Working from Home and Data Protection

Omar A. Pérez
Master in Computer Science
Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

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.*

Key Terms *— Asymmetric key, Cryptography, Decryption, Encryption, Hybrid Encryption, Public Key, Symmetric Key.*

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 you share a battle strategic and your enemy managed to intercept the message, then the enemy have the advantage. There are several possibilities to exactly how encryption first started, but it is known that it did start in ancient Egypt. One of the beliefs of how encryption started is that the Egyptians wished to preserve the secrecy of the religious rituals from the casual observer or another reason is it might have been a political move to promote their religion [1]. But Julius Caesar was the first person to use the encryption for military purposes.

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 [3]. In this project we are going to talk about encryption methods as asymmetric, symmetric and hybrid encryption.

The History of Encryption

The Caesar cipher, also called a Caesar shift, gets its name from Julius Caesar, who occasionally used this encoding method in his own private messages. As one of the most basic encryption techniques, the Caesar cipher works by replacing each letter in the original plaintext message with a different letter based off a fixed shift of the alphabet (figure 1).

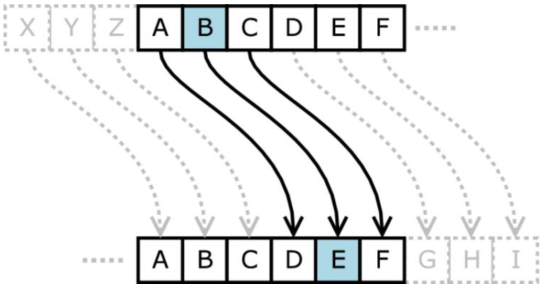


Figure 1
Caesar cipher

To encode a secret message using a Caesar shift of 7 to the right. First, we create our substitution table by printing the alphabet followed by the alphabet shifted 7 places to the right.

Original:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shifted:
TUVWXYZABCDEFGHIJKLMNOPQRS

Next, we take each letter of our plaintext message and replace it with its corresponding letter in the shifted alphabet.

Plaintext:
THISISASECRETMESSAGEBURNAFTERREADING

Ciphertext:
MABLBLTLXVKXMFXLLTZXUNKGTYMXKKXTWBGZ [2]

To revert the encoded message back into its readable plaintext form, the recipient must re-create the substitution table using the appropriate shift and then substitute each encoded character with its original character, according to the shift [2].

Cryptographic science would continue to progress in the following centuries. A remarkable advance in cryptography would be described, but perhaps never built, by Thomas Jefferson in the 1790s. His invention, known as a cipher wheel, consisted of 36 letter rings on movable wheels, which could be used to achieve complex coding. This concept was so advanced that it would serve as the basis for American military cryptography until World War II.

World War II would bring with it the perfect example of analog cryptography: The Enigma machine. Like the encryption wheel, this device, employed by the Axis powers, used rotating wheels to encrypt a message - making it virtually impossible to read without another Enigma machine. Early forms of computer technology would be employed to eventually help break Enigma's encryption. The successful decryption of Enigma messages is still considered a critical component of the subsequent Allied victory.

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 [3].

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. In 1990, a whole new form of cryptography, dubbed quantum cryptography, would be launched by computer scientists who hoped to once again raise the level of protection offered by modern encryption.

More recently, cryptographic techniques have also been used to make cryptocurrencies possible. Cryptocurrencies take advantage of several advanced cryptographic techniques such as hash functions, public key cryptography, and digital signatures. These techniques are mainly used to ensure the security of data stored in blockchains and to authenticate transactions. A specialized form of cryptography, called the Elliptic Curve Digital Signature Algorithm (ECDSA), serves as a prop to Bitcoin and other cryptocurrency systems, by providing supplemental security and ensuring that funds can only be used by their rightful owners.

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 (figure 2) is a type of encryption where 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 where a pair of keys, one public and one private, is used to encrypt and decrypt messages [4].

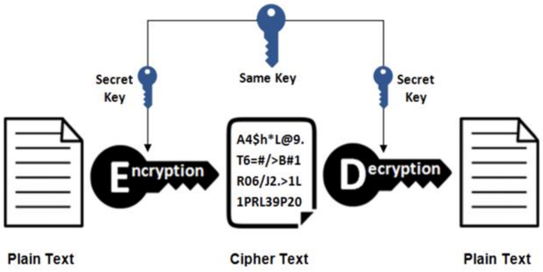


Figure 2
Symmetric encryption

By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. The secret key that the sender and recipient both use could be a specific password/code or it can be random string of letters or numbers that have been generated by a secure random number generator (RNG). For banking-grade encryption, the symmetric keys must be created using an RNG that is certified according to industry standards, such as FIPS 140-2 [4].

