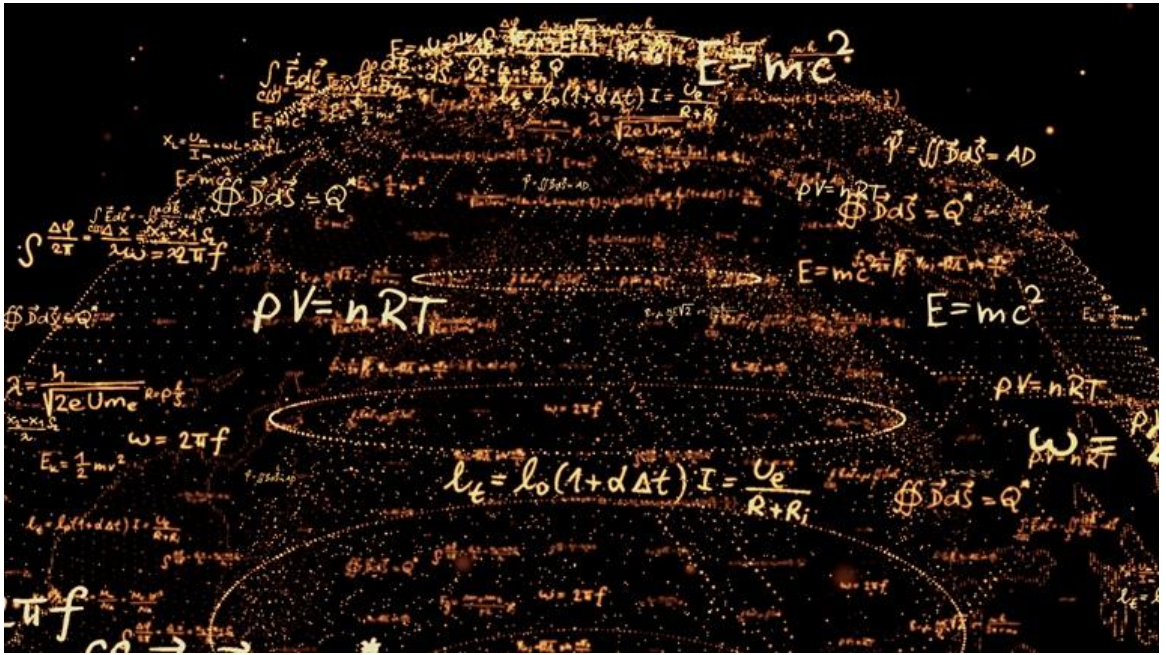
Lesson 9b: Applications of Cryptography



Digital certificates

- PKI (public key infrastructure) uses asymmetric key pairs and combines software, encryption and services to provide a means of protecting security of business communication and transactions.
- PKCS (Public Key Cryptography Standards) Put in place by RSA to ensure uniform Certificate management throughout the internet.
- A Certificate is a digital representation of information that identifies you as a relevant entity by a trusted third party (TTP)
- A CA (Certification Authority) is an entity trusted by one or more users to manage certificates.
- RA (Registration Authority) Used to take the burden off of a CA by handling verification prior to certificates being issued. RA acts as a proxy between user and CA. RA receives request, authenticates it and forwards it to the CA.
- CPA (Certificate Practice Statement) describes how the CA plans to manage the certificates it issues.
- CP (Certificate Policy) is a set of rules that defines how a certificate may be used.

Digital certificates Continued

- X.509 This is an international standard for the format and information contained in a digital certificate. X.509 is the most common type of digital certificate in the World. It is a digital document that contains a public key signed by the trusted third party which is known as a Certificate Authority, or CA.
- CRL (Certificate Revocation List) is a list of certificates issued by a CA that are no longer valid. CRLs are distributed in two main ways: PUSH model: CA automatically sends the CRL out a regular intervals. Pull model: The CRL is downloaded from the CA by those who want to see it to verify a certificate. End user is responsible.
- Status Checking: The concept of Status checking is to use a relying party to “real-time” check the validity of evidence supporting a high-value transaction. CRLs are created with specific lifetimes (possibly unbounded) they are not suitable for real-time status checks. The most prominent technology proposed for this type of verification within the PKIX infrastructure is the “Online Certificate Status Checking Protocol” [OCSP], and it is on track to become an Internet standard. OCSP has two important characteristics: first, OCSP depends upon the emergence of its own three-tier (Client - Certificate Authority – Designated Responder) infrastructure, and second, OCSP defines a new set of message formats extending beyond those contained in the base PKIX standard

