Working from Home and Data Protection

Author: Omar A. Perez Ruiz
Advisor: Dr. Jeffry Duffany
Department of Computer Science

Abstract

Thanks to the pandemic the new order is working from home. When you work from the office the security of the data is responsibility of you as employee and the corporation to provide a safe network. Maybe you see it but working from home you have a lot of responsibility to keep that data save no matter what. Imagen working for a company that is building a Top-Secret Jet and you are just happy working from home and sending this information using an unsecure method and someone managed to get that information. In the next couple of months, you will see a "great value" jet from another country and probably you will get fired. Working from home you have more responsibility to keep the data and network secure all the time.

Introduction

Since the beginning of the times when people started to communicate, they looked a way to hide the message from another person, enemy, country etc. Since then at war armies have been trying to keep any information they share from the enemy because this can be the leverage between winning or lost.

If the human has been trying to secure massages since Egypt nowadays with all the technological advance, easy communication, Internet, emails, cloud storage, etc. is very important to keep your data safe. Beyond the obvious benefit of protecting private information from being stolen or compromised, encryption also provides a means of proving that information is authentic and comes from the point of origin it claims to come from. It can be used to verify the origin of a message and confirm that it hasn't been altered during transmission [1]. In this project we are going to talk about encryption methods as asymmetric, symmetric and hybrid encryption.

Computers and Cryptography

In the computing world, encryption is the conversion of data from a readable format into an encoded format that can only be read or processed after it's been decrypted. Encryption is the basic building block of data security and is the simplest and most important way to ensure a computer system's information can't be stolen and read by someone who wants to use it for nefarious means. Utilized by both individual users and large corporations, encryption is widely used on the internet to ensure the sanctity of user information that's sent between a browser and a server. That information could include everything from payment data to personal information. Firms of all sizes typically use encryption to protect sensitive data on their servers and databases [2].

With the rise of computers, cryptography reached much higher levels of progress than in the analog age. 128-bit mathematical encryption, much stronger than any ancient or medieval encryption, is now the standard for many sensitive devices and computer systems.

Cryptographic Usage

- **Confidentiality:** Keep information secret from everyone except for those who have access authorization.
- **Integrity:** Ensure that the data hasn't been altered.
- **Message Authentication:** Confirm the source of the message.
- **Identification:** Check the identity of the entity.
- **Digital signature:** Verify entity with the message.
- **Certification:** Approval of certain information by a trusted entity
- **Anonymity:** Hide the identity of an entity involved in some process.
- **Revocation:** Withdraw from any certification or authorization.
- **Disavowal:** Prevent the denial of previous agreements or actions.

Symmetric Key Encryption

Symmetric encryption (Next figure) is a type of encryption in which only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption, in which a pair of keys, one public and one private, is used to encrypt and

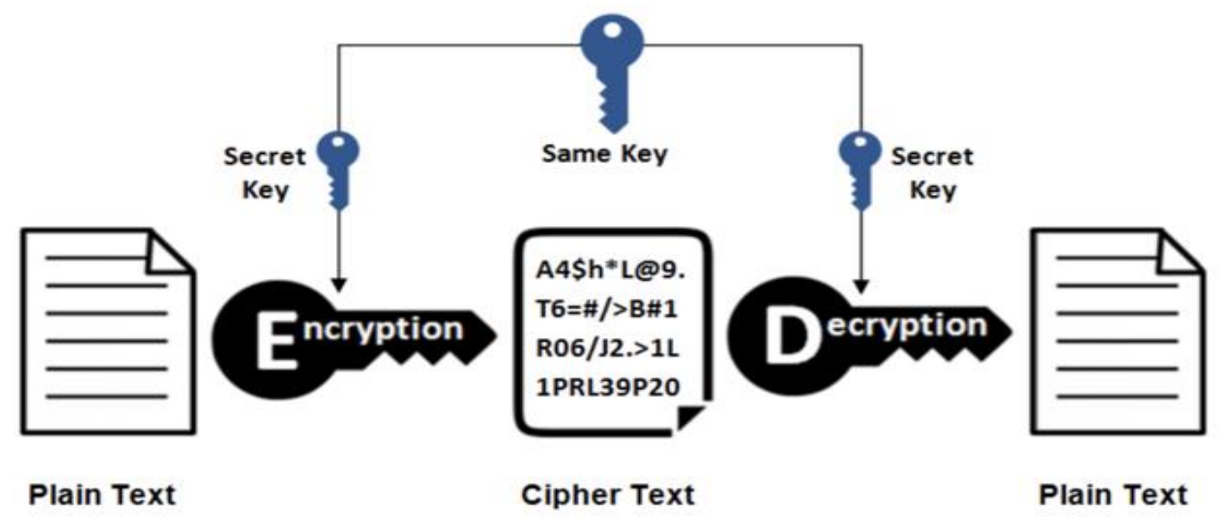


Figure 2
Symmetric encryption

Asymmetrical Key Encryption

Asymmetrical encryption (Next figure) is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know. A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet [4].

