Sri Lanka Institute of Information Technology

Mini Research Paper

Group Assignment

IE3082 - Cryptography

Submitted by:

Student Registration Number	Student Name
IT20028046	Gunathilaka S.B.M.B.S. A
IT19108100	Herath H.M.C.S.B
IT20045258	Abeywickrama J.A.S.T
IT20166656	Seneviratne S.M.N.H

Date of submission
11th of October 2022

Cryptographic approaches for secure communication

Gunathilaka S.B.M.B.S.A
IT20028046
It20028046@my.sliit.lk
SLIIT- cyber security (undergraduate)
Student at the Sri Lanka Institute of Information Technology

Herath H.M.C.S.B
IT19108100
it19108100@my.sliit.lk
SLIIT- cyber security (undergraduate)
Student at the Sri Lanka Institute of Information Technology

Seneviratne S.M.N.H
IT20166656
it20166656@my.sliit.lk
SLIIT- cyber security (undergraduate)
Student at the Sri Lanka Institute of Information Technology

Abeywickrama J.A.S.T
IT20045258
It20045258@my.sliit.lk
SLIIT- cyber security (undergraduate)
Student at the Sri Lanka Institute of Information Technology

***Abstract*— In the past several years, there have been significant advancements in cryptographic algorithms. In order to strengthen the security of the internet and make it a safer location to handle sensitive information, cryptographic services were created. Once users started using these programs, researchers were able to spot problems with them. We will discover how cryptographic encryption works for secure communication from this essay and what kinds of developments to expect in the future.**

Keywords—algorithms, communication, cryptographic, encryption, information, internet, researchers, sensitive

I. Introduction

Cryptography is a means of securing information and communications by using codes to ensure that only those who are supposed to read and use the information may do so. Cryptography is a term used in computer science to describe secure information and communication systems built from mathematical principles and a set of rule-based computations known as algorithms. These deterministic algorithms are utilized for digital signature, data privacy protection, credit card transactions, and communications including email and online surfing [16]. Cryptography gives the necessary communications protection and secures the channel's data from malicious attackers. Modern cryptography is concerned with the four goals listed below:

- Confidentiality- The knowledge is incomprehensible to anyone who was not supposed to receive it.
- Integrity - The information cannot be changed while in storage or transit between the sender and the intended receiver without being discovered.
- Non-repudiation- The information's creator/sender cannot later disavow their intentions in creating or transmitting the information.
- Authentication - The sender and recipient can validate their identities as well as the origin/destination of the information.

A. *Types of cryptographic techniques*

1) Symmetric-key Cryptography: Both the sender and the recipient use the same key. The transmitter uses this key to encrypt plaintext and send it to the recipient as cipher text. The receiver, on the other hand, uses the same key to decode the message and retrieve the plain text [16].

2) The most innovative concept in the last 300-400 years is public-key cryptography. Two related keys (public and private key) are utilized in public-key cryptography. The public key can be freely transmitted, but the paired private key must be kept hidden. The public key is used for encryption, and the private key is used for decryption [16].

3) This algorithm does not utilize a key. A fixed-length hash value is produced based on the plain text, making it difficult to reconstruct the plain text's contents. Many operating systems employ hash methods to secure passwords [16].

B. *What issues does cryptography address?*

Cryptography can secure the integrity of data both in transit and at rest. It can also authenticate senders and receivers and guard against repudiation. When utilized effectively, crypto can assist to give these guarantees when conversations take place across untrustworthy networks.

An attacker using passive assaults simply listens on a network segment and attempts to read important information as it travels. Passive assaults can be conducted online (with an attacker reading traffic in real time) or offline (an attacker simply captures traffic and views it later). An active attack involves an attacker impersonating a client or server, intercepting messages in transit, and examining and/or changing the contents before forwarding them to their intended destination.

Encryption may be used to safeguard sensitive information in a variety of ways. It can give people confidence that they are talking with the systems they are utilizing. Data on portable disks or in databases can also be encrypted to prevent sensitive data from being disclosed if the physical media is lost or stolen.

C. History

If we get the word Cryptography, it brings a meaning like hiding something. This work is cryptography made from two words. crypt means something protected or vault, and graphy means writing. Even though we have some clues from a few historical places, it is considered the origin happened in 2000 BC from Egyptian hieroglyphics. It means a massive amount of complex pictures, and historiographers believe few elites only knew the meaning of those pictures [17]. Then we can find a tremendous cryptographic application from 100 BC created by Julius Caesar to communicate with his officers securely.to make it, he used the roman alphabet and developed a cryptosystem to replace each character with another character three positions ahead of that character. We call this a Caesar cipher. Nowadays, cryptography is used in battlegrounds and most other areas, so mathematicians and scientists are together trying to find new approaches. The reason war and businesses use cryptography is that they know their success relies on their communications. So they try to protect their communication channels using cryptography [18]. In many countries, governments implemented some restrictions to protect their valuable information by stopping the public dissemination of developed cryptosystems and mathematical concepts that they are using. But it does not have that many effects on people because online communities let people learn the techniques and knowledge of cryptography, and the very famous cryptosystems are developed with the help of the public domain.

