 2011.**

[6] Mudgal, Piyush Kumar, et al. "Application of genetic algorithm in cryptanalysis of mono-alphabetic substitution cipher." 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE, **2017.**

[7] Banerjee, Amit, Mahamudul Hasan, and Him Kafle. "Secure cryptosystem using randomized rail fence cipher for mobile devices." Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 2. Springer International Publishing, **2019.**

[8] Arroyo, Jan Carlo T., Cristina E. Dumdumaya, and Allemar Jhone P. Delima. "*Polybius square in cryptography: a brief review of literature.*" International Journal Vol. **9**, Issue.**3**, **2020**.

[9] Lasry, George, et al. "*Deciphering ADFGVX messages from the eastern front of world war I.*" Cryptologia 41.2 (**2017**): **101-136.**

[10] Machiavelo, António, and Rogério Reis. "*Automated Ciphertext—Only Cryptanalysis of the Bifid Cipher.*" Cryptologia Vol. **31**, Issue.**2**, pp.**112-124, 2007**

[11] Arroyo, Jan Carlo T., and Allemar Jhone P. Delima. "*A Modified Nihilist Cipher Based on XOR Operation.*" International Journal Vol. **9**, Issue.**3, 2020.**

[12] Mihaljević, Miodrag, and Frédérique Oggier. "A wire-tap approach to enhance security in communication systems using the encoding-encryption paradigm." 2010 17th International Conference on Telecommunications. IEEE, **2010.**

[13] Sari, Rita Novita, et al. "Implementation of Trifid Cipher Algorithm in Securing Data." 2019 7th International Conference on Cyber and IT Service Management (CITSM). Vol. **7**. IEEE, **2019.**

[14] Hu, Zhichen, et al. "Analysis and implementation of the enigma machine." 2022 International Conference on Big Data, Information and Computer Network (BDICN). IEEE, **2022.**

[15] Lasry, George, Nils Kopal, and Arno Wacker. "*Ciphertext-only cryptanalysis of Hagelin M-209 pins and lugs.*" Cryptologia Vol. **40**, Issue.**2**, pp.**141-176, 2016**

[16] Bart Wessel, "The Hagelin Cryptographers C-52 and CX-52 Crypto Museum", 24 February **2021**.

[17] Lee, Michael. Cryptanalysis of the SIGABA. Diss. University of California, Santa Barbara, **2003**.

[18] Davies, Donald W. "*The Lorenz cipher machine SZ42*." Cryptologia Vol. **19**, Issue.**1**, pp.**39-61, 1995**.

[19] "TSEC/KL-7 Canadian User Report After First Year of Operation National Security Agency (NSA)". CSEC **115**. 1 May **1959**, **15** pages. SECRET, **1959.**

[20] Hellman, Martin E. "An overview of public key cryptography." IEEE Communications Magazine Vol.**40**, Issue.**5**, pp.42-49, **2002**.

[21] Bellare, Mihir, and Bennet Yee. "Forward-security in private-key cryptography." Topics in Cryptology—CT-RSA 2003: The Cryptographers' Track at the RSA Conference 2003 San Francisco, CA, USA, April 13–17, 2003 Proceedings. Springer Berlin Heidelberg, **2003.**

[22] Biryukov, Alex, and Vesselin Velichkov. "Automatic search for differential trails in ARX ciphers." Topics in Cryptology–CT-RSA 2014: The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February **25-28**, **2014**. Proceedings. Springer International Publishing, **2014**.

[23] Dalmasso, Loic, et al. "Evaluation of SPN-based lightweight crypto-ciphers." IEEE Access **7**, pp**.10559-10567, 2019.**

[24] Sajadieh, Mahdi, et al. "Recursive diffusion layers for block ciphers and hash functions." Fast Software Encryption: 19th International Workshop, FSE 2012, Washington, DC, USA, March **19-21, 2012.** Revised Selected Papers. Springer Berlin Heidelberg, **2012.**

[25] Ramanujam, Sriram, and Marimuthu Karuppiah. "*Designing an algorithm with high avalanche effect.*" IJCSNS International Journal of Computer Science and Network Security Vol. **11**, No.**1**, pp.**106-111, 2011.**

[26] Feng, Jingya, and Lang Li. "*SCENERY: a lightweight block cipher based on Feistel structure."* Frontiers of Computer Science Vol. **16**, Issue.**3**, pp.**163813, 2022**.

