Understanding the Mathematical Principles Behind Encryption and Decryption Algorithms, and Their Applications in Modern Communication and Security

1.Ameer Hasan Almuqdadi
Department of Mathematics, Faculty of Mathematics and Computer Science, University of Kufa, Iraq. Email: ameerh.almuqdadi@student.uokufa.edu.iq.
Tel: 009647815559878

2. Adil AL-Rammahi
Department of Mathematics, Faculty of Mathematics and Computer Science, University of Kufa, Iraq.
Email: adilm.hasan@uokufa.edu.iq
Tel: 009647803742806

ABSTRACT

In our world, cybercrime abounds, Specialists uses many methods to defend security of network, as there are several ways of trying to hack it.
The importance of mathematics lies in the domain of cybersecurity. One can see the strength of the current mathematical apparatus in information and Internet protection. Solving problems of security technologies such as averting cyber-attacks, secure cryptography, and risks are analyzed using different sections of math.

Keywords:

Introduction

With the increasing complexity in the world of technology, information and network security has become one of the biggest challenges facing companies and society. Cyber-attacks can lead to data harm or maybe loss, Privacy and integrity data violations and damage to business line and reputation. Cyber security assurance has become a highly important task for companies, organizations and society. Consequently, there is a need for tools that help protect data from cyber-attacks [1]. Mathematics algorithms are very important lines that can avoid hazards and hacker attack.

Cryptography: All of cyber-security and information and network security are fall under cryptography science. It uses mathematics to encrypt internet connections and keep systems safe from undesirable hackers, while making sure that entitled users have the permission they need.
Cryptography use simple math and extremely advanced one too. The domain of high-level engineers usually use more advanced encryption; they design and emend advanced algorithms that keep systems secure.

The History of mathematics in cryptography:

Although modern cryptographic mathematics is more different from which it was in the past, it still built on the same concepts used in old times.

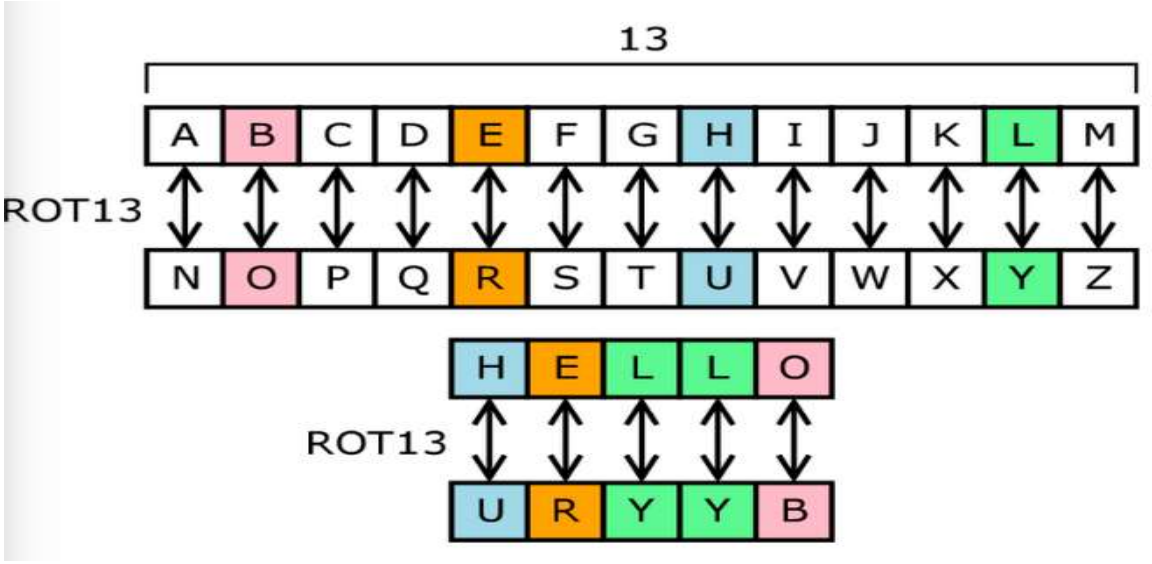
The earliest known cases of cryptography found in the hieroglyphics engraved into a tone from the Old Kingdom of Egypt, it is dating back to 1900 BCE. While historians do not believe that

the message was meant to be intricate, it was still intended to be interesting and entertaining to solve instead.