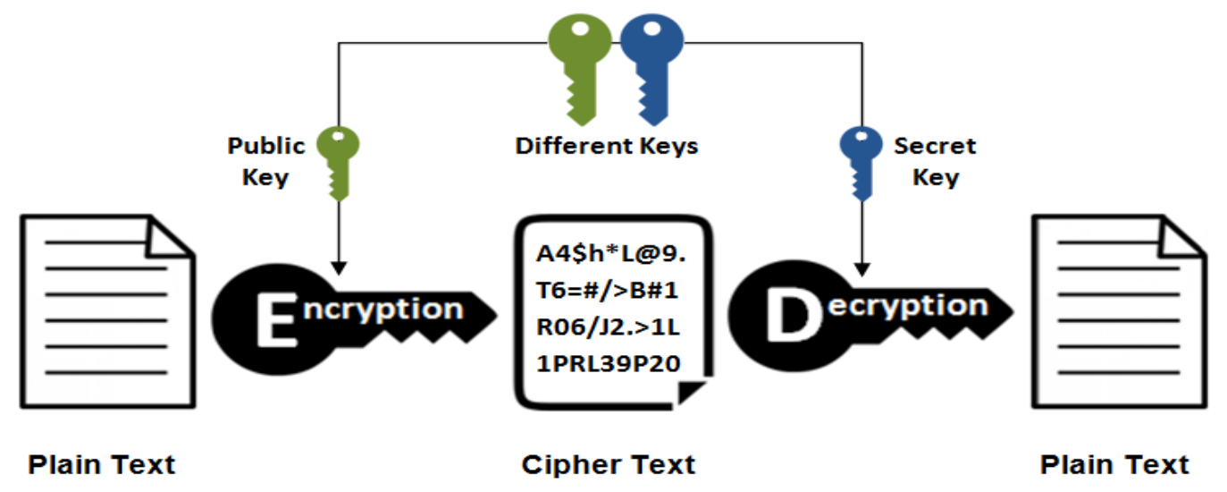


Figure 3
Asymmetric encryption

Hybrid Encryption

Hybrid encryption (Next figure) is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme.

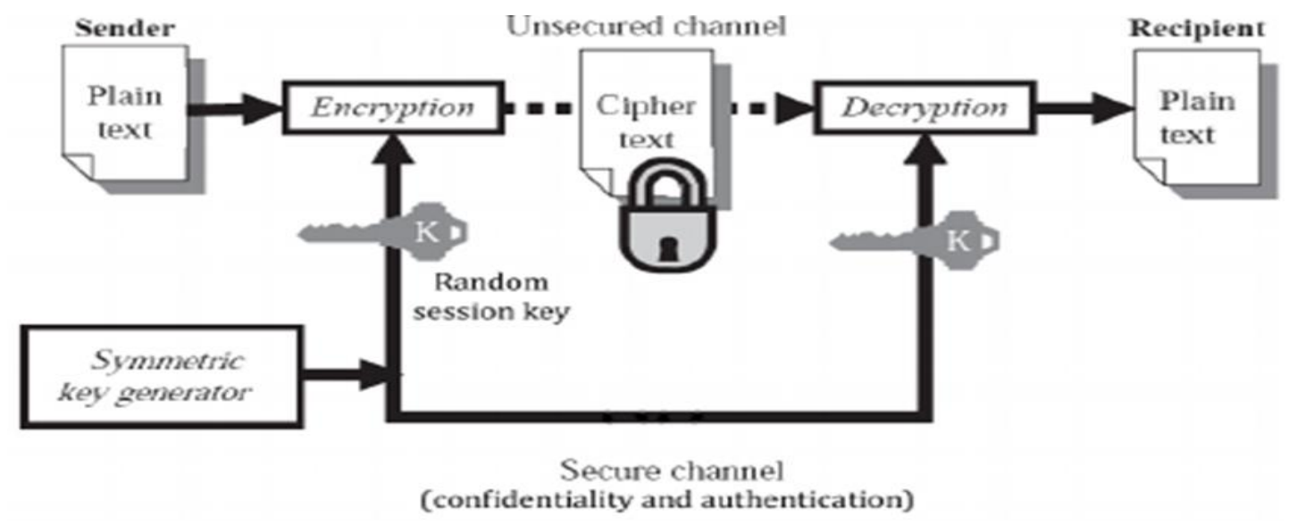


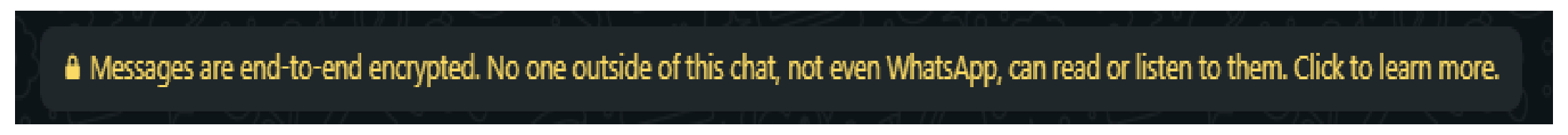
Figure 4
Hybrid encryption

Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message [5].