[27] Lo, Hoi-Kwong. "*Quantum cryptology." Introduction to quantum computation and information*. pp**.76-119, 1998.**

[28] Scarani, Valerio, et al. "*The security of practical quantum key distribution.*" Reviews of modern physics Vol. **18**, Issue.**3**, pp.**1301-1350**, **2009**.

[29] Pirker, Alexander, and Wolfgang Dür. "*A quantum network stack and protocols for reliable entanglement-based networks.*" New Journal of Physics Vol. **21**, No.**1**, pp.**033003, 2019.**

[30] Alagic, Gorjan, and Alexander Russell. "Quantum-secure symmetric-

key cryptography based on hidden shifts." Annual international conference on the theory and applications of cryptographic techniques. Cham: Springer International Publishing, **2017**.
[31] Bernstein, Daniel J., and Tanja Lange. "*Post-quantum cryptography.*" Nature Vol. **549**, No. **7671**, pp.**188-194**, **2017**.
[32] Nejatollahi, Hamid, et al. "*post-quantum lattice-based cryptography implementations: A survey.*" ACM Computing Surveys (CSUR) Vol. **51**, No. **6**, pp.**1-41**, **2019**.
[33] Balamurugan, Chithralekha, et al. "*post-quantum and code-based cryptography—some prospective research directions*." Cryptography Vol. **5**, No. **4**, pp**. 38**, **2021**.
[34] Benadjila, Ryad, Thibauld Feneuil, and Matthieu Rivain. "MQ on my mind: Post-quantum signatures from the non-structured multivariate quadratic problem." 2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P). IEEE, **2024.**
[35] Noel, Moses Dogonyaro, et al. "*Review and analysis of classical algorithms and hash-based post-quantum algorithm.*" Journal of Reliable Intelligent Environments pp**. 1-18**, **2021.**
[36] Peng, Cong, et al. "*Isogeny-based cryptography: a promising post-quantum technique.*" IT Professional Vol.**21**, No.**6**, pp**.27-32**, **2019.**
[37] Wang, Liu-Jun, et al. "*Experimental authentication of quantum key distribution with post-quantum cryptography.*" npj quantum information Vol. **7**, No.**1**, pp**.67**, **2021.**
[38] Giron, Alexandre Augusto, Ricardo Custódio, and Francisco Rodríguez-Henríquez. "*Post-quantum hybrid key exchange: a systematic mapping study*." Journal of Cryptographic Engineering Vol.**13**, No.**1**, pp**.71-88**, **2023.**
[39] Zheng, Zibin, et al. "*Blockchain challenges and opportunities: A survey.*" International journal of web and grid services Vol.**14**, No.**4**, pp**.352-375**, **2018.**
[40] Madakam, Somayya, Ramya Ramaswamy, and Siddharth Tripathi. "*Internet of Things (IoT): A literature review.*" Journal of Computer and Communications Vol.**3**, No.**5**, pp**.164-173**, **2015.**
[41] Kong, Jia Hao, Li-Minn Ang, and Kah Phooi Seng. "*A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments.*" Journal of Network and Computer Applications Vol.**49**, pp**.15-50**, **2015**.
[42] Mavrovouniotis, Stathis, and Mick Ganley. "*Hardware security modules.*" Secure Smart Embedded Devices, Platforms and Applications. New York, NY: Springer New York, **2013**. Pp.**383-405**, **2013.**
[43] Sriramudu, Nalla Venu, Dharavath Narendar and G. Padmavathi. "Model for capturing noise free traces for Side Channel Power Cryptanalysis based on SAKURA-G FPGA and Case study of AES." 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC). IEEE, **2022**.
[44] Goldman, Jeremy. "Quantum cryptography—Current methods and technology. Tech". Rep, **2014.**
[45] Vozhakov, Vsevolod A., et al. "**State control in superconducting quantum processors.**" Phys.-Uspekhi, Vol.**65**, pp**.457-476**, **2022**.
[46] Kumari, Swati, et al. "*Post‐quantum cryptography techniques for secure communication in resource‐constrained Internet of Things devices: A comprehensive survey."* Software: Practice and Experience Vol.**52**, No.**10**, pp**.2047-2076**, **2022.**
[47] Vaudenay, Serge. "*A classical introduction to cryptography: Applications for communications security*". Springer Science & Business Media, **2005**.
[48] Hutter, Michael, and Erich Wenger. "Fast multi-precision multiplication for public-key cryptography on embedded microprocessors." Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13. Springer Berlin Heidelberg, **2011**.
[49] Malina, Lukas, et al. "Assessment of cryptography support and security on programmable smart cards." 2018 41st International Conference on Telecommunications and Signal Processing (TSP). IEEE, **2018**.
[50] Hupp, William, et al. "Module-OT: A hardware security module for operational technology." 2020 IEEE Texas Power and Energy Conference (TPEC). IEEE, **2020.**
[51] Osborn, Justin D., and David C. Challener. "*Trusted platform module evolution.*" Johns Hopkins APL Technical Digest (Applied Physics Laboratory) Vol.**32**, No.**2**, pp**.536-543**, **2013**.
[52] Xu, Feihu, et al. "*Quantum cryptography with realistic devices.*" arXiv preprint arXiv, Vol.**1903**, No. **09051**,**2019**.
[53] Zapatero, Víctor, et al. "*Advances in device-independent quantum key distribution.*" npj quantum information, Vol.**9**, No.**1**, pp**.10**, **2023.**
[54] Saini, Anish, Athanasios Tsokanos, and Raimund Kirner. "*Quantum randomness in cryptography—a survey of cryptosystems, RNG-based ciphers, and QRNGs*." Information Vol.**13**, No.**8**, pp**.358, 2022**.
[55] Wei, Shi‐Hai, et al. "*Towards real‐world quantum networks: a review.*" Laser & Photonics Reviews Vol.**16**, No.**3**, pp**.2100219**, **2022.**
[56] Zhou, Yiqing, E. Miles Stoudenmire, and Xavier Waintal. "*What limits the simulation of quantum computers?*" Physical Review X Vol.**10**, No.**4**, pp**.041038**, **2020.**
[57] Roy, Kumar Sekhar, and Hemanta Kumar Kalita. "*A survey on post-quantum cryptography for constrained devices."* International Journal of Applied Engineering Research Vol.**14**, No.**11**, pp**.2608-2615, 2019.**
[58] Li, He, et al. "FPGA accelerated post-quantum cryptography." IEEE Transactions on Nanotechnology Vol.**21**, pp**.685-691**, **2022.**
[59] Marzougui, Soundes, and Juliane Krämer. "Post-quantum cryptography in embedded systems." Proceedings of the 14th International Conference on Availability, Reliability and Security. **2019**.