In Mesopotamian There are clay tablets, dating back to 1500 BCE, they were supposed to have ciphers to stash a pottery glaze recipe, as they were likely to be of commercial and specific value to the vendor.

Perhaps the use of monoalphabetic alternate ciphers was the most famous ancient cryptography source that as far as 400 BC in India, when Mlecchita vikalpa was explained "art of writing in a cypher" which documented of the Kama Sutra, which was known as the lovers' communication.

Cryptography has greatly advanced in the last 100 years. You've probably seen simple ciphers, such as cipher of Caesar, also called the shift cipher. ROT13 is one of the most common types of shift ciphers, which means that the alphabet shifts "13" times as this figure below:



Anyway, Caesar cipher is not the type of the mathematical encryption that can defend data in these days. The newest technologies are mostly used to defend personal and sensitive important financial information as it is transmitted carefully over the internet. However, all types of data must be stored securely and kept private from those who wish to sell it or use it fraudulently. Preserving this data unharmed depends on cyber security.

Mathematics departments:

Math is one of the main tools used to ensure cyber security.

There are different sections of mathematics used to protect detailed data and personal info:

1. **The theory of numbers**: is about studying the properties of numbers and mathematical operations used in encryption to keep data safe.

Generally, the base types of cryptographic closure, such as encryption and data encoding. Up-to-date cryptography includes four main divisions: symmetric cryptosystems, electronic signature systems, the keys of controlling systems and public keys cryptosystems. Cryptographic methods divided into two categories:

- **Encryption:** processing information by replacing and transposing characters, in which the size of the data doesn't change;
- **Encoding:** compression of information by replacing individual combinations of letters, words or phrases [2].

Cryptography is the most important part of all information systems, ensuring accountability, clarity, accuracy and exclusiveness. It prevents fraud attempts in e-commerce and gives financial transactions legal force. Cryptography helps identity you and ensures anonymity. It prevents hooligans from hacking into the server and does not allow competitors to access confidential documents. In the future, even trade and communications will become more and more linked to

computing networks; encryption will become vital [1].

**** Binary Number Theory:**

Is the language of math that uses only "0" and "1" values in together, binary math operates everything a computer does, from generating and routing IP addresses to running a client operating system security.

**** Complex Numbers:**

Complex numbers appear in various cyber security operations. A complex number is a term includes the real number part and the imaginary part "with letter i". The "i" number is the square root of the number /-1/, because the mathematic principles do not allow this number existence.

2. **Algebra**: Algebraic structures used in cryptography such as groups, loops, and fields, they can help creating cryptographic the set of rules "protocols" and cipher encryption systems that ensure the security of data transmitted over the internet. Algebraic structures can support to create cryptographic systems. For instance, to exchange keys the Diffie-Hellman protocol uses groups, RSA uses loops and fields to encrypt and decrypt data. Moreover, algebra can identify potential vulnerabilities and attacks by analyze cryptographic protocols and cryptographic systems in order [3].

Algebraic techniques can help identify likely ways to attack cryptographic systems and help increase their security.

Computer programming uses Boolean algebra widely. Which describes logical actions using two values, "true" (symbolized by the digit 0) and "false" (symbolized by the digit 1). Boolean algebra handles these values using the logical functions "AND" and "OR".

Boolean doesn't involve any numerical calculations unlike other forms of algebra. The answer is clearly "yes" or "no," which is why they are so helpful in computer coding.

Consequently, algebra in cyber security is an important section of math that maintains information and data security and helps avert probable cyber-attacks [2].

3. **Probability Theory:** For evaluating the strength of cipher protocols and cipher systems, probability and probability distributions used by cryptography science.

A specialist should have skills for:

- Calculate the probability of an event using combinatorial rules and formulas.
- Apply the basic formulas of probability theory (formulas of addition and product of probabilities, full probability, limit theorems, Bayes, Bernoulli…).
- Find the numerical properties and distributions of random variables.
- Build a state graph of the Markov process; calculate marginal probabilities and other properties of the Markov chain.
- Construction of a geometrical personification of the variable chain and its experimental distribution function.
- Calculate speculation of the factors of distributions of random variables based on the results of a statistical test.
- Apply standards of the simplest statistics [4, pages 55-60].