Built-In Encryption Programs

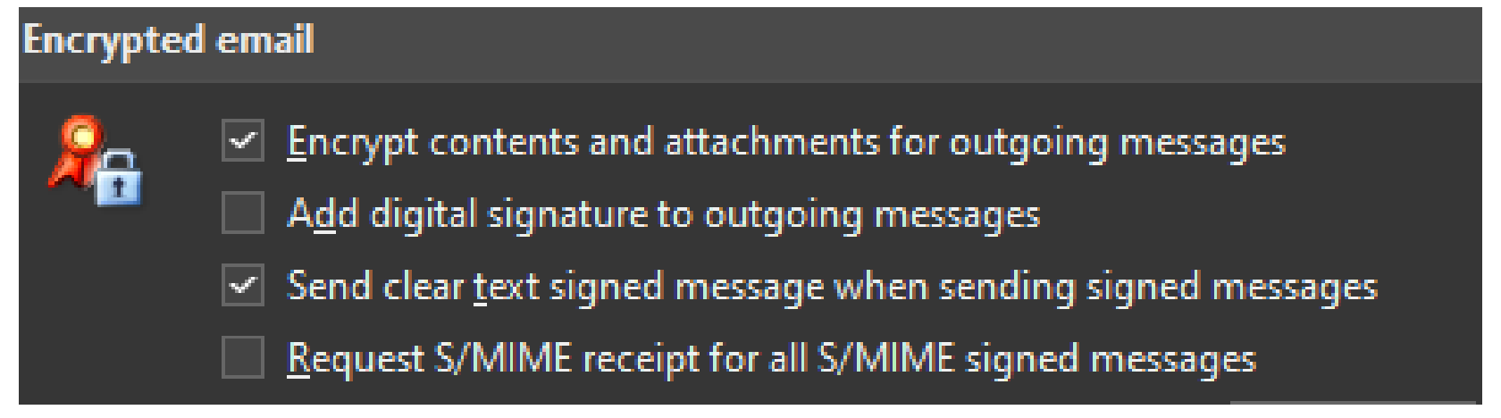
Because encryption is so important and is part of our daily basis, you can find multiples programs with built-in encryption. Perhaps the most common daily-use application is WhatsApp.

WhatsApp uses open source Signal Protocol developed by Open Whisper Systems (They have their own messaging application, Signal). Signal Protocol uses primitives like Double Ratchet Algorithm, pre-keys, Triple Diffie Hellman, Curve25519, AES and HMAC_SHA256. Figure shows WhatsApp's encryption message.



🔒 Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more.

Another common application that most user use is Outlook. Outlook has protection on they servers but also has a build in encryption that use S/MINE. S/MINE or Secure/Multipurpose Internet Mail Extensions is a technology that allows you to encrypt your emails. S/MIME is based on asymmetric cryptography to protect your emails from unwanted access. It also allows you to digitally sign your emails to verify you as the legitimate sender of the message, making it an effective weapon against many phishing attacks out there [5].



Encrypted email

☑ Encrypt contents and attachments for outgoing messages
☐ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
☐ Request S/MIME receipt for all S/MIME signed messages