II. Importance of cryptography

It now functions as a unified layer of protection for all digital transformation projects that are now referred to as digital businesses. Cryptography is used to secure transactions and communications, protect personally identifiable information (PII) and other private data, verify identity, prevent document manipulation, and create trust between servers. It is the basis of contemporary security systems. One of the most crucial technologies used by organizations to protect their most valuable asset, data, whether it is at rest or in motion, is cryptography. Data, including personally identifiable information (PII) about customers, employees, intellectual property, company strategies, and other types of secret information, is essential information. As a result, cryptography is an essential component of the infrastructure since it is increasingly necessary to secure sensitive data. Critical infrastructure may become vulnerable if the cryptography is unreliable or disguised. Data leaks get public attention, which damages brands. Organizations must be aware of how cryptography is applied and maintained across the company in the current context. We have shifted a significant percentage of our communication to the internet since its inception. We leave traces of the communication and ourselves along the way since the internet is a communication medium that depends on millions of computers to handle the transfer of the bits of information we share.[8] Outsiders may not be able to learn too much from a single transaction, but since we use the internet so frequently, the sheer volume of information left behind can and will inevitably be combined to identify you. Your personal information could potentially be exposed online. To minimize the amount of information you leave behind, keeping conversation secret is crucial. You effectively conceal the information from sources that are accessible to the general public when you protect your connection. Encryption is typically used to keep communication confidential. Encryption essentially makes your communication invisible to every other machine that the information passes through. Since the data is handled by untrusted computers (remember, anybody can set up a node on the internet), the method encryption keys are shared can potentially be a weak spot. The encryption algorithm affects how safe the encryption is. Three major objectives of cryptography are to provide security. Among these, data integrity comes first. The recipient of the message should be able to tell if the message was tampered with while transmitting messages between two sources. To put it another way, the receiver should be able to tell if a certain section of the message has been altered or not. Authentication is the second objective in keeping communications secure. The recipient of a communication should be able to identify the sender when they get it. Finally, non-repudiation is another goal of cryptography, which states that after a communication is sent, the sender should not be able to deny that they were the original author [8]. These objectives must all be met for cryptography to be successful: integrity, authentication, and nonrepudiation. These objectives are very simple to achieve for communications written in pen on paper since personal signatures offer a way to confirm who the original author is and what they intended. The objectives of cryptography are becoming progressively harder to achieve as we go farther into the era of digital communication.

- Cryptography protects the confidentiality of information
- It ensures the integrity of data
- It assures that the sender or receiver is the right one
- Both sender and receiver are held accountable through non-repudiation
- Cryptography also ensures the availability of data
- Uphold information security with powerful cryptography strategies

III. Public Key Cryptography

Public key cryptography uses two distinct keys to encrypt or sign data, with one of the keys—the public key—being used by everyone. The other key is referred to as the private key. Data encrypted with the public key may only be decrypted with the private key. Because two keys are used instead of just one, public key cryptography is also known as asymmetric cryptography. It is commonly used, especially for TLS/SSL, which makes HTTPS possible. [9]

Most implementations of public key cryptography, also known as public-key encryption and asymmetric encryption, are built on the Rivest-Shamir-Adelman (RSA) Data Security algorithms. In public key cryptography, a public key pair is employed and is connected to an entity that needs to digitally authenticate its identity, sign, or encrypt documents. The corresponding public key is made visible while each private key is kept secret. Data encrypted with the public key may only be decrypted using the corresponding private key. Data exchanged between two communicating parties can be concealed via encryption and decryption thanks to public key cryptography. The sender scrambles or encrypts the data before sending it. The receiver then decrypts or unscrambles the data after receiving it. A third party cannot decrypt the data while it is being sent.

• The capacity to convey data without worrying that the sender would later claim that it was never sent is known as nonrepudiation.

Asymmetric cryptography, often known as public-key cryptography, employs two sets of keys—a public key and a private key—that are mathematically linked but not identical. Each key serves a different purpose, unlike symmetric key algorithms that use the same key for both encryption and decryption. Encryption and decryption are accomplished using the public and private keys, respectively. The calculation of the private key using the public key is computationally impossible. Because of this, private keys may be kept a secret, guaranteeing that only the owners of the private keys can decode material and generate digital signatures, while public keys can be widely distributed, giving users a simple and practical way for encrypting content and authenticating digital signatures. Public keys are kept on digital certificates for safe travel and sharing since they must be transferred yet are too large to be readily memorized. Private keys are just kept in your operating system or program, or on hardware (such a hardware security module or USB token) that has drivers to work with your software or operating system since they are not shared.[10]
The main business applications for public key cryptography are:

- Digital Signature: An individual's public key and private key are used to digitally sign and verify material.
- Encryption: Material is encrypted using a person's public key, and only that person's private key may decrypt the content.

A. Benefits of Public key Encryption

The fundamental advantage of public key cryptography is the improved data security it offers. Because users never need to communicate or divulge their private keys to anybody, public key cryptography continues to be the most secure protocol (over private key cryptography), decreasing the likelihood that cybercriminals would learn a person's secret key during the transfer.
Additionally, public key cryptography offers irrefutable digital signatures. Private key systems demand users to exchange secret keys and maybe even trust third parties for transmission, whereas public key cryptography requires each user to be responsible for safeguarding his or her own private key. With the secret key mechanism, senders may assert that one of the parties engaged in the process compromised the shared secret key.

B. Challenges of Public Key Cryptography

Speed is frequently mentioned as the biggest problem with public key cryptography. The existing public key encryption approach is significantly slower than a number of private key cryptography techniques. Combining public key cryptography with secret key systems to provide the security benefits of the public key system and the speed of the secret (private) key system is one technique to get around this problem. Public key cryptography has additional difficulties since it has historically been vulnerable to attacks involving falsified or hacked certifying authority. Cybercriminals that carry out these attacks choose a public key certificate from the authority that has been hacked, allowing them to pass as almost anybody. This makes it possible for online thieves to link a public key to the name of another users.[11]

C. Characteristics of Public Encryption key

- Private key Because the decryption key cannot be determined with just the encryption key and cryptographic procedure, encryption is crucial.
- A different key might be used for decryption together with either of the two keys (public or private).
- Due to public key cryptosystem, private keys may be kept hidden, guaranteeing that only the owners of the private keys can decode material and produce digital signatures. Public keys can be freely shared, giving users a simple and practical means for encrypting content and validating digital signatures.
- RSA is the most used public-key cryptosystem (Rivest–Shamir–Adleman). The core of RSA is the difficulty in determining the prime factors of a composite number.

D. Components of Public Key Encryption

- Plain text: The message that can be read or understood is this. The Encryption algorithm receives this message as input.
- Cipher Text: The encryption algorithm's output is the cipher text. We can't just take this statement at its value.
- Encryption Algorithm: In order to create encrypted text from plain text, an encryption algorithm is employed.
- Decryption Algorithm: The original plain text is generated once the matching key (a private key or a public key) and the encrypted text are input.
- Public and Privet Key: A private key, sometimes known as a secret key, or a public key, which is known to everyone, are both used for encryption and decryption.