4. **Information Theory**: studying of entropy information complexity and other concepts that used in cryptography to define the power of cryptographic systems encryption and protocols. Info theory, also named the mathematical theory of communication, it focuses on the study of data transmission, processing of data , and measurement of information. The authors of this theory were Claude Shannon and Warren Weaver, it published in 1940. The sender and the receiver represent the basis of his theory [4]. As they mentioned, the message flows from the sending entity to the receiving one by a chosen channel for this communication process. This theory places particular emphasis on the study and measurement of information, as well as the evaluation of existing communication systems for optimal transmission of these information data.

The necessity of info theory in cybersecurity

It essentially used for:

- Lets the study of salient aspects of the info operation. For example, channels

of communication or understanding of transmitted data.

- Attempts to identify elements that might corrupt the message or stop it from reaching the recipient effectively. It should be note that it is important for the recipient to be able to absorb the content coming from the sender.
- Analyzes the speed of sending messages and their encoding and decoding time.
- Its main objective is to identify the most economical, simple and effective way to deliver a message without changing it during the process [5].

5. **Compatibility:** cryptography used the study of permutations and combinations for creating cipher protocols and cipher schemes. Compatibility is about counting things as permutations and combinations, geometry, limited configurations, and chart theory. Compatibility considered part of discrete math, but in a separate primary math course, there is time only for basic concepts [4, p 5 to 15].
6. **Discrete Mathematics:** The study of discrete elements as graphs and sequences, which used in cryptography to create cryptographic protocols and systems. Discrete math is a branch of mathematics that agrees with separable and distinct numbers. Includes sets, graph theory, and Booleans, and numbers can be limit or unlimited.

Although there are no hard and fast explanations of discrete math, it is well known for the ever-changing quantities and all excludes things related. Discrete math is commonly associated with computer science and is vital to electronic devices. It used for developing software and when all the elements under study are separated from each other. This includes all limited math and the integers study [6]. Discrete math doesn't consider anything to do with continuity, and it leaves out a lot of geometry and mathematical analysis. Boolean and predicate logic can considered parts of discrete mathematics because there are only two values: true and false. However, there is a lot of logic involved, and it makes sense to see a lot of mathematical logic as beyond discrete mathematics. The study of finite sets belong to discrete math discrete because this sets are discrete, but advanced set theory should reflected as a separate subject with connections to the logic of math.

7. **Matrix:**

The matrix defined as a specific arrangement of numbers in the form of columns and rows. Matrixes usually written in the form of a square or rectangular box. The vertical line inside the matrix is called the column, while the horizontal line is called the row, and the size of the matrix can be expressed through the number of rows, and the columns it contains as follows: Matrix size: number of rows x number of columns [7]. Matrixes are used in encryption in order to scramble data for security purposes to encrypt and decrypt data that we need. There is a key helps in encrypting and decrypting the data, it generated by the arrays.

Understanding Cryptography Mathematics

Cryptographic mathematics - This refers to the use of mathematical techniques to encrypt the plaintext with hash functions and perform cryptanalysis to determine the original text from the cipher keys.

Terms of Mathematical Cryptography

Some important terms are essential to understanding how cryptographic mathematics works and the role algorithms play in modern cryptography.

The Importance of Keys in Crypto Algorithms

Keys in cryptography are as a secret number (PIN), password, or pattern. It works similar to a physical key with any safe or security door lock. If the attacker can discover that key, it is probably you don't have the up-to-dated algorithms to keep your system safe, and they

were able cracking the key, which indicates poor encryption.

It is also important for system administrators to take notes about keys and how to keep it safe. Even with the latest technology, attacker sand hackers often get into security vaults simply by studying and understanding how to use and save keys after spending time inside your system [8]. As we see, the management of keys is very important as creating them.

Classes of Cryptographic Algorithms

The math of the algorithm changes depending on the class of the algorithm. With digital cryptography, it is easier than ever to create an algorithm, but not all of them are as robust as other algorithms. There are more elaborated methods with unique mathematical inputs within these categories of algorithms.

The classes of Encryption include:

- Symmetric
- Asymmetric
- Hash Functions

Symmetric Encryption

The main functions of a symmetric encryption algorithm contain:

- ✓ Achieve confidentiality through encryption and decryption, which done using just a single key.
- ✓ Authenticates integrity and sources by using Message Authentication Codes (MAC), which automatically generated and validated by the same key.
- ✓ Generates virtual random numbers.