Uses of Digital Certificates

- Bind a user's identity to a public key
- Encrypt channels to provide secure communication between clients and servers
- Encrypt messages for sécure Internet e-mail communication
- Verify the identity of clients and servers on the Web
- Verify the source and integrity of signed executable code

TYPES OF DIGITAL CERTIFICATES

Personal digital certificates

- Used to send email from one person to another
- Free from Thawte

Server digital certificates

- Used by Web servers to make HTTPS connections
- $250 / year from Thawte

Software publisher digital certificates

- $300 / year from Thawte

Types of Digital Certificates (continued)

Single-sided certificate	Dual-sided certificates
Contains both the signature and the encryption information	Certificates in which the functionality is split between two certificates Signing certificate Encryption certificate

Managing Digital Certificates

For Alice and Bob to use asymmetric cryptography:

Alice and Bob must generate public and private keys

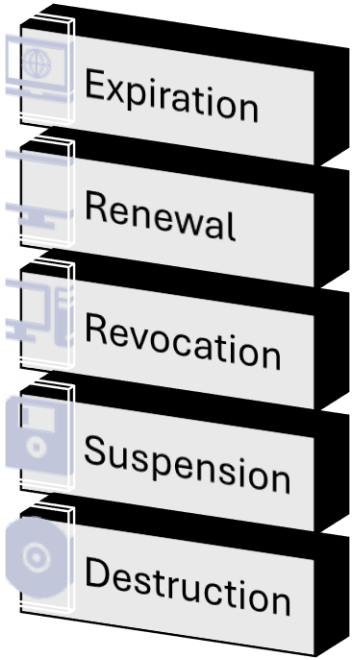
A Certificate Authority (CA) or Registration Authority (RA) must verify the identities of Alice and Bob

The certificates must be placed in a Certificate Repository (CR)

When they expire, they must be placed on a Certificate Revocation List (CRL)

All these things are done by Public key infrastructure (PKI)

DIGITAL CERTIFICATES CONTINUED- CANCELLATION AND HISTORY PHASE



X.509 certificate content

- Version
- Certificate holder’s public key info
  - Public Key Algorithm
  - Certificate holder’s Public Key
- Serial number
- Certificate holder’s distinguished name
- Certificate’s validity period
- Unique name of certificate issuer
- Digital signature of issuer
- Signature algorithm identifier

- RFC 5280

X.509 certificate signature

- To validate a certificate, one needs a second certificate that matches the Issuer (Thawte Server CA) of the first certificate. First, one verifies that the second certificate is of a CA kind; that is, that it can be used to issue other certificates. This is done by inspecting a value of the *CA* attribute in the *X509v3 extension* section. Then the RSA public key from the CA certificate is used to decode the signature on the first certificate to obtain a MD5 hash, which must match an actual MD5 hash computed over the rest of the certificate. The data is hashed, and the hash is signed

- According to the RFC 5280 “The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as the input to the signature function.”

CA – VERISIGN

- Class 1 for individuals, intended for email.
- Class 2 for organizations, for which proof of identity is required.
- Class 3 for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority.
- Class 4 for online business transactions between companies.
- Class 5 for private organizations or governmental security.