E. Weaknesses of Public key Encryption

- Brute-force attacks can break public key encryption.
- When a user loses his private key, this technique also fails, making public key encryption the most susceptible one.
- Additionally vulnerable to a man-in-the-middle attack is public key encryption. In this attack, a third party can obstruct the exchange of public keys before changing the public keys themselves.
- A "man-in-the-middle attack" is also conceivable if the user private key used to create certificates on servers higher up in the PKI (Public Key Infrastructure) server hierarchy is hacked or unintentionally made public. This renders any subordinate certificates completely unsecure. This is another area where public key encryption falls short.

F. Applications of the public key Encryption

- Encryption and Decryption: Public Key Encryption can be used to maintain confidentiality. Using the recipient's public key, the plain text is encrypted in this. This will guarantee that the cipher text can only be decrypted with the recipient's private key.

- Digital Signature: The goal of a digital signature is to authenticate the sender. In this case, the sender uses his own private key to encrypt the plain text. Because the recipient may only decode the cipher text with the sender's public key, this stage ensures the sender's authentication.[12]

IV. Symmetric Key Cryptography

A. *What is symmetric key*

Information may be encrypted and decrypted using a symmetric key. This implies that the encryption key used to encrypt the data need also be used to decode it. In reality, the keys stand for a shared secret that a group of individuals might use to keep a connection to sensitive information open. One of the primary disadvantages of symmetric key encryption vs public-key encryption is the necessity that both parties have access to the secret key [1].

Encoding data in this manner has been widely utilized in earlier decades to permit covert communication between governments and armies. Symmetric-key cryptography is also known as shared-key cryptography, secret-key cryptography, single-key cryptography, one-key cryptography, and finally private-key cryptography. With this type of encryption, it is obvious that the key must be known by both the sender and the recipient. The distribution of the key is the source of the approach's intricacy.

Typically, symmetric key cryptography techniques are classified as stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and use feedback loop to keep the key changing.

A block cipher gets its name from the fact that it encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will repeatedly encrypt to the same ciphertext while using the same key in a block cipher, but the same plaintext will encrypt to different ciphertext in a stream cipher.

Block ciphers can function in one of various modes, the most common of which are as follows:

- Electronic Codebook (ECB) mode is the most basic application, and the shared key may be used to encrypt the plaintext block to generate a ciphertext block. If two plaintext blocks are identical, they will always generate the same ciphertext block. Despite being the most used mode of block ciphers, it is vulnerable to many brute-force assaults.
- In Cipher Block Chaining (CBC) mode, a feedback mechanism is added to the encryption algorithm. Prior to encryption in CBC, the plaintext is exclusively-ORed (XORed) with the preceding ciphertext block. In this method, two identical blocks of plaintext are not encrypted to the same ciphertext.
- Cipher Feedback (CFB) mode is a self-synchronizing stream cipher block cipher implementation. CFB mode allows data to be encrypted in units smaller than the block size, which is useful in some applications such as interactive terminal input. The ciphertext is decoded at the receiving end, and the additional bits in the block are discarded.
- The Output Feedback (OFB) mode of a block cipher is essentially similar to a synchronous stream cipher. OFB uses an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams to prevent comparable plaintext blocks from generating the same ciphertext block.

B. *The symmetric cipher's basic idea*

When using a symmetric cipher, the parties must quickly disclose the secret key since an unauthorized party to the transmission can prevent this and eavesdrop on subsequent communications. This is a well-known difficulty.

The following are some of the several symmetric cipher principles:

- Plaintext is the genuine, understandable message or information that is sent into the algorithm as input [3].
- The encryption algorithm performs a number of replacements and conversions on the plaintext [3].
- The encryption algorithm also requires the secret key. The key is a value that is independent of the plaintext and the algorithm. The method will generate numerous outputs dependent on the specific key that is being used at the moment. The algorithm's exact replacements and conversions are determined by the key [2].
- Cipher Text, this is the chaotic news that was generated as output. It works with the plaintext and the secret key. Two separate keys will generate two different cipher texts for the same message. The cipher text is an incoherent, seemingly random flow of information [3].
- Decryption algorithm, this is essentially the inverse of the encryption method. It generates the first plaintext from the cipher text and the secret key [3].

The following are the two prerequisites for secure usage of conventional encryption.

- A robust encryption algorithm is necessary. It is an algorithm that is designed in such a way that an opponent who understands the method and has access to one or more cipher texts would be unable to decipher the cipher text or contemplate the key. Even if the opponent had numerous cipher texts in addition to the plaintext, the opponent should be insufficient.
- As a result, the key is transferred to the receiver over an independent secure channel. These chips are widely available and are used in a variety of products. The usage of symmetric encryption, the main security challenge is sustaining the key's secrecy. A reputable third party can generate the key and assign it to both the source and destination.

C. *Symmetric Algorithm*

- Step 1: The symmetric algorithm is also known as the secret key algorithm. The same key is used on both sides to encrypt and decrypt data, resulting in a faster and simpler process [5].

- Step 2: For encryption and decryption, both the sender and the receiver must use the same key. That is, the plain text is turned into cipher text with the aid of the public key and transmitted to the destination from the source, and the same key used by the sender must be used by the receiver to decode the cipher text back into plaintext [5].

- Step 3: To decrypt and encrypt data, both the sender and the receiver must be aware of the public key, also known as a secret key [5].

- Step 4: Stream Ciphers only function on one bit at a time. In stream cipher, the same key is utilized to encrypt data [5].

- Step 5: Block Ciphers never work on more than one block at a time. A separate key is used in stream cipher to encrypt a block of data [5].

D. Symmetric Multiprocessing

Multiple processors share a shared memory and operating system in symmetric multiprocessing. All of these processors operate together to perform procedures, and no processor is set off for specific tasks. The operating system respects all CPUs equally, with no processor being prioritized over another.