Before getting ahead of ourselves, we should discuss how we look at *encryption* for mathematical cryptography. Moreover, encryption and decryption go hand in hand. They are usually meant to describe making a message absolutely meaningless to all those without authorized access. If you can decrypt a message, you are a highly skilled cryptanalyst, or it could just be that your encryption was not that strong.

In order for appropriately and securely use encryption to protect data; we need a key made up of ciphertext.

With symmetric encryption, the equal key is used to encrypt and decrypt the message. In present cryptography, that may look like this string of Ruby and OpenSSL code:

```ruby
require 'openssl'
require 'pry'

data_to_encrypt = 'now you can read me!'

cipher = OpenSSL::Cipher.new('aes256')
cipher.encrypt

key = cipher.random_key
iv  = cipher.random_iv

data_to_encrypt = cipher.update(data_to_encrypt) + cipher.final

binding.pry
true
```

Here we reassign the variable that involved the original string of raw data. This shows exactly how we are able to encrypt and decrypt data.

You can see how this data encrypted by looking at in Pry console for Ruby:

```
[14:28:59] encryption
// ♥ ruby symmetric.rb

From: /Users/chris-dev/Development/code/encryption/symmetric.rb @ line 15 :

    10: iv  = cipher.random_iv
    11:
    12: data_to_encrypt = cipher.update(data_to_encrypt) + cipher.final
    13:
    14: binding.pry
 => 15: true

[1] pry(main)> data_to_encrypt
=> "1\xFF\xA9\xD5\xC1\x94q\v\xC8y\xBA\x13/e\xE1\x96\xDC\xE5\xF5z[A\xDB\x10\xE5+\
xD5\xA8\aq\xD4?"
[2] pry(main)>
```

Here we can see how moving from *data_to_encrypting* variable, which was formerly showing “now you can read me!” is an enigmatic string of gobbledygook.

The decrypting process:

```
From: /Users/chris-dev/Development/code/encryption/symmetric.rb @ line 15 :

    10: iv  = cipher.random_iv
    11:
    12: data_to_encrypt = cipher.update(data_to_encrypt) + cipher.final
    13:
    14: binding.pry
 => 15: true

[1] pry(main)> data_to_encrypt
=> "1\xFF\xA9\xD5\xC1\x94q\v\xC8y\xBA\x13/e\xE1\x96\xDC\xE5\xF5z[A\xDB\x10\xE5+\
xD5\xA8\aq\xD4?"
[2] pry(main)> cipher.decrypt
=> #<OpenSSL::Cipher:0x007fbe25a58710>
[3] pry(main)> cipher.iv = iv
=> "\xDD\xDB\xEE\xFEUCj\x94\xAA&\t\x1A\x1F\xCE\xAF\x93"
[4] pry(main)> cipher.key = key
=> "\xEA\x97|m\t\xAF#\xD2\xEF\xA8\xDC</\x97\xA2U'\xF9\x98W\xDA\x8A\xC8o\x01Q\x10
h\x87\xC6\\\xEC"
[5] pry(main)> data_to_encrypt = cipher.update(data_to_encrypt) + cipher.final
=> "now you can read me!"
[6] pry(main)>
```

We will see the original message when you use the same key for encryption.