Some examples of symmetric encryption algorithms are:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

AES, DES, IDEA, Blowfish, RC5 and RC6 are block ciphers. RC4 is stream cipher.

Advantages of Symmetric Encryption

- A symmetric system is faster.
- Symmetric systems the encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.
- The Symmetric System uses a password for the authentication to verify the receiver identity.
- The system that has the secret keys is the only one capable of decrypt the message [6].

Disadvantages of Symmetric Encryption

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. The only secure way of exchanging keys would be exchanging them personally.
- Cannot provide digital signatures that cannot be repudiated [6].

ASYMMETRIC KEY ENCRYPTION

Asymmetrical encryption (figure 3) 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.

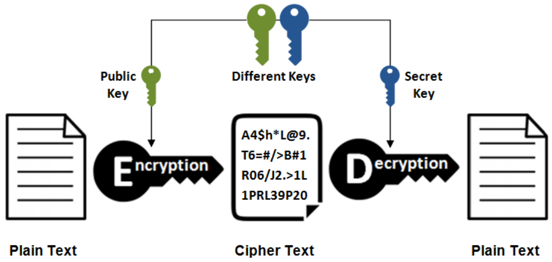


Figure 3
Asymmetric encryption

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. Asymmetric key has a far better power in ensuring the security of information transmitted during communication [5].

Some examples of asymmetric encryption algorithms are:

- RSA (Rivest Shamir Adleman)
- ECC (Elliptic Curve Cryptopraphgy)
- El Gamal
- DSA (Digital Signature Algorithm)
- Diffie-Hellman

Advantages of Asymmetric Encryption

- In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
- The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
- Can provide digital signatures that can be repudiated [6].

Disadvantages of Asymmetric Encryption

- Asymmetric encryption uses longer keys than symmetric encryption in order to provide better security than symmetric key encryption. While the longer key length in itself is not so much a disadvantage, it contributes to slower encryption speed. [7].
- Due to the fact one of the keys in an asymmetric encryption infrastructure is public, most business must implement a full public key infrastructure (PKI) to properly manage the certificates. A full PKI manages issuance, revocation and validity, typically through trusted third-party certificate authorities (CAs). These CAs sell their services, adding to the expenses of those companies or individuals who buy their certificates [7].

HYBRID ENCRYPTION

Hybrid encryption (figure 4) 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 [8].

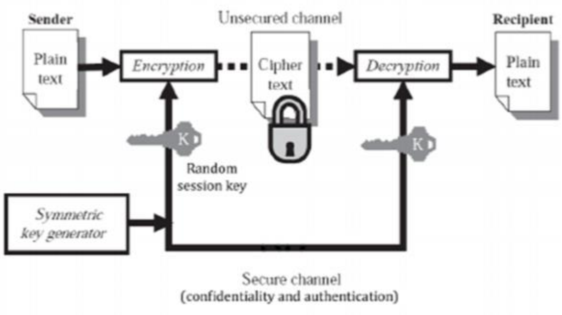


Figure 4
Hybrid encryption

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. 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. The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance [9].

Hybrid encryption provides some extra security. Its encryption procedure is as follows:

- Employs public key encryption to share a key for symmetric encryption.
- The message that is being sent at the moment is encrypted using its own private key.
- The encrypted message is then sent to the recipient.
- Since sharing a symmetric key is not secure, it is different for each session.
- The session key (symmetric key) is encrypted with the recipient's public key.
- The outgoing message is encrypted with the symmetric key, all automatically combined into a single packet.

The essential feature about hybrid encryption is that symmetric key is created over and over for every new conversation or every new data exchange, e.g. every new session. Session key is a one-time randomly generated set of numbers which is used to transform plain text into cypher. Every time for any intention to communicate with others crypto system creates a new symmetric key (generates a set of random numbers). The power of random numbers is that its consequence cannot be guesses, repeated or predicted by a hacker. This approach ensures forward security of communication is case of leaks of symmetric keys from previous sessions or contacts.

According to [11], the steps of hybrid encryption are:

- Generate a symmetric key. The symmetric key needs to be kept a secret.
- Encrypt the data using the secret symmetric key.
- The person to whom we wish to send a message will share her public key and keep the private key a secret.
- Encrypt the symmetric key using the public key of the receiver.
- Send the encrypted symmetric key to the receiver.
- Send the encrypted message text.
- The receiver decrypts the encrypted symmetric key using her private key and gets the symmetric key needed for decryption.
- The receiver uses the decrypted symmetric key to decrypt the message, getting the original message.