In symmetric multiprocessing, each processor is equal and may run different processes as needed, regardless of where these processes are stored in memory. This implies that if data is accessible in the cache, each CPU may access it considerably faster, reducing the load on the system bus.

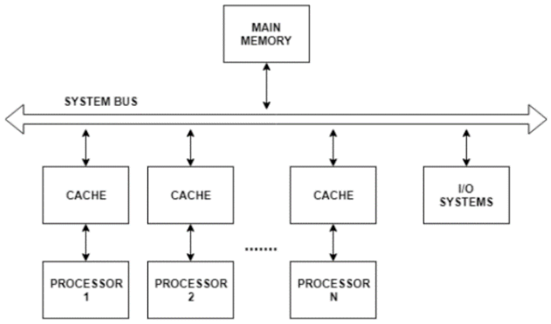


Figure 1 symmetric multiprocessing

E. Uses of Symmetric Multiprocessing

- Because time sharing systems have numerous processes running in parallel, symmetric multiprocessing is advantageous. As a result, utilizing symmetric multiprocessing, these operations may be scheduled on parallel processors.
- Unless multithreaded programming is used, symmetric processing is not very helpful on personal computers. On parallel computers, several threads can be scheduled.
- Symmetric multiprogramming can be used in time sharing systems that employ multithreading programming.

V. Cryptographic Algorithms Commonly Used in Secure Communication

Information security in many different types of civilian systems is now frequently protected by encryption. Encryption is the process of decoding communications (or information) such that only persons with the proper authorization may read it. Although it doesn't stop hacking, it stops the hacker from accessing the encrypted data. In an encryption method, the message or information, which is sometimes referred to as plaintext, is encrypted using an encryption algorithm to create cipher text, which is unreadable text. And an encryption key is typically used to do this. The message's encoding method is specified in this encryption key. An authorized party can use a decryption technique to decode the encrypted text, but doing so necessitates a secret decryption key that attackers are unable to obtain.[13]

Symmetric-key encryption and Public-key encryption are the two fundamental categories of encryption techniques. The encryption key is made public in public-key systems so that anybody can use it to encrypt messages. Nevertheless, the recipient has access to the decryption key and is able to decrypt the messages. This encryption technology is pretty new. The encryption and decryption keys are identical in symmetric-key methods. Before communicating, the parties involved must agree on a secret key. Private-key schemes are another name for symmetric-key encryption.[13]

A. RC4 Encryption Algorithm

The RC4 algorithm was created by RSA employee Ronald Rivest. This shared key stream cipher method necessitates a safe key exchange. Because it involves repeated exchanges of state inputs based on the key sequence, the algorithm is serial. Numerous programmers use this algorithm, which has been made available to the general public. The data stream is simple XORed with the created key sequence, and the technique is used the same way for encryption and decryption. Standards like IEEE 802.11 use a 40-bit and 128-bit key to encrypt data using this encryption technique. [13]

There are various variations of the RC4 algorithm's VOCAL implementation. The forms use UDI instructions and original, optimized hardware at various hardware complexity levels. When specialized hardware isn't really available, the software is used to carry out the byte manipulation and exchange operations. The algorithm fully disregards the kind of plaintext being applied to the key stream. The variable-size key affects the permutation. An 8 x 8 S-Box (S0, S255) with each entry being a permutation of 0 to 255. The algorithm uses two counts, I and j, both initialized to 0.[13]

B. AES Algorithm

Here, they develop and implement an encryption system based on the ARM(S3C6410) algorithm that can encrypt and decode data stored in various memory devices, including U Disk, SD card, and mobile HDD. In this study, they created and developed an ARM-based encryption system to encrypt the stored data (S3C6410). There are a number of encryption methods and key generators available through the system that makes use of visualization technology and human-computer interaction. In this study, they created and developed an ARM-based encryption system to encrypt the stored data (S3C6410). The chaotic map generates PN sequences with good features, and the system offers two types of encryption algorithms: stream cipher with X OR operation, while the other is a hybrid technique combining AES and chaos. The

U.S. National Institute of Standards and Technology developed the Advanced Encryption Standard (AES) as a standard for the encryption of electronic data (NIST). [14]

C. *The Caesar Cipher*

Julius Caesar is credited with creating one of the early encryption methods and using it during the Gallic War. In order to protect the communications he sent to his men, Julius Caesar used cipher, replacing each letter with the next three letters in the alphabet. 'ABC' changes to 'def.' Clearly, this is a rather outdated encryption algorithm.[15]

D. *Data Encryption Standard (DES)*

was the first encryption protocol that the National Institute of Standards and Technology approved (NIST). DES stands for (64 bits block size and 64 bits key size). Since then, numerous attacks and techniques have exposed DES's flaws, rendering it an unsafe block cipher.[15]

E. *Pretty Good Privacy (PGP)*

a public key system that uses the RSA public key cipher to encrypt electronic correspondence. Using a randomly generated key and the IDEA cipher, it encrypts the message. The recipient's public key is then used to encrypt the key. PGP uses his personal RSA key to decrypt the IDEA key before using the IDEA key to decrypt the message when the receiver receives it.[15]

F. *Diffie-Hellman (DH)*

The first publicly available public key cryptography method, Diffie-Hellman, enables two users to share a secret key across an insecure channel without knowing each other's past secrets. Two input variables, P and G, were part of the original protocol. Both of them are open to use and available to all system users. Due to the fact that the Diffie-Hellman key exchange doesn't really validate the participants, it was susceptible to a man-in-the-middle attack. A power of g exists such that n = gk mod p for each and every number n among 1 and P-1 inclusive, where k is a secret number. Parameter p is a prime number, and parameters g is an integer less than p.

VI. Cryptographic Applications

In this section, we are going to merge cryptographic developments in the previous areas to come up with cryptographic applications for secure communication. Since we are focusing on secure communications, the primary objective is to create a secure session or channel for communicating safely.