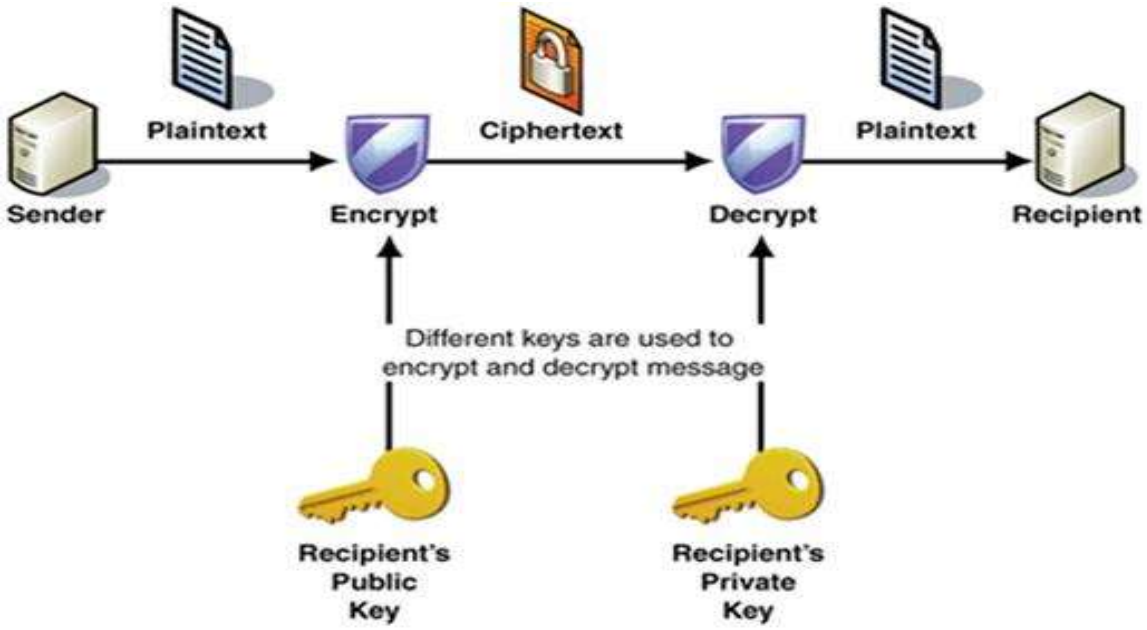
Asymmetric Encryption

An important point of cryptography used in cryptocurrency is using key that used to encrypt and decrypt a message, it is required to send to open up a protected connection. Therefore, that means we must send the key across an unprotected connection, which means that the key maybe intercepted all its way and used by a third party. To solute that, you need to use the asymmetric encryption algorithms.

It also called a *public key encryption*. The algorithms use two keys that are mathematically similar, but they used for not

the same purposes. These known as public or private keys. The first used for data encryption, and the second key decrypts the data. The owner never reveals the private key.

As shown in the following Figure sending entity uses the recipient's public key to convert plaintext to ciphertext. The ciphertext sent and the receiving entity using its private key to recover the plaintext. (Decrypting the message, document, etc.) can only opened by the person who has private key corresponding to the public key. It works for the reason that the two keys, although separate, are intertwined with mathematics.



Anyway, everyone have the access because of the public key can spread to the public. Moreover, the private key is set up in such a way that it cannot be deduced once the public key known.

Integer factorization, discrete logarithmic and other problems are mathematical problems; they are generally used asymmetric key algorithms. These can make digital signatures and establish session keys to provide communications security over the network as TLS protocol.

Feature / Algorithm	Hash	Symmetric	Asymmetric
No. of Keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used	SHA	AES	RSA
Key Management/Sharing	N/A	Big issue	Easy & Secure
Effect of Key compromise	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384 or SHA-512	AES, Blowfish, Serpent, Twofish, 3DES, and RC4	RSA, DSA, ECC, Diffie-Hellman

Using Asymmetric and Symmetric Algorithms at the same time

Many in data security believe that the best algorithms take a double-headed way by using a hybrid from asymmetric and symmetric algorithms. In most cases, Ciphers for asymmetric algorithms use for ID authentication, which is carried out through digital signatures and certifications. It can also used for the distribution of symmetric

encryption keys in bulk, as well as non-repudiation services and key agreement.

Specific Algorithms in Cryptography Mathematics

Big-O-Notation

Determined by an entry O(n), O denotes the order of n, and this notation is a way of indicating the number of arithmetic operations required to perform it.

Prime Factorization

It is a common technique in mathematics, which uses the multiplication of two large prime numbers to secure a cryptographic system using public keys.

Pseudo Random Number Generation

It used to generate a random number series. However, unlike similar devices, they do not generate truly random numbers. They used because of their rapidity.

The Birthday Problem

This is a visualization of how likely it is that many people in a group will have the same date of birth. This concept has adopted to explain the possibility of other phenomena occurring.

RSA Algorithm

It is the most widely known asymmetric algorithms and used. It also serves as the essential tools for biometric Cryptography. This takes the biometrics model even further within cryptographic principles. The RSA algorithm started from the RSA Data Corporation, whose name derived from Ron Rivest, Leonard Adelman, and Ali Shamir.

You must study the power of prime numbers to understand the RSA Algorithm. As these are central to this algorithm's function. The RSA algorithm uses prime numbers to generate public and private keys, and the keys must be larger to accommodate copious amounts of data and information.