In the hybrid method, the data to be encrypted is not limited by the length of the encryption key. Additionally, the encrypted symmetric key is secure because it is encrypted using the public key of the receiver. Even if the encrypted data and the encrypted key are intercepted by another person, they will not be able to get the original data as long as the private key is maintained as a secret [10].

How Hybrid Encryption Works

Like mentioned before the process is to encrypt the data with a symmetric and the symmetric key is encrypted with an asymmetric encryption but depending on how the data is going to be transferred on real time or storage the management of the encryption key is different. For example, a real time can be like a voice call, messages, internet browsing, chat, etc. some examples of storage can be an email, documents, data, etc.

Real-Time Communication Using Hybrid Encryption

- Users exchange with their public keys. Essentially, initiator of communication request should get a public key of request acceptor.
- Initiator of communication generates a random on-time session key (figure 5).

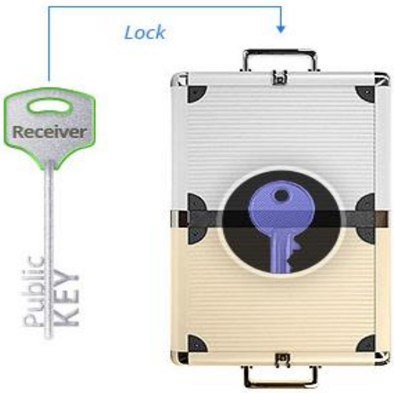


Figure 5
Initiator's side

- Initiator of communication encrypts the session key using recipient's public key and sends encrypted key to receiver via unsecure cyber space.
- Receiver of communication request accepts encrypted key and decrypts it using matching private key (figure 6).

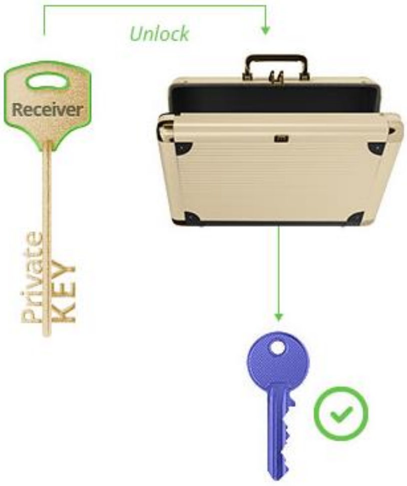


Figure 6
Receiver's side

- Now both sides communicate using same session key. Communication stream is encrypted with strong symmetric encryption algorithm and only users who have matching one-time generated key can decrypt the flow. Interception of encrypted data is useless because bits of data will make only mess and no sense (figure 7).

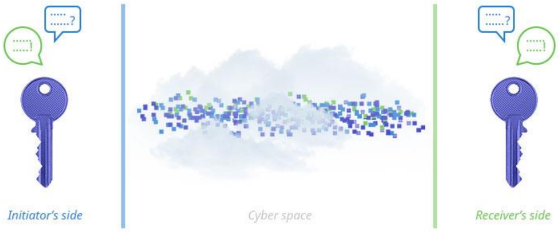


Figure 7
Real-time hybrid communication after connection was established

Storing Using Hybrid Encryption

Case when encrypted data is sent now and will be read by a recipient some day in the future requires management policy which is different from real-time communication. Examples of this type of hybrid encryption application could be e-mail encryption, PGP encryption, sending sensitive documents etc. [10].

- Users exchange with public keys.
- Sender writes a message (creates a document).
- Sender generates a random one-time session key and encrypts the message with the session key.
- Sender encrypts the asymmetric session key with recipient's public key which was obtained on step 1 (figure 8).

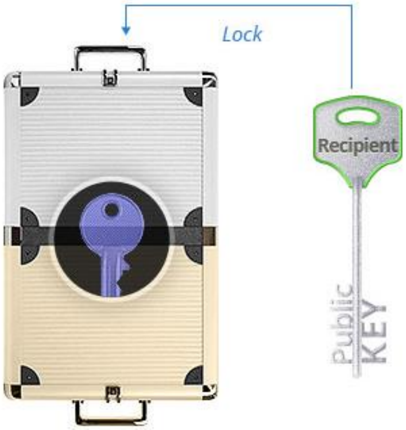


Figure 8
Asymmetric Session Key Encrypted with the Recipients Public Key

- Sender sends both encrypted message and encrypted key to recipient.
- Such secured data package may stay untouched for some time until recipient initiates decryption process. To do it recipient should have valid private key which matches the case. First, recipient unlocks the case using private key and releases the session key. Then session key is used to decrypt the message, e-mail or file (figure 9).