Let's get a session creation scenario and see what happens during that process. Most of the secure sessions require an authentication process to identify what is the entity that is going to communicate. We call that process peer authentication. After that, the public key exchange is done with an verified key agreement protocol. Then the secret key sharing happens with the support of asymmetric encryption. We call this a hybrid approach because it requires symmetric and asymmetric encryption. The secret key we are exchanging is a derived key of the symmetric master key. The message integrity, authentication, and confidentiality are ensured with the help of MAC and secret key encryption(symmetric encryption) [26].

In addition, we need some other features to ensure the session security, such as sequentially of the message. Then we can say an attacker can't reply to a message, swap, or delete messages.to add this feature, we need something called a synchronized message counter. Like this, we need more security features. Some additional security .some of them are given below.

- On-time message delivery – the sender entity is ensured that he is sent to the correct recipient entity on time.
- Termination – both entities must ensure effectively end the session in its current state. If the termination happens in the usual way, it's a termination success, and if there is some issue with one entity, then another party has to do the early abortion.
- Anonymity – both entities ensure that their identity is not revealed to the outside.
- Untraced ability- entities involved in the communication must ensure that the other party cannot recognize that entity in different sessions. Every identification feature should be temporary.
- Unlinkability – both entities should ensure that they can't identify the same entity sharing two different sessions.

A. *Certificates*

We know that we can exchange a secure key.in that case, we are using a public key cryptosystem to send the secret key K. hence the public key is publicly available. It is pretty easy to share the public key as the standard authenticated key in a client-server protocol. Then later, we can use this to build a secure channel for communication [27]. If we look at how the critical agreement protocol works, we send the public key (K_p) between the client and the server side through a trustworthy channel before the data distribution begins. This established channel might created by either a dependable third party as well. The CA (certificate authority) issues a signature which is σ for K_p, and using it guarantees the public key authentication. The next problem is to protect the asymmetric key (K_p) transmission to the Certificate authority from either the webserver, and we need to provide the same protection to the asymmetric authoritative key (K_p^{CA}) to that same client. If we consider a certificate, it can adhere to the X.509 specification and create using the given formatting. It can also have the internet specification “RFC-2459” to create a certificate. After viewing a certificate, it looks like this.

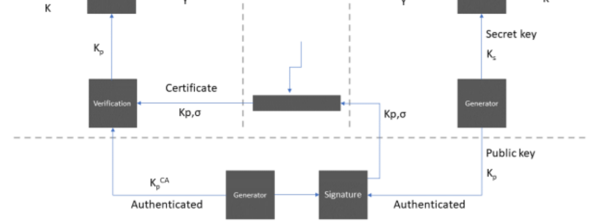
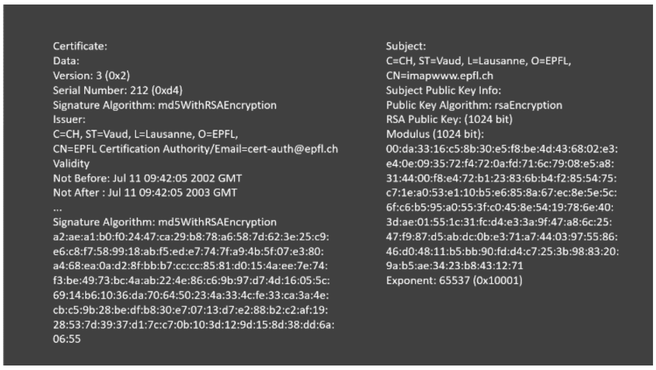


Figure 2 Key exchange using certificates

The first image shows the general structure, consisting of the information related to the issuer, the validity period, and the signature for this certificate(md5WithRSAEncryption algorithm). The second image shows the subject-related information. It includes the subject entity (“IMAP” server for electronic mailboxes in “EPFL”) and the cryptographic algorithm, and the public key [28].



```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 212 (0xd4)
Signature Algorithm: md5WithRSAEncryption
Issuer:
C=CH, ST=Vaud, L=Lausanne, O=EPFL,
CN=EPFL Certification Authority/Email=cert-auth@epfl.ch
Validity
Not Before: Jul 11 09:42:05 2002 GMT
Not After : Jul 11 09:42:05 2003 GMT
...
Signature Algorithm: md5WithRSAEncryption
a2:ae:a1:b0:f0:24:47:ca:29:b8:78:a6:58:7d:62:3e:25:c9:
e6:c8:f7:58:99:18:ab:f5:ed:e7:74:7f:a9:4b:5f:07:e3:80:
a4:68:ea:0a:d2:8f:bb:b7:cc:cc:85:81:d0:15:4a:ee:7e:74:
f3:be:49:73:bc:4a:ab:22:4e:86:c6:9b:97:d7:4d:16:05:5c:
69:14:b6:10:36:da:70:64:50:23:4a:33:4c:fe:33:ca:3a:4e:
cb:c5:9b:28:be:df:b8:30:e7:07:13:d7:e2:88:b2:c2:af:19:
28:53:7d:39:37:d1:7c:c7:0b:10:3d:12:9d:15:8d:38:dd:6a:
06:55
```

```
Subject:
C=CH, ST=Vaud, L=Lausanne, O=EPFL,
CN=imapwww.epfl.ch
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:da:33:16:c5:8b:30:e5:f8:be:4d:43:68:02:e3:
e4:0e:09:35:72:f4:72:0a:fd:71:6c:79:08:e5:a8:
31:44:00:f8:e4:72:b1:23:83:6b:b4:f2:85:54:75:
c7:1e:a0:53:e1:10:b5:e6:85:8a:67:ec:8e:5e:5c:
6f:c6:b5:95:a0:55:3f:c0:45:8e:54:19:78:6e:40:
3d:ae:01:55:1c:31:fc:d4:e3:3a:9f:47:a8:6c:25:
47:f9:87:d5:ab:dc:0b:e3:71:a7:44:03:97:55:86:
46:d0:48:11:b5:bb:90:fd:d4:c7:25:3b:98:83:20:
9a:b5:ae:34:23:b8:43:12:71
Exponent: 65537 (0x10001)
```