Managing Digital Certificates

For Alice and Bob to use asymmetric cryptography:

Alice and Bob must generate public and private keys

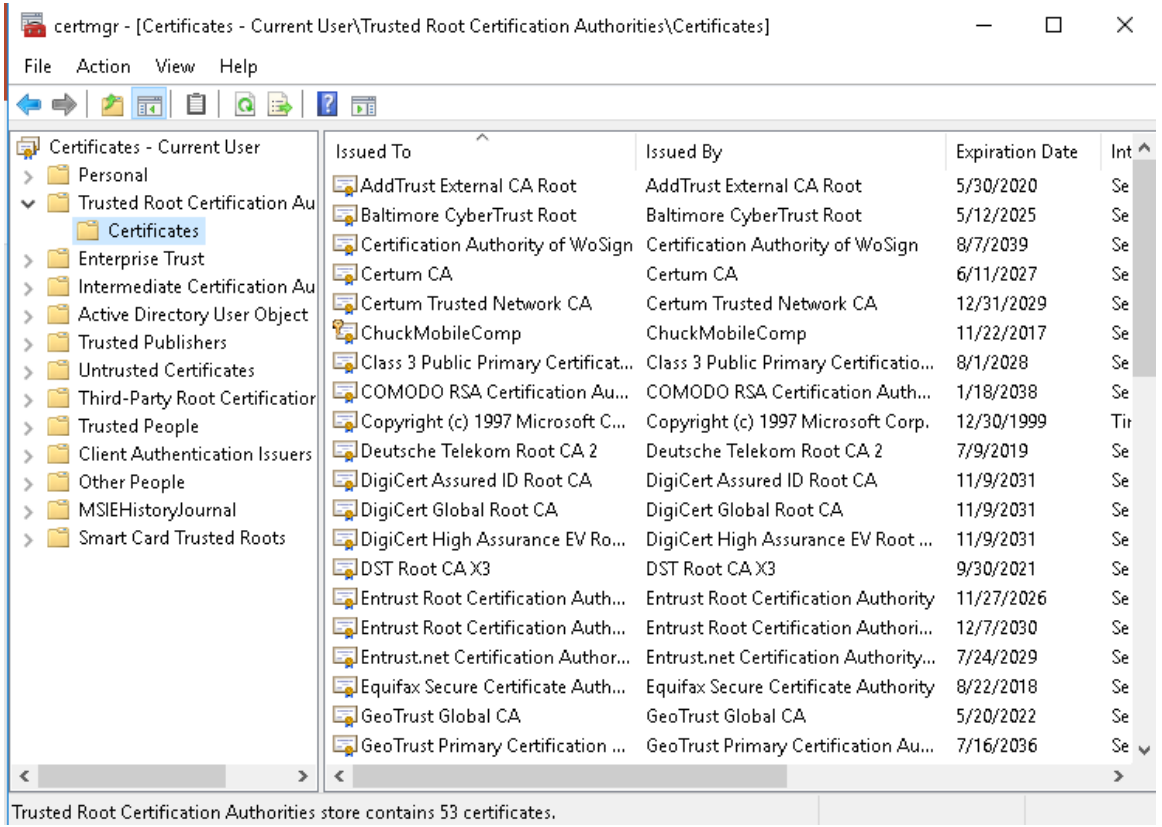
A Certificate Authority (CA) or Registration Authority (RA) must verify the identities of Alice and Bob

The certificates must be placed in a Certificate Repository (CR)

When they expire, they must be placed on a Certificate Revocation List (CRL)

All these things are done by Public key infrastructure (PKI)

Certificate Store



Public Key Infrastructure (PKI)

Public key infrastructure involves

- Public-key cryptography standards
- Trust models
- Key management

PKI – Stapling and Pinning

Stapling is a method used with OCSP, that allows a web server to provide information on the validity of its own certificate, rather than needing to go to the certificate vendor. This is done by the web server essentially downloading the OCSP response from the certificate vendor in advance, and providing that to browsers.

Pinning is a method designed to mitigate the use of fraudulent certificates. Basically, once a public key or certificate has been seen for a specific host, that key or certificate is pinned to the host. Should a different key or certificate be seen for that host, that might indicate an issue with a fraudulent certificate.

.