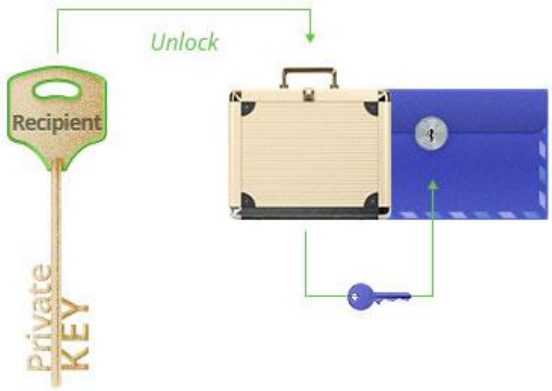


Figure 9
Data Secured Until Recipient Open it.

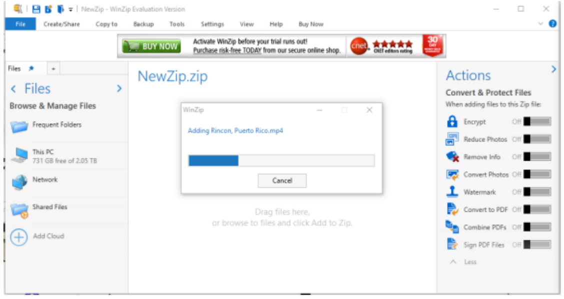
Hybrid Encryption in Action

Every day you use hybrid encryption in emails, web browsing, communications, etc. But the programs do all the encryption behind the scene you never see the process. I'm going to show you the steps to do a hybrid encryption for yourself to store data.

For this I will by using WinZip, a 256-bit key generated on allkeysgenerator.com, JSEncrypt to encrypt the 256-bit passphrase and a personal video file for the test.

WinZip is trusted by millions of businesses and consumers to boost productivity, simplify file sharing and keep information private. The world's number one compression and encryption software, WinZip offers apps for all of today's most popular platforms and devices, giving users a better way to exchange files in the cloud, email and social media. WinZip's product line also includes powerful utilities to improve system performance and help keep PCs secure. WinZip is part of the Corel family of companies [11]. Jsencrypt is a Javascript library to perform OpenSSL RSA Encryption, Decryption, and Key Generation [12].

- Open WinZip and drop the file you want to zip (figure 10).



Activate WinZip before your trial runs out!
Purchase risk-free TODAY from our secure online shop.

This PC 731 GB free of 2.05 TB

Adding Rincon, Puerto Rico.mp4

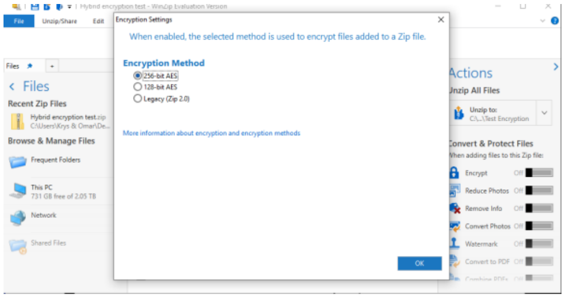
Drag files here,
or browse to files and click Add to Zip.

When adding files to this Zip file:

Encrypt	Off
Reduce Photos	Off
Remove Info	Off
Convert Photos	Off
Watermark	Off
Convert to PDF	Off
Combine PDFs	Off
Sign PDF Files	Off

Figure 10
WinZip software

- Zip the data by pressing File, Save As and enter the name and location and press save. This will zip all the data you added to WinZip to one single file.
- Locate the zip file do a right click and go to WinZip and select Encrypt. Before that be sure that on WinZip encryption settings 265-bit AES is selected (figures 11 and 12).



Encryption Settings

When enabled, the selected method is used to encrypt files added to a Zip file.

Encryption Method

● 256-bit AES
○ 128-bit AES
○ Legacy (Zip 2.0)

More information about encryption and encryption methods

OK

Figure 11
WinZip Encryption Settings

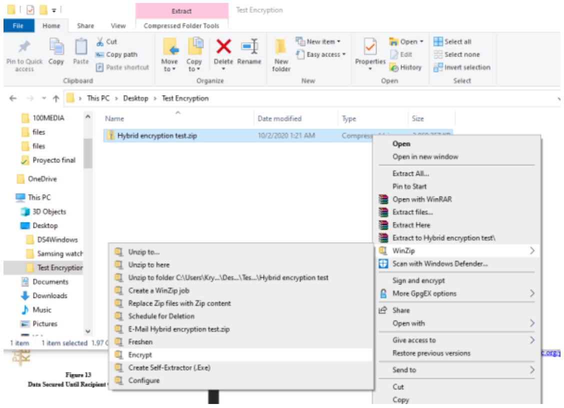
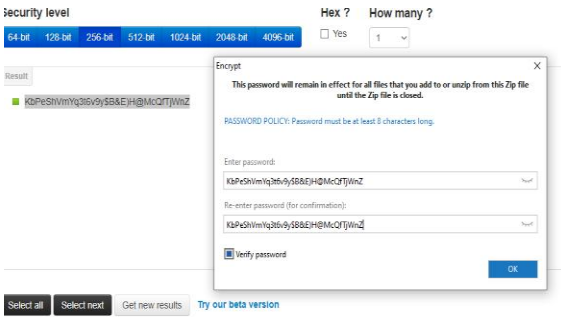