Alternatively, in RSA, the encryption handled by symmetric algorithms for the private key and then goes through further encryption to generate a public key, which then used by the sending entity.

When the public key received, the private key, which has created through the symmetric algorithm, then decrypted. Now, the public key originally generated by the RSA algorithm used to decrypt the rest of the message.

The Diffie-Hellman Algorithm

In short DH Algorithm. Although, DH is important for data security, it actually not used for encryption of the factual ciphertext. Alternatively, the main goal for this algorithm is to find a solution to send the public key and private key packet over a secure channel.

Here is a systematic look at the Diffie-Hellman algorithms:

1. . The receiver acquires the generated public key and private key, but is automatically generated by the DH algorithm
2. The sender receives the public key generated by the receiver, thus using the Diffie-Hellman algorithm to create another section of public keys that only generated on a temporary basis.
3. The ownership of the new temporary private and public keys is taken by The sender, as we see, they were sent by the receiver.
4. The key of session can mathematically reveal itself when the receiver finally gets the cipher text message from the sender
5. Now the receiver can decrypt the remnant of the ciphertext message.

Hash Function

Hash functions build all elements of modern cryptography. They're the mason bricks of all algorithms, they can be applied to switch unordered size data into a small string of fixed-size. Then the resulted data can be termed as "the hash value" or "digest". The basic process of these functions works without any key to run. It works simply in a one direction case. Therefore, it is unattainable to detect the input from the output.

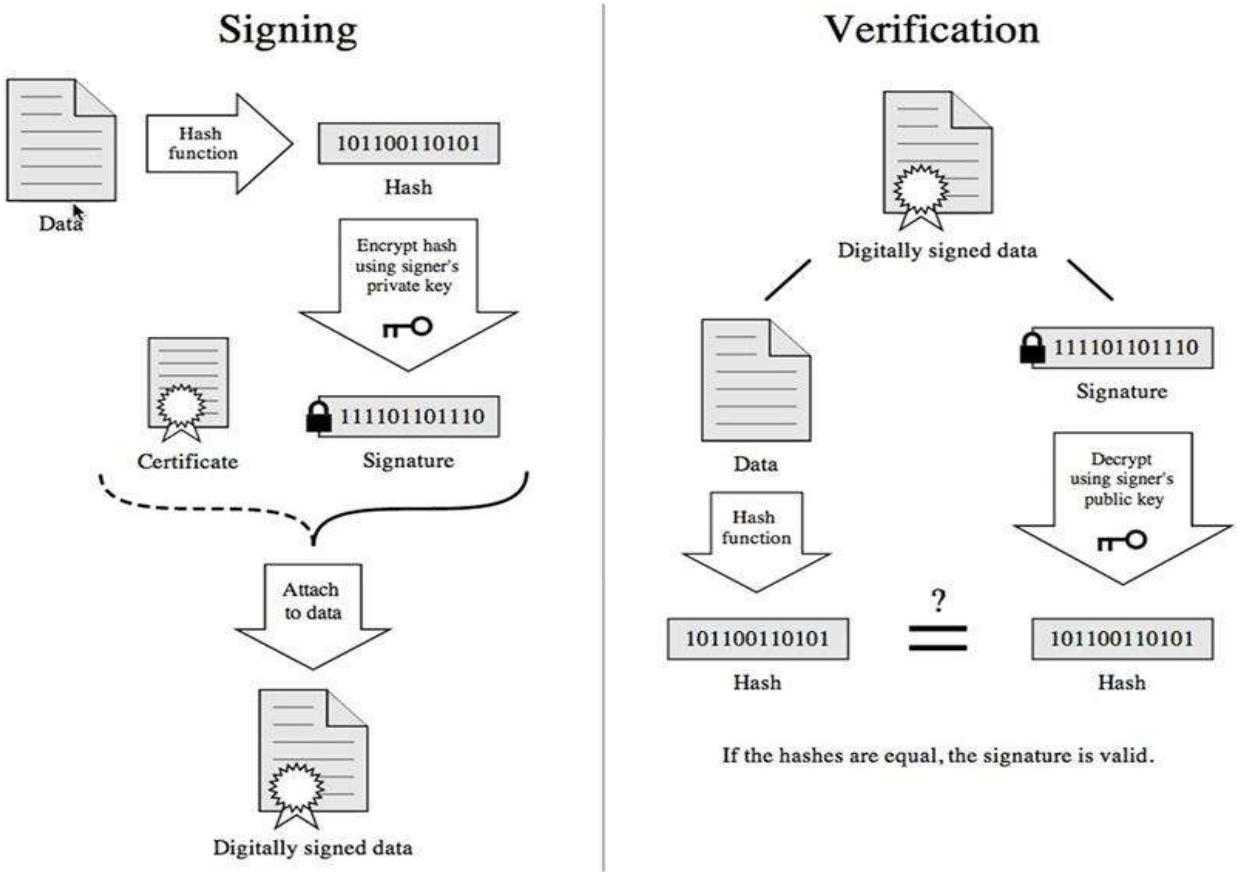
We can use hash functions for these following actions:

- Digital signatures: generating and verifying.
- Checksum and message integrity assurance
- Source integrity services (By MAC)

- Deduce subkeys into key- generation algorithms and protocols
- Pseudo-random numbers generation

Digital signatures

Although not really encryption, the asymmetric keys has another usage: electronic signatures or as known: (Digital signatures). If Bob wants to empower verification that he truly sent a message, he can certainly sign it.



Referring to the chart. Bob's private key used by signature process, because he is the single person who has it [8]. The private key is used while processing the message body through the hash function. A hash is a fixed-length value that appears the content of message. The hash value changes when the content changes. Moreover, the hacker cannot use the hash value to access plaintext.

When Bana gets Bob's message, she can verify that the message came from Bob and has not altered: if She has Bob's public key. She rehashes the message text using Bob's public key. If the hash values match together, here they have a valid signature, and the data arrived to Bana unaltered.

If hash values don't equal, the message text altered or the key used to generate the signature hash value is not Bob's key. In some cases, the public key might not be Bob's. If hacker, Eve, is able to persuade Bana that a fake certificate she sends to her is Bob's key, Eve can send signed messages using a fake "Bob" key that Bana will verify. The recipient must ensure that the public key used in this operation is valid [9].

The use of mathematics in cybersecurity

Cyber security can be a dream job for an analytical, tech-inclined person. It is probable to grow by a whopping 38% from 2023 to 2033 that will add thousands of jobs every year. These careers often reward six-figure wages.

Computer and communication security attracts many new experts and career changers, but it can be a daunting prospect, especially when it comes to math.

Data Encryption Mechanism

The data that needs to encrypt is termed plaintext or clear text. The plain text has to express through some encryption algorithm, which essentially mathematical calculations performer on the primary information. Several encryption algorithms vary by application and security index.

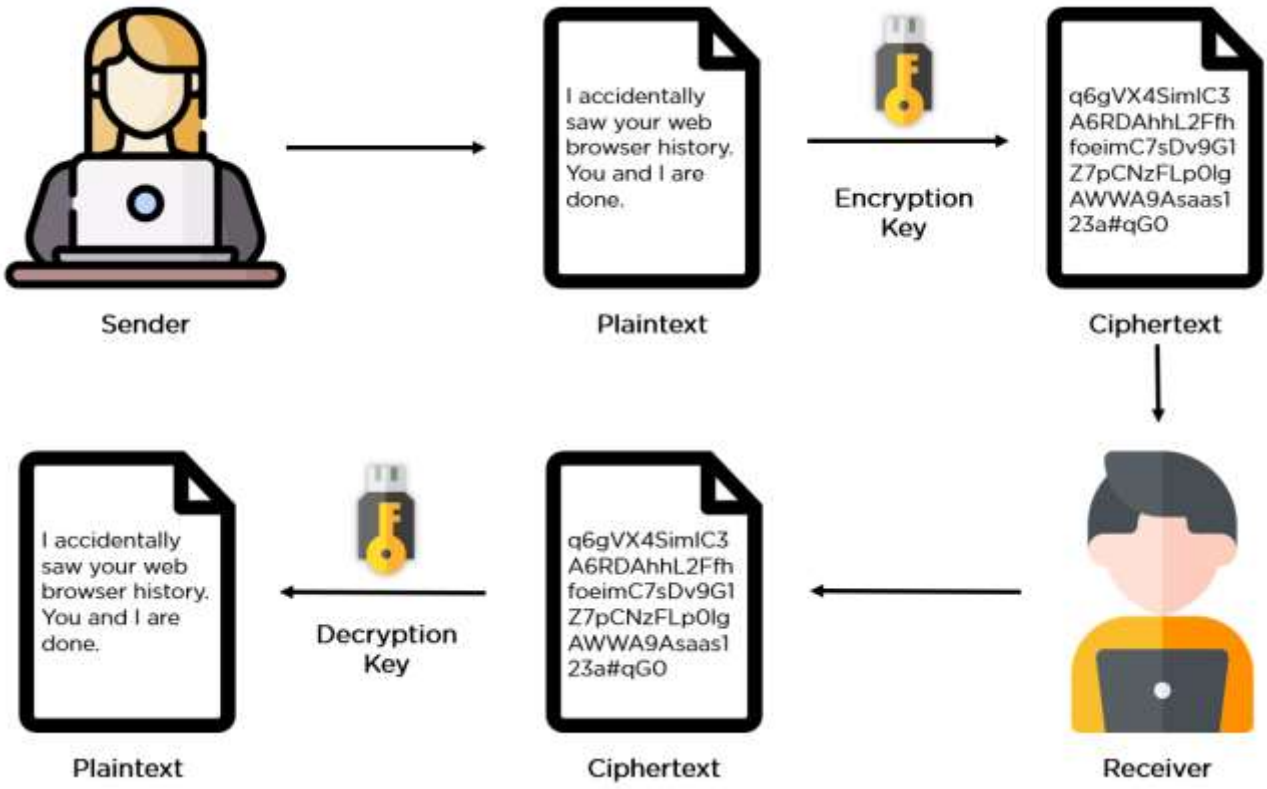
Away from them, a person also needs an encryption key. Also needs an encryption key and a convenient encryption algorithm, the plaintext is transformed into the encrypted piece of data "cipher text". Rather of sending plain text to the receiver, cipher text sent over unsecured communication channels.