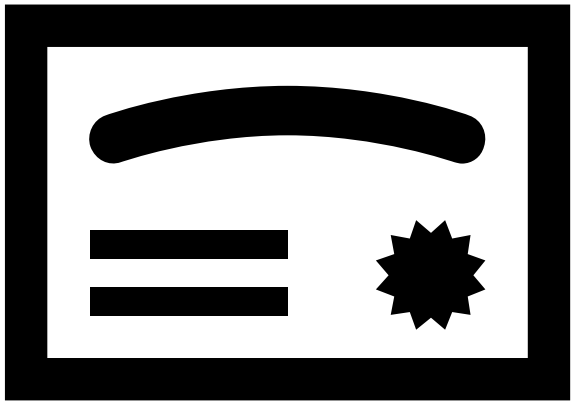
PKI – Offline CA

Certificate authorities can be online or offline. Online certificate authorities are the most common. They are always connected and always accessible. Offline is usually for a root certificate authority that has been isolated from network access. It is brought online for specific purposes. The concept is that, since it is isolated, the chances of it being compromised are reduced. That is one reason why this is usually only done with root certificate authorities.

.

Digital certificates Continued- Key recovery agents

- Person who can recover keys from the keystore on behalf of a user
- Highly-trusted person
- Issue recovery agent certificate
  - EFS Recovery Agent certificate
  - Key Recovery Agent certificate

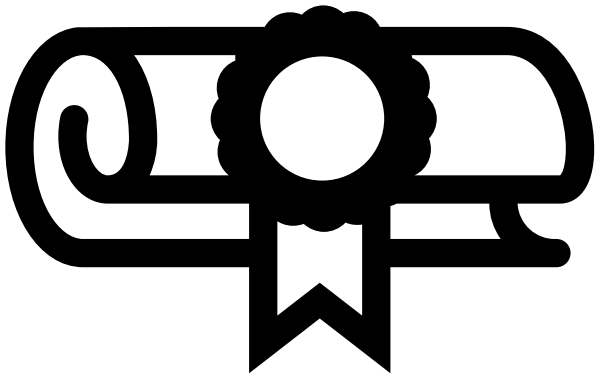


More on certificates

- A root certificate is either an unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme
- Root certificates are updated on Windows automatically. When a user visits a secure Web site (by using HTTPS SSL), reads a secure email (S/MIME), or downloads an ActiveX control that is signed (code signing) and encounters a new root certificate, the Windows certificate chain verification software checks the appropriate Microsoft Update location for the root certificate. If it finds it, it downloads it to the system. To the user, the experience is seamless. The user does not see any security dialog boxes or warnings. The download happens automatically, behind the scenes.

EV certificates

Extended Validation (EV) SSL Certificates: where the Certificate Authority (CA) checks the right of the applicant to use a specific domain name PLUS it conducts a THOROUGH vetting of the organization. The issuance process of EV SSL Certificates is strictly defined in the EV Guidelines, as formally ratified by the CA/Browser forum in 2007, that specify all the steps required for a CA before issuing a certificate



Other certificate types

Organization Validation (OV) SSL Certificates: where the CA checks the right of the applicant to use a specific domain name PLUS it conducts some vetting of the organization. Additional vetted company information is displayed to customers when clicking on the Secure Site Seal, giving enhanced visibility in who is behind the site and associated enhanced trust.

Domain Validation (DV) SSL Certificates: where the CA checks the right of the applicant to use a specific domain name. No company identity information is vetted and no information is displayed other than encryption information within the Secure Site Seal

Other certificate types

Wildcard certificates, as the name suggests, can be used more widely. Usually with multiple sub-domains of a given domain. So rather than have a different X.509 certificate for each sub-domain, you would use a wild card certificate for all sub-domains.

SAN or Subject Alternative Name is not so much a type of certificate as a special field in X.509. It allows you to specify additional items (IP addresses, domain names, etc.) to be protected by this single certificate.

Code signing certificates where mentioned earlier in this chapter. These are X.509 certificates used to digitally sign some type of computer code.