Figure 12
Selection of the encryption

- Insert the 256-bit passphrase obtained from https://allkeysgenerator.com. This will encrypt the zip file using the symmetric encryption (figure 13).



□ Yes

1

KbPeShVmYq3t6v9y$B&E)H@McQfTjWnZ

Encrypt

This password will remain in effect for all files that you add to or unzip from this Zip file until the Zip file is closed.

PASSWORD POLICY: Password must be at least 8 characters long.

Enter password:

KbPeShVmYq3t6v9y$B&E)H@McQfTjWnZ

Re-enter password (for confirmation):

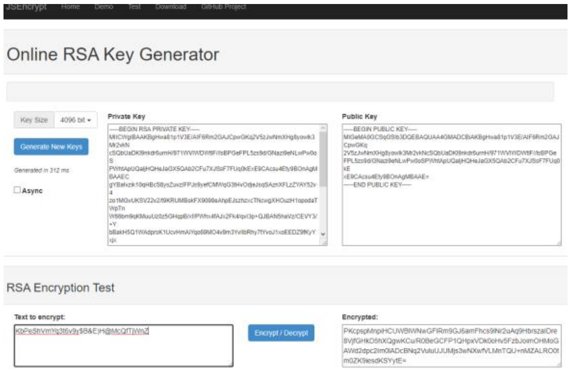
KbPeShVmYq3t6v9y$B&E)H@McQfTjWnZ

☑ Verify password

OK

Figure 13
Symmetric zip file encryption

- Now visit the webpage https://travistidwell.com/jsencrypt/demo/index.html and insert the 256-bit passphrase ok the Text to encrypt and press the Encrypt/Decrypt bottom to encrypt the passphrase. This will encrypt the passphrase with the recipient public key. After this step, the file and the encrypted key is ready to be stored or sent to another user. The other user will need to decrypt the symmetric key with his private key (figure 14).



Online RSA Key Generator

Key Size 4096 bit

Generated in 312 ms

□ Async

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgHwa81p1V3E/AIF6Rm2GAJCpwGKq2V5zJwNmXHg8yowk3
Mr2vkN
cSQbUaDK9nkdr6umH/971WVIWDWtF/IsBPGeFPL5zs9d/GNazi9eNLwPw0o
S
PWhtApUQajHQHeJaGX5QAb2CFu7XJSsF7FUq0kExE9CAcsu4Ety9BOnAgM
BAAEC
gYBalvzik10qHBcS8ysZuvzIFPJs9yefCMWqG38HvOdjeJsqSAznXFLzZYAY52v
4
zo1MGvUKSV22v2/l9KRUMBokFX9098aAhpEJszhzxcTNcwgXHOuzH1opodaT
WpTn
Wt66bm9qKMuuU20z5GHqpB/xIPWhx4fAJx2Fk4/qvl3p+QJBAN5haVz/CEVY3/
+Y
bBakH5Q1WAdprsK1UcvHmA/Yqo69MO4x9m3YvIbRhy7tYvoJ1xoEEDZ9fKyY
xjx
```

Public Key

```
-----BEGIN PUBLIC KEY-----
MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgHwa81p1V3E/AIF6Rm2GAJ
CpwGKq
2V5zJwNmXHg8yowk3Mr2vkNcSQbUaDK9nkdr6umH/971WVIWDWtF/IsBPGe
FPL5zs9d/GNazi9eNLwPw0oSPWhtApUQajHQHeJaGX5QAb2CFu7XJSsF7FUq0
kE
xE9CAcsu4Ety9BOnAgMBAAE=
-----END PUBLIC KEY-----
```

RSA Encryption Test

Text to encrypt:

KbPeShVmYq3t6v9y$B&E)H@McQfTjWnZ

Encrypted:

```
PKcpspMnpiHCUWBIWNwGFIRm9GJ6amFhcs9lNr2uAq9HbrszalOre
8VjfGHKD5hXQgwKCu/R0BeGCFP1QHpxVDk0oHv5FzbJoimOHMoG
AWd2dpc2lm0lADcBNq2VuluUJUMjs3wNXwfVLMnTQU+nMZALRO0t
m0ZK9lesdKSYytE=
```

Figure 14
Passphrase encryption

- After obtaining the decrypted key the recipient is able to decrypt the zip file and access the data.

We have achieved a hybrid encryption and secured a large data file and secured send it over a public network. This method is very effective when it comes to cloud storage data transfers.

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 Encryption

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, prekeys, Triple Diffie Hellman, Curve25519, AES and HMAC_SHA256 [14]. Figure 15 shows WhatsApp's encryption message.

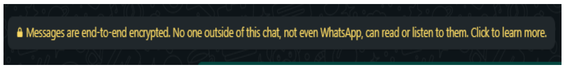

🔒 Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more.

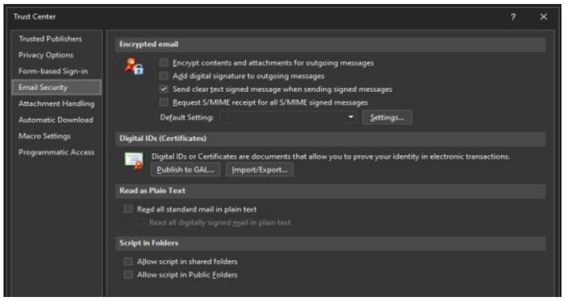
Figure 15
WhatsApp encryption message

Outlook Encryption

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 [15].

To use S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard. Outlook supports the S/MIME standard. To use the encryption:

- You have to add the certificate keychain on the computer from Outlook application in Trust Center and under Email Security and activate the checkbox of Encrypt message contents and attachments (figure 16).



Trust Center

Trusted Publishers
Privacy Options
Form-based Sign-in
Email Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access

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

Default Setting: [Settings...]

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

[Publish to GAL...] [Import/Export...]

Read as Plain Text

□ Read all standard mail in plain text
□ Read all digitally signed mail in plain text

Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

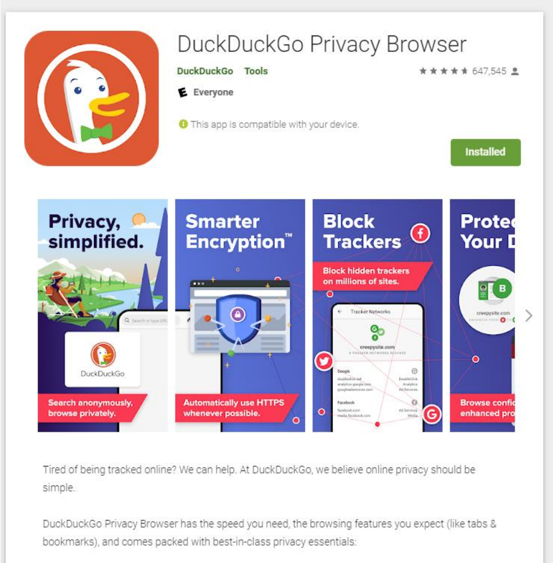
Figure 16
Outlook Encryption Configuration

- Now just create your message and send it all your messages are now encrypted.

Web Browser Encryption

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 also known as the anti-Google search engine, 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. You can clear tabs and data automatically at the end of each session, or you can wipe this data manually with a single tap. You can even set a timer to automatically clear out your history after a period of inactivity [16].

To get DuckDuckGo on mobile devices go to the store and search for DuckDuckGo Privacy browser and installed (figure 17). The app will take care of the rest to protect your information and searches.



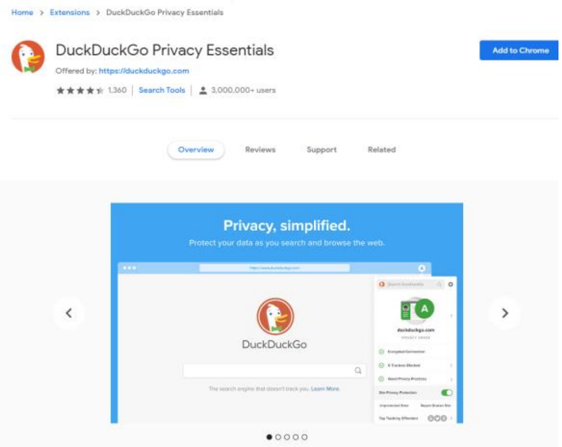
This app is compatible with your device.

Tired of being tracked online? We can help. At DuckDuckGo, we believe online privacy should be simple.

DuckDuckGo Privacy Browser has the speed you need, the browsing features you expect (like tabs & bookmarks), and comes packed with best-in-class privacy essentials:

Figure 17
Android Store and DuckDuckGo Browser

For browsers like Chrome you can download and install the extension (figure 18). In Opera is already part of it and just by changing in your settings the search engine to DuckDuckGo you are ready to go (figure 19).



Home > Extensions > DuckDuckGo Privacy Essentials

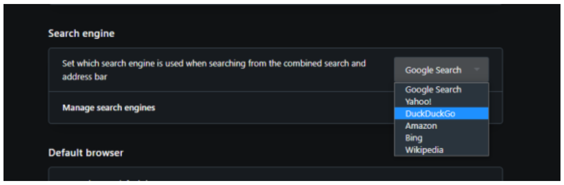
DuckDuckGo Privacy Essentials

Offered by: https://duckduckgo.com

★★★★½ 1,360 | Search Tools | 3,000,000+ users

Add to Chrome
Overview
Reviews
Support
Related
Privacy, simplified.
Protect your data as you search and browse the web.
DuckDuckGo
The search engine that doesn't track you. Learn More.
A
duckduckgo.com

Figure 18
DuckDuckGo in Chrome Store



Search engine