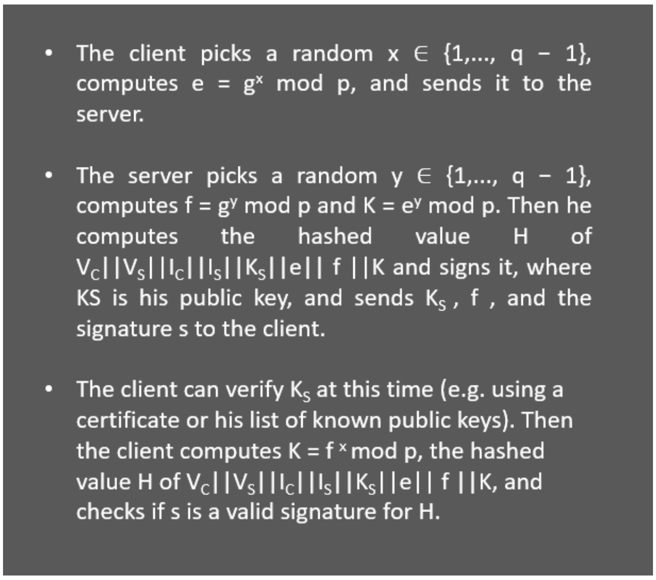
Figure 3 content in a certificate

B. SSH: Secure Shell

SSH was developed with the intention of accessing a computer in a distance a secured manner under OS, such as UNIX.it was created to get the same functionality of the rlogin(remote login) command. Later, there were a series of commercial applications utilizing open-source and secure shell applications constructed using the openSSH library [25]. In the Linux OS, the ssh command is very familiar to Linux users. The Linux community has implemented ssh and SCP commands because it is easy to close all connection ports using these commands for system admins.

C. SSH key exchange

Here we are going to discuss SSH2.it requires a Digital signature standard for authenticating the server entity and DH key agreement used for setting up the secret key (symmetric).both parts rely on generator call g. It generates a derived version of Z_p* of the order of q(prime).it is a mandate to share I_c and I_s as the initial messages between the client entity and the server entity. Then they exchange V_c and V_s., the protocol versions they support. Then it will start the key agreement procedure, which looks like this [23].



- The client picks a random x ∈ {1,..., q − 1}, computes e = g^x mod p, and sends it to the server.
- The server picks a random y ∈ {1,..., q − 1}, computes f = g^y mod p and K = e^y mod p. Then he computes the hashed value H of $V_C||V_S||I_C||I_S||K_S||e||f||K$ and signs it, where KS is his public key, and sends K_S , f , and the signature s to the client.
- The client can verify K_S at this time (e.g. using a certificate or his list of known public keys). Then the client computes K = f ^{x} mod p, the hashed value H of $V_C||V_S||I_C||I_S||K_S||e||f||K$, and checks if s is a valid signature for H.

Figure 4 key agreement procedure

Then both client and server entities can use the secret key(symmetric) for the encryption, and MAC. between both entities, chosen algorithms are arranged. Then few encryption mechanisms are suggested, such as 3DES, AES, RC4, and IDEA [24].

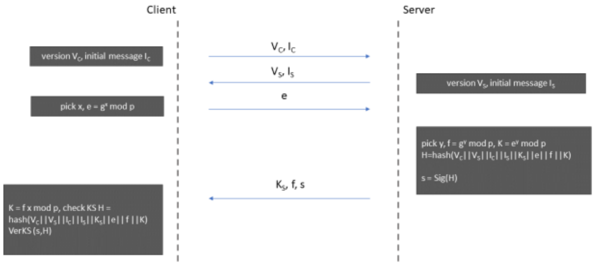

Client
Server
version V_C, initial message I_C
V_C, I_C
V_S, I_S
version V_S, initial message I_S
e
pick x, e = g^x mod p
pick y, f = g^y mod p, K = e^y mod p
H=hash($V_C||V_S||I_C||I_S||K_S||e||f||K$)
s = Sig(H)
K_S, f, s
K = f x mod p, check KS H =
hash($V_C||V_S||I_C||I_S||K_S||e||f||K$)
VerKS (s,H)

Figure 5 key exchange in SSH

If we consider MAC, it is generally an HMAC based on MD5 or SHA1. We know to set up a protected channel, we need keys for that. We created six subkeys which were derived from K, and H.to generate keys, we need a generator function (G (K||H||string||session id)). This generator takes the first bits of the K1, K2 sequence where

$$k_1 = \text{hash}(K||H||\text{string}||\text{session id})$$

And

$$k_{i+1} = \text{hash}(K||H||k_1||\cdots||k_i).$$

D. SSL

Netscape developed secure sockets layer as a communication protocol, and nowadays, it's a very famous protocol among people working with the internet. The structure of this Secure Sockets Layer protocol is similar to the TCP/IP model .it means the objective is to let the applications communicate securely and open/close sockets similarly. Secure sockets layer has a few versions, and the most popular one is v3.0, and later, an improved version of secure sockets layer was introduced as TLS v1.0.so we are going to look at the improved version, which is TLS v1.0.TLS most of the time used on browsers to communicate with HTTP servers through a secured channel. Other than web browsers, TLS also used by other services and applications, such as email managers are required to connect with a mail server. TLS does not rely on any specific cryptographic algorithm, so that it can be used universally. In the beginning client and the server, both entities should arrange a cipher suite. Here, we are going to discuss essential things about secure sockets layer [21].

If we consider Secure Sockets Layer, Two components of protocols available. The second layer is the secure sockets layer record protocol layer, which is implemented between the TCP and other higher-level data transmission protocols. As the HTTP. Next layer is the secure sockets layer handshake protocol layer, and that layer is implemented at the same level as the HTTP. This handshake protocol helps to initiate a session with other protocols such as key agreement and asymmetric authentication. The secure sockets layer record protocol lets us launch a few connections within one session. This provides a secure channel and is protected by symmetric cryptography. Before creating this type of channel secured by symmetric cryptography, it is mandatory to exchange the symmetric using asymmetric cryptography between two entities.