Other certificate types

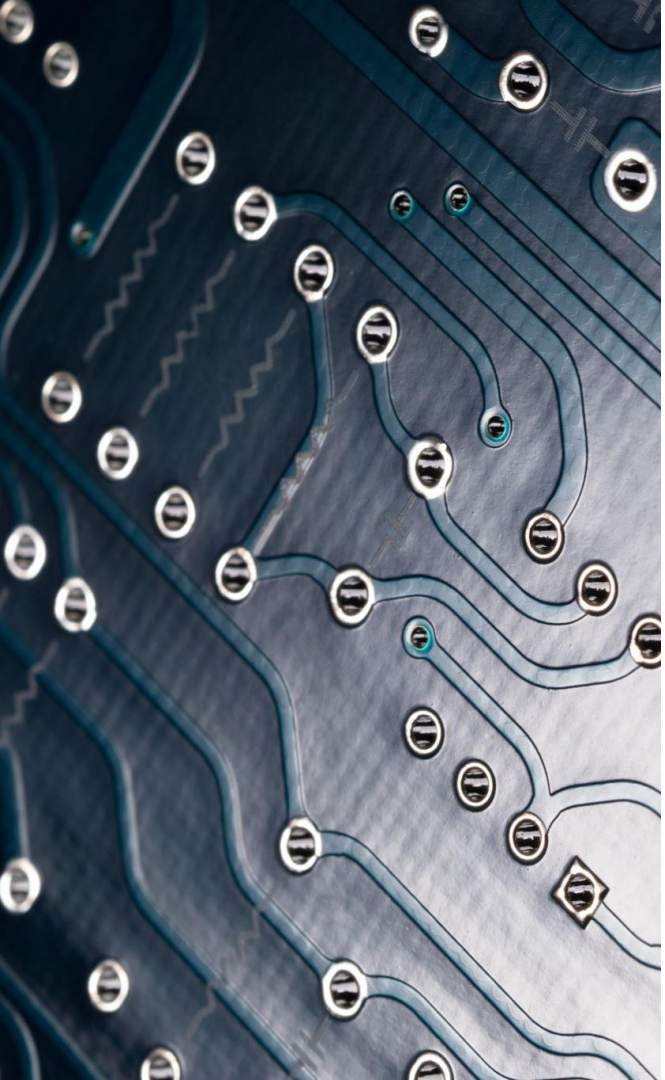
- Machine/computer certificates are X.509 certificates assigned to a specific machine. These are often used in authentication schemes. For example, in order for the machine to sign into the network, it must authenticate using its machine certificate.
- Email certificates are used for securing email. Secure Multipurpose Internet Mail Extension (S/MIME) uses X.509 certificates to secure email communications.
- User certificates are used for individual users. Like machine/computer certificates, these are often used for authentication. The user must present his or her certificate to authenticate prior to accessing some resource.

PKCS Standards

- PKCS #1: RSA Cryptography Standard
- PKCS #2: Incorporated in PKCS #1
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #4: Incorporated in PKCS #1
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #14: Pseudorandom Number Generators
- PKCS #15: Cryptographic Token Information Format Standard

Certificate file extension

- .pem - (Privacy Enhanced Mail) Base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----“
- .cer, .crt, .der - usually in binary DER form, but Base64-encoded certificates are common too .p7b, .p7c - PKCS#7 Signed Data structure without data, just certificate(s) .p12 - PKCS#12, may contain certificate(s) (public) and private keys (password protected)
- .pfx - PFX, predecessor of PKCS#12



Hardware Encryption

- Full disk encryption (FDE) or whole disk encryption often signify that everything on disk is encrypted
- Disk encryption does not replace file encryption
- Trusted Platform Module (TPM) is a secure cryptoprocessor embedded in the motherboard that can be used to authenticate a hardware device
- TPM can be used to tie the hard disk drive (HDD) encryption to a particular device. If the HDD is removed from that particular device and placed in another, the decryption process will fail
- *Hardware Security Modules (HSMs)* are devices that handle digital keys. They can be used to facilitate encryption as well as authentication via digital signatures. Most HSMs support tamper resistant mechanisms to prevent the tampering of the keys.