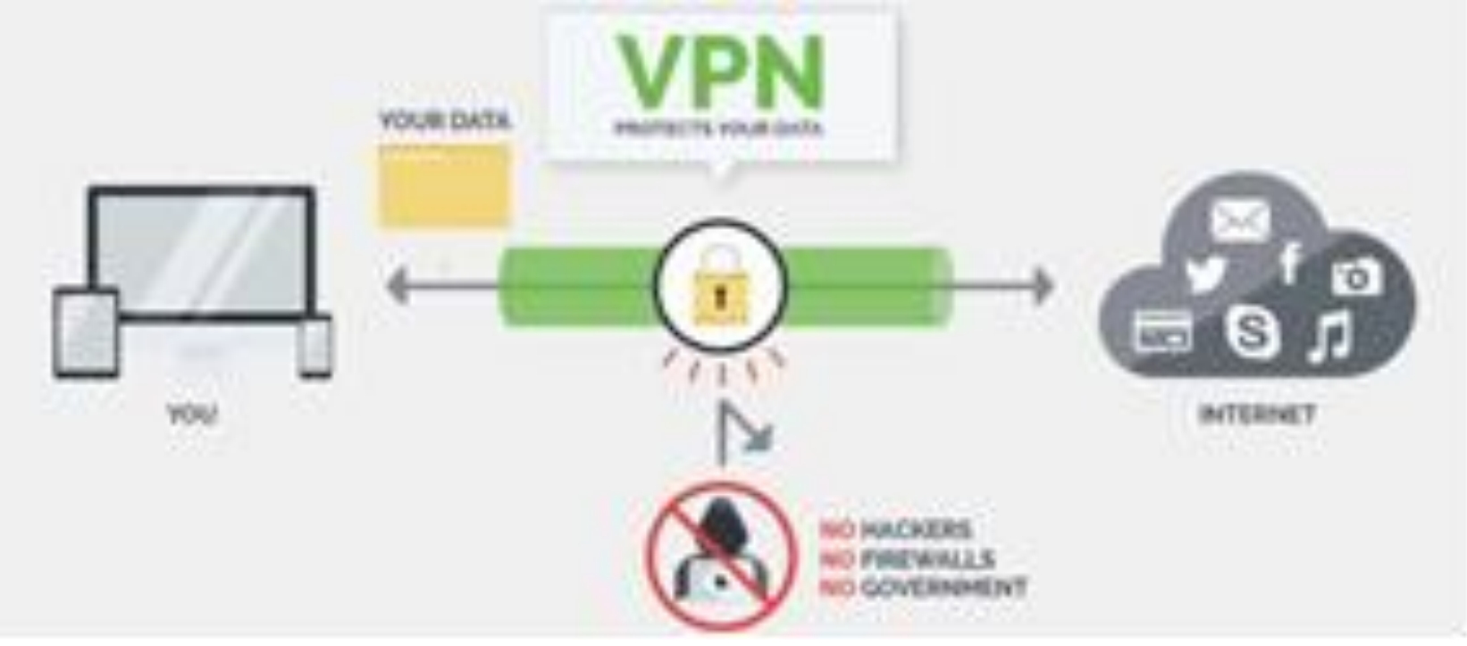
What else do you do in your day? Of course, internet browsing. For this we have DuckDuckGo that is available for iOS, Android and as browser extension. DuckDuckGo not only do they keep you better protected online they give you plenty of information about what they're blocking. DuckDuckGo starts by enforcing encrypted HTTPS connections when websites offer them, and then gives each page you visit a grade based on how aggressively it's trying to mine your data. To keep you anonymized online, DuckDuckGo blocks tracking cookies that are able to identify you and your device, and even scans and ranks sites' privacy policies.

DuckDuckGo

Now With Driving & Walking Directions

VPN

VPN A virtual private network gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot (Next figure).



Conclusion

Humans have been seeking ways to protect information since Egyptian times, and this will continue in the future. Ways to protect personal or a company's data will keep arising, and encryption will get stronger and stronger. New encryption algorithms will be created to fix the flaws and disadvantages of the existing ones.

Protecting data doesn't have to be expensive. There are many free applications or add-ons that are very good for encryption and for keeping information protected all the time.

As mentioned at the beginning, now that working from home is the new normal, each employee has a larger responsibility to secure the company's data. This can be done via encryption or combining ways to secure how data is transferred. Users may add a VPN, encryption, validate the recipient's information before sending, etc. Any of these methods could avoid any company or government agency to be "cloned" or copied.

Future Work

When it comes to security there's a lot but a lot of information and program. Most of the programs that we mentioned here are mostly oriented to a single user or household users. We can find programs that are made for corporations that they can cost millions of dollars but the security on those programs and VPN are top of the line.

Any user that wants to protect their data must choose the best option for them. Get a software that you can understand and get the most out of it to protect your data. Maybe a user doesn't need to encrypt every single file, so a VPN is more than enough for their needs.

References

1. Kapersky, "What is data encryption?" Accessed October 14, 2020. [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/encryption

2. M. Laliberte, "Historical cryptography ciphers," Secplicity, May 25, 2017. [Online]. Available: https://www.secplicity.org/2017/05/25/historical-cryptography-ciphers/

3. P. Smirnoff and D. M. Turner, "Symmetric key encryption - why, where and how it's used in banking," Cryptomathic, January 18, 2019. [Online]. Available: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking

4. SSL2BUY, "Symmetric vs. asymmetric encryption – What are differences?" Accessed October 14, 2020. [Online]. Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

5. Techopedia, "Hybrid encryption," October 28, 2012. [Online]. Available: https://www.techopedia.com/definition/1779/hybrid-encryption