The secure sockets layer client and the server maintain internal data such as session id, peer certificate, cipher suite, and the master secret key for each session. It also contains a compression algorithm choice, and one session can have few connections, as we discussed earlier. A start-up vector, a sequence number that is increased with every message, a server and client nonce, a set of four secret symmetric keys for Message authentication code, and encryption in two different ways—two for the client and two for the server—are all included in the connection state [22].

The cipher suite defines the symmetric encryption and Message authentication code algorithms used in the record protocol, as well as the method used for peer authentication and key agreement in the handshake protocol. The second algorithm pair is called the "cipher specification." Through the secure sockets layer Change Cipher Specification Protocol, a session's cipher specification can be modified. To set it up, it is typically just executed once at the beginning of the procedure.

Alert messages are handled by a separate protocol called the secure sockets layer Alert Protocol. Simple warning notifications or deadly alerts are both possible. The connection fails in the latter scenario. The session's current connections can continue, but no new connections can be started.

E. Handshake

When there is a new secure sockets layer session about to establish the sender entity and the receiver entity should specify a version of the protocol., arrange a cipher specification, confirm both entities using asymmetric keys, and those keys are exchanges happens .this key exchanging happens as it is shown.

1. The sender entity sends a “ClientHello” message consisting of the session id, a list of cipher suites that the client can agree with, and a nonce to the server entity.
2. Then for the client's request server sends its response as the “ServerHello” message, and this message includes the session id and a chosen cipher suite that the client also supported, and a nonce. Usually, the server sends its certificate; hence it is required to be authenticated. This certificate may consist of the data for DH (Diffie-Hellman) key agreement .if not the server should mention one particular key transmission message. The server can send a certificate request if the server needs to authenticate the client entity [19].
3. If the server has requested the client's certificate, then based on it, the client will send its certificate to the server. The client also sends the key exchange message to the corresponding cipher suite and the key algorithm. we call this message the ClientKeyexChange.then both server and client can start computing a few symmetric keys. These keys consist of two for one-way encryption and another two for Message authentication code in one way or another [20].
4. Then the sender sends previous handshake messages, but those are sent as a protected MAC. This confirm that any of the letters are not lost, replayed, or swapped.
5. In the same way, the client-server also sends a protected Message authentication code of previous handshake messages as the response.

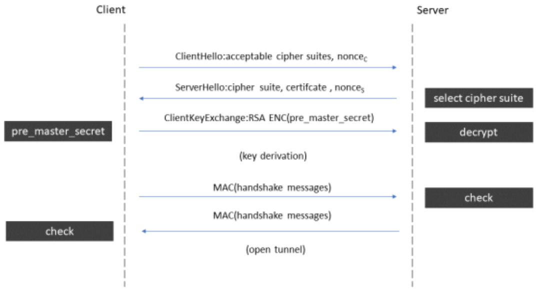


Figure 6 Secure Sockets Layer handshake

Then the client-server can maintain a secure route for communication.

VII. FUTURE OF CRYPTOGRAPHY AND ENCRYPTION

Encryption is an unnoticed element of everyday life, protecting data on anything from emails to bank accounts. As quantum computing gains traction, there are worries that information will become more vulnerable to hackers. Quantum encryption tries to secure data from hacking risks by utilizing quantum physics. Let's start with the fundamentals.

A. Quantum Computing

1) What is quantum computing

A qubit is the fundamental unit of quantum computing. These qubits can exist in numerous states at the same time. If the bit existed between one and zero, it might be 20 percent zero and 80 percent one, or any combination of the two. A computer would examine each possibility separately, but a quantum computer would evaluate all possibilities simultaneously.

In comparison, a few qubits combined have the computing power to tackle a problem in an instant that some computers would take hundreds of years to solve. In addition to this computing power, it is capable of solving the vast majority of math-based encryptions now in use in a short period of time[7].

2) Why quantum computing

Quantum encryption introduces a new dimension in which the numbers can actually be random. The quantum encryption then adopts quantum particle features such as having numerous states of existence and being impossible to measure without upsetting the particle. It is especially safe against hacking since any intervention changes the state of the particle, rendering it unmeasurable and incapable of replicating[7].

3) What does quantum cryptography?

The present method for quantum cryptography, also known as quantum key distribution, delivers photons in an ordered sequence across fibre optic cables. The photon sequence is processed by a polarizer, which randomizes the direction of the photon supplied to the receiver. A receiver selectively takes photons with a specific direction and ignores the rest. These photons are subsequently accepted as the key to decrypt the data.

Although quantum cryptography is theoretically uncheckable, it does have several drawbacks. Data transport is still confined by physical constraints. Quantum and post-quantum encryption are still quite theoretical. Quantum cryptography is predicted to play an important role in the future of data encryption.

B. Homomorphic Encryption

Homomorphic encryption enables data owners or a third party (such as a cloud provider) to perform operations on encrypted data without revealing the data's values. The findings are similarly encrypted and must be accessed using a key. When used in conjunction with blockchain, homomorphic encryption has the potential to bring in a new age of flexible, resilient cybersecurity and encryption methods. However, given its potential, numerous significant industry giants, including IBM, Microsoft, and AWS, are also exploring and creating homomorphic encryption solutions.