Set which search engine is used when searching from the combined search and address bar — Google Search

Manage search engines

Default browser

Figure 19
Opera Browser Settings

VPN

Most of the companies that works with very important use VPN to keep all inside within they own network. 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 (figure 20).

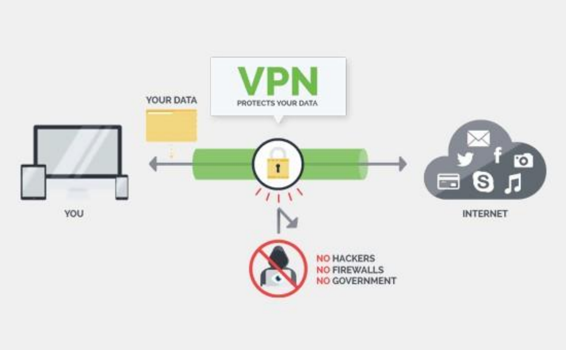


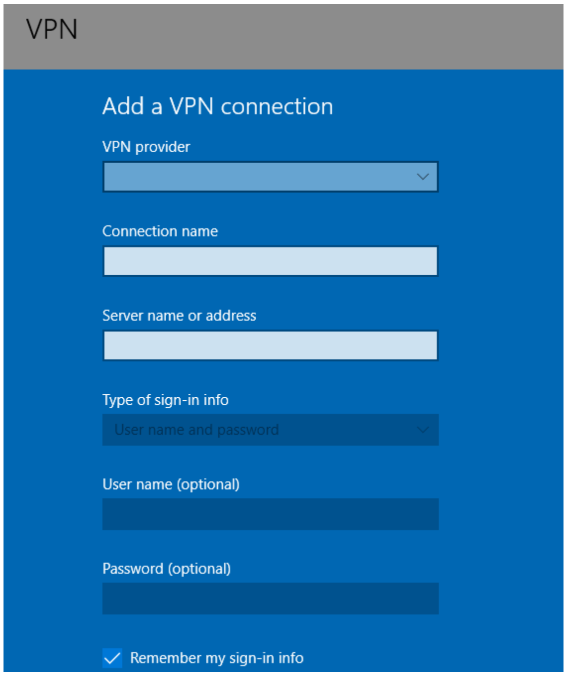
Figure 20
How a VPN works

VPNs essentially create a data tunnel between your local network and an exit node in another location, which could be thousands of miles away, making it seem as if you’re in another place. This benefit allows online freedom, or the ability to access your favorite apps and websites while on the go [17].

You can find multiple VPN providers from free to annual subscriptions.

If your corporation has a VPN Windows provide a setting to create the VPN connection. You will need the Internet Address.

- Go to VPN settings and press the add VPN.
- Fill out all the information that has been provided from your company and create the VPN connection (figure 21).



VPN

Add a VPN connection

VPN provider

Connection name

Server name or address

Type of sign-in info

User name and password

User name (optional)

Password (optional)

☑ Remember my sign-in info

Figure 21
Windows Add VPN Connection Settings

Free VPNs has some limitations like limit the amount of bandwidth you can use in a given period. Some keep the number of simultaneous connections low, generally to one or two. Some restrict you to certain servers, meaning you can't jump to a better-performing server, or a server in a particular location. Some of the popular free VPN are:

- ProtonVPN
- TunnelBear VPN
- Hotspor Shield VPN
- Avira Phantom VPN
- Hide.me VPN
- Kaspersky Secure Connection VPN

Finding the best free VPN is an exercise in balancing those restrictions. TunnelBear, for example, lets you use any server on its network but limits you to 500 MB-1 GB per month. Avira Phantom VPN lets you use as many devices as you like and any server you like, but also restricts you to 500 MB per month. Hotspot Shield also places no limits on the number of devices but restricts you to 500 MB per day and only US-based servers. Kaspersky Secure Connection doesn't limit your devices but doesn't let you choose a VPN server the app does it automatically.

ProtonVPN has the unique distinction of placing no data restrictions on free users. You can browse as much as you want, as long as you want. You will be limited to just one device on the service at a time and can only choose between three server locations, but the unlimited data makes up for all that. It doesn't hurt that ProtonVPN, from the same people that brought you super-secure ProtonMail email, is very concerned about security and customer privacy [18]. Paying a VPN service will provide you more features and options to protect your data.

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.

As user that wants to protect your data you will need to check what is better for you. Get software’s that you can understand and that you can get the most out of it to protect the data you want. Maybe you don’t need to encrypt every single file and just a VPN is more than enough for your needs. In the other hand you are a scientist creating a space ship like no other in the planet in that case you will need very good programs and possible encrypt everything.

Conclusion

The human has been looking ways to protect the information since the Egypt times and this will continue to the future. Ways to protect your company data or your data will keep surging and all kind of encryption will get stronger and stronger. New encryptions algorithms are going to be created to fix the flaws and disadvantages of the existing ones.