AUTHORS PROFILE

Sriramudu working as a researcher in C R Rao AIMSCS and Pursing Ph.D. in Acharya Nagarjuna University, Guntur. He earned his M. Tech., in VLSI System Design from JNTU Hyderabad 2015. His filed of interest is Cryptography and cryptanalysis and especially in Side channel cryptanalysis.

G.Padmavathi is working as an assistant professor in CRRAOAIMSCS, Hyderabad. She received gold medal in M.Sc. (Maths) from Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. Awarded Ph.D. in Mathematics from JNTUH University, Hyderabad. She has published research papers in reputed international and national journals and conferences, including IEEE and they're also available online. She holds one Indian patent publication derived from her research. She has 20 years of combined experience in teaching & Research. Her main research interest includes Cryptology, Machine learning, Modelling and Analysis.

Nagendar Yerukala is presently working as Research Scientist in CRRAO AIMSCS, Hyderabad. He obtained Ph.D(CSE) from JNTUH Hyderabad. He did his M.Tech from NITK surathkal and M.Sc from Kakatiya university. His areas of interest are Network security and Cryptology.

Neelima Guntupalli is an Assistant Professor working in the Department of Computer Science and Engineering, ANU College of Science, Acharya Nagarjuna University. She got a Ph.D. in Computer Science and Engineering (in the field of cryptography and network security). Her research areas include cryptography, cloud computing, and machine learning.