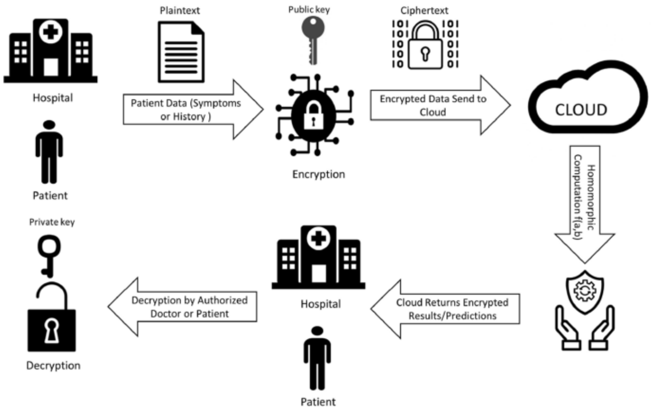

Plaintext
Public key
Ciphertext
Hospital
Patient Data (Symptoms or History)
Encryption
Encrypted Data Send to Cloud
CLOUD
Patient
Homomorphic Computation f(a,b)
Private key
Decryption by Authorized Doctor or Patient
Hospital
Cloud Returns Encrypted Results/Predictions
Decryption
Patient

Figure 7 Homomorphic Encryption

Homomorphic encryption is significant because it allows consumers and businesses to securely store sensitive data on the cloud. Without ever decrypting the data or learning anything about the client's sensitive information, the cloud may compute on it in its encrypted state and deliver encrypted forecasts or encrypted analytics[7].

CONCLUSION

When comes today, we have to use cryptographic applications or services to protect our personal information on our devices. If we look at history, people could not do online purchasing or banking using their devices. Then, after some time, protocols like HTTP were introduced. With that, more cryptographic applications were developed to harden the www's security, making it a safer place to deal with sensitive information. Then people began to use these applications, and researchers were able to identify issues with that applications. Because of this time to time, more advanced cryptographic algorithms have been introduced, and we can see massive improvements over the last few years. Now everything related to information technology uses cryptography, such as banking, online stores, smartphones, ID cards, and other devices are cooperating with cryptography .cryptography will be evolved with time and become more advanced day by day.

REFERENCES

[1] Boloorchi, A., Samadzadeh, M. and Chen, T., 2014. Symmetric Threshold Multipath (STM): An online symmetric key management scheme. Information Sciences, 268, pp.489-504.

[2] Kumar, A. and Kumar, A., 2016. File Encryption System Based on Symmetric Key Cryptography. International Journal Of Engineering And Computer Science,

[3] Tutorialspoint.com. 2022. What are the principle of Symmetric Cipher in Information Security?. [online] Available at: <https://www.tutorialspoint.com/what-are-the-principle-of-symmetric-cipher-in-information-security> [Accessed 11 October 2022].

[4] Tutorialspoint.com. 2022. Symmetric Multiprocessing. [online] Available at: < https://www.tutorialspoint.com/Symmetric-Multiprocessing > [Accessed 11 October 2022].

[5] Patil, T. and Kulhalli, P., 2018. Symmetric Key Cryptography Algorithm for Data Security. International Journal of Trend in Scientific Research and Development, Volume-2(Issue-2), pp.586-589.

[6] Google.com. 2022. homomorphic encryption - Google Search. [online] Available at: <https://www.google.com/search?q=homomorphic+encryption&sxsrf=ALiCzsa5yn-

QVN0lZ2nEHkS2_lfJrIu1Rg:1665500486551&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiv2P7muNj6AhVjxDgGHZ1OCtMQ_AUoAXoECAIQAw#imgrc=HnAGr__OA1PlQM> [Accessed 11 October 2022].

[7] Nelaturu, K., Du, H. and Le, D., 2022. A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions. Cryptography, 6(2), p.18.

[8] https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/

[9] Ferguson, Niels; Schneier, Bruce (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.

[10] Salomaa, Arto (1996). Public-Key Cryptography (2 ed.). Berlin: Springer. 275

[11] IEEE 1363: Standard Specifications for Public-Key Cryptography

[12] hristof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners".

[13] https://www.ijsr.net/archive/v2i12/MDIwMTM1Mjk=.pdf

[14] Chunlei Wang, Guangyi Wang, Yue Sun and Wei Chen "ARM Realization of Storage Device Encryption Based on Chaos and AES Algorithm" 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications

[15] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.9723&rep=rep1&type=pdf

[16] The Economic Times, “Definition of Cryptography | What is Cryptography? Cryptography Meaning - The Economic Times,” The Economic Times, 2019. https://economictimes.indiatimes.com/definition/cryptography

[17] Tutorialspoint.com.. Origin of Cryptography [online] Available at:https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm

[18] wikipedia.org , history of cryptography https://en.wikipedia.org/wiki/History_of_cryptography

[19] SSL Corp. (2021, February 25). The SSL/TLS Handshake: an Overview. SSL.com. Retrieved October 11, 2022, from https://www.ssl.com/article/ssl-tls-handshake-overview/

[20] cloudflare.com , What happens in a TLS handshake? | SSL handshake [online] available at: https://www.cloudflare.com/en-gb/learning/ssl/what-happens-in-a-tls-handshake/

[21] ssl.com , What is SSL? [online] available at:https://www.ssl.com/faqs/faq-what-is-ssl/

[22] cloudflare.com , What is SSL? | SSL definition SSL handshake [online] available at https://www.cloudflare.com/en-gb/learning/ssl/what-is-ssl/

[23] www.ssh.com. (n.d.). Public Key authentication - security, automatic log-in, no passwords. [online] Available at: https://www.ssh.com/academy/ssh/public-key-authentication.

[24] Harris, B. (2006). RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol. doi:10.17487/rfc4432.

[25] www.ssh.com. (n.d.). SSH Secure Shell home page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, how-tos. [online] Available at: https://www.ssh.com/academy/ssh.

[26] www.sciencedirect.com. (n.d.). Symmetric Encryption - an overview | ScienceDirect Topics. [online] Available at: https://www.sciencedirect.com/topics/computer-science/symmetric-encryption#:~:text=Symmetric%20encryption%20uses%20a%20single.

[27] Shacklett, M. E., & Loshin, P. (2021, September 23). digital certificate. SearchSecurity. Retrieved October 11, 2022, from https://www.techtarget.com/searchsecurity/definition/digital-certificate

[28] Wikipedia contributors. (2022, October 8). Public key certificate. Wikipedia. Retrieved October 11, 2022, from https://en.wikipedia.org/wiki/Public_key_certificate