When the cipher text arrives the meant receiver, receiver can use a decryption key to transform the cipher text back to the original clear format i.e. plain text. This decryption key must be kept secret always, and may or may not be the same as the first key that used to encrypt the message.

Understanding the work process with the flowing example:

When a girl wants to send her partner a special text, so she encrypts it using specific application that mixes data into unreadable nonsense. Then she sends the message out, and her partner, will use the correct de-cryption to return it readable text.

And so on, it explained by this chart:



Happily, the keys do all the actual encryption/decryption work in complete privacy.

Conclusion

Technology evolves rapidly. Over time, computer based technological developments have revolutionized how we react with the world that would have been unimaginable just a few short decades ago.

The algorithms generated through cryptography are compound and unparalleled. While they absolutely deal with key creation and use, mathematics is mainly important for determining how keys will behave between sending entity and receiving entity. The algorithms also guarantee that the cipher text unreadable unless the keys are used precisely specified by the neutralization. So authenticating by two-factor, digital signatures, and email messages need so much protection.

References

1. Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019). MATHEMATICAL METHODS IN CYBER SECURITY: FRACTALS AND THEIR APPLICATIONS IN INFORMATION AND CYBER SECURITY.
2. Cybersecurity: Education, Science, Technique, (5), 31–39. URL: https://doi.org/10.28925/2663-4023.2019.5.3139
3. Панасенко С.П., Захист інформації в комп'ютерних мережах // Журнал«Світ ПК»2002 року No2.
4. Ковальчук М. В Методи сучасної криптографії URL: https://kovalchukmm14.wordpress.com/2014/12/16/rsa-
5. %D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC/
6. 4. C. McMullen. (2011). Probability Theory , Course Notes — Harvard University — 2011 and Rading, pages 55-60.
7. Dr.Bill Young Department of Computer Sciences,University of Texas at Austin (2020).Information Theory and Rading, pages
8. 18-22.URL: https://www.cs.utexas.edu/~byoung/cs361/slides4-info-theory.pdf
9. Discrete Mathematics Tutorial URL: https://www.geeksforgeeks.org/discrete-mathematics-tutorial/
10. What Is Data Encryption: Types, Algorithms, Techniques and Methods By Simplilearn 2023 URL: https://www.simplilearn.com/data-encryption-methods-article
11. Guide to Cryptography Mathematics Privacy Canada Toronto, Ontario. Canada URL: https://privacycanada.net/mathematics/
12. The role of cryptography in information security 2012 by Tom Olzak https://resources.infosecinstitute.com/topic/role-of-cryptography/