Hybrid encryption is fast, super strong and has a safe key distribution but maybe doesn’t fill the user requirements so this can choose between a symmetric or asymmetric encryption to satisfy the users demands. Technically speaking hybrid encryption hasn’t been around for a lot of time and this will continue growing until it gets the same or better result as any other encryption method.

Protect your data or what you do doesn’t have to be expensive. There is a lot of applications or add-ons for free that are very good for encryption and for keeping your information protected all the time.

Like I mentioned in the beginning now that the new order is work from home you as employee has a bigger responsibility to secure the company data. It can be via encryption or combine multiple ways to secure how you transfer the data. You can add a VPN, encryption, validate the recipient information before sending it, etc. Any of this method can be the difference between any company or government to get “cloned” or copied.

References

[1] R. Prichard. (2002, January 26). Global Information Assurance Certification Available: https://www.giac.org/paper/gsec/1555/historyencryption/102877).

[2] M. Laliberte. (2017, May 25). Historical Cryptography Ciphers Available:

https://www.secplicity.org/2017/05/25/historical-cryptography-ciphers/

[3] What is Data Encryption? Available: https://usa.kaspersky.com/resource-center/definitions/encryption

[4] P. Smirnoff & D. TurnerK. (2019, January 18). Symmetric Key Encryption - why, where and how it’s used in banking. Available: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking#:~:text=Symmetric%20encryption%20is%20a%20type,used%20in%20the%20decryption%20process.

[5] Symmetric vs. Asymmetric Encryption – What are differences? Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

[6] Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems Available: http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf

[7] A. Hughes. The Disadvantages of Asymmetric Encryption Available: https://www.techwalla.com/articles/the-disadvantages-of-asymmetric-encryption.

[8] P. Kuppuswamy, S. Al-Khalidi. (2014, March) Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm Available: https://pdfs.semanticscholar.org/87ff/ea85fbf52e22e4808e1fcc9e40ead4ff7738.pdf

[9] (2012, October 28) Hybrid Encryption Available: https://www.techopedia.com/definition/1779/hybrid-encryption

[10] The core idea of hybrid cryptography Available: https://no1bc.com/more/articles/hybrid-encryption/

[11] B. Patwardhan. (2019, May 21) Encryption, Part 3: Hybrid Encryption Available: https://dzone.com/articles/encryption-part-3-hybrid-encryption-symmetric-publ

[12] About WinZip Available: https://www.winzip.com/win/en/about.html

[13] Jsencrypt Available: https://www.npmjs.com/package/jsencrypt

[14] A. Pemghal. (2018, October 6) WhatsApp‘s End to End Encryption, How does it work? Available: https://medium.com/@panghalamit/whatsapp-s-end-to-end-encryption-how-does-it-work-80020977caa0

[15] R. Publico. (2017, February 14) What is S/MIME and How Does it Work? Available: https://www.globalsign.com/en/blog/what-is-s-mime

[16] D. Nield. (2019, June 16) It's Time to Switch to a Privacy Browser Available: https://www.wired.com/story/privacy-browsers-duckduckgo-ghostery-brave/

[17] S. Symanovich. What is a VPN? Available: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

[18] M. Eddy. (2020, September 15) The Best VPN Services for 2020 Available: https://www.pcmag.com/picks/the-best-vpnservices?test_uuid=01jrZgWNXhmA3ocG7ZHXevj&test_variant=b