File and Drive encryption

File Encryption

- Prevents alteration of data
- Prevents file from being replaced
- Usually uses public key
- Windows uses EFS
  - Enhances NTFS permissions security
  - Might need cipher.exe to decrypt files

Drive Encryption

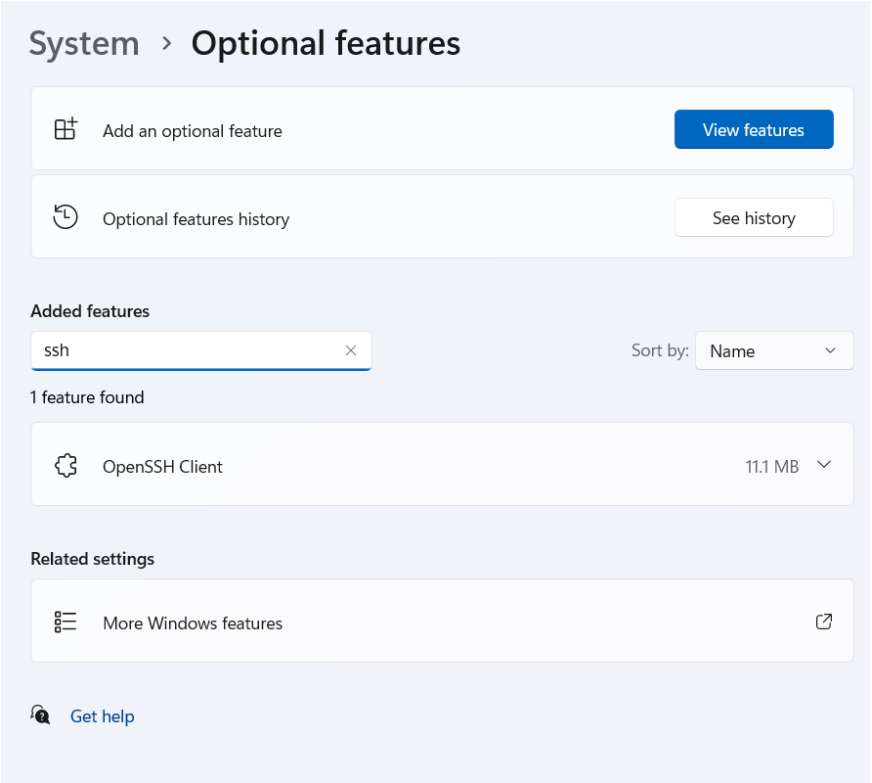
- Microsoft Bit Locker
- Key stored on separate device
- Requires TPM or USB flash drive

SSH in Windows

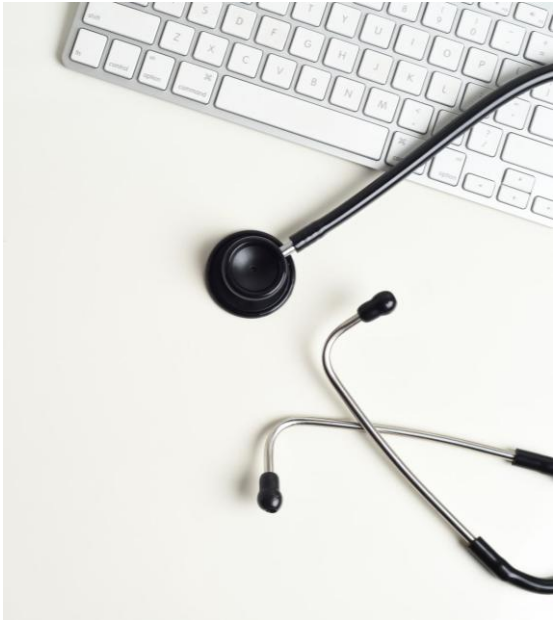
The latest builds of Windows 10 and Windows 11 include a built-in SSH server and client that are based on OpenSSH, a connectivity tool for remote sign-in that uses the SSH protocol. OpenSSH encrypts all traffic between client and server to eliminate eavesdropping, connection hijacking, and other attacks.

SSH in Windows

SSH Client is an optional feature one can easily add in Windows 10 or 11



SSH in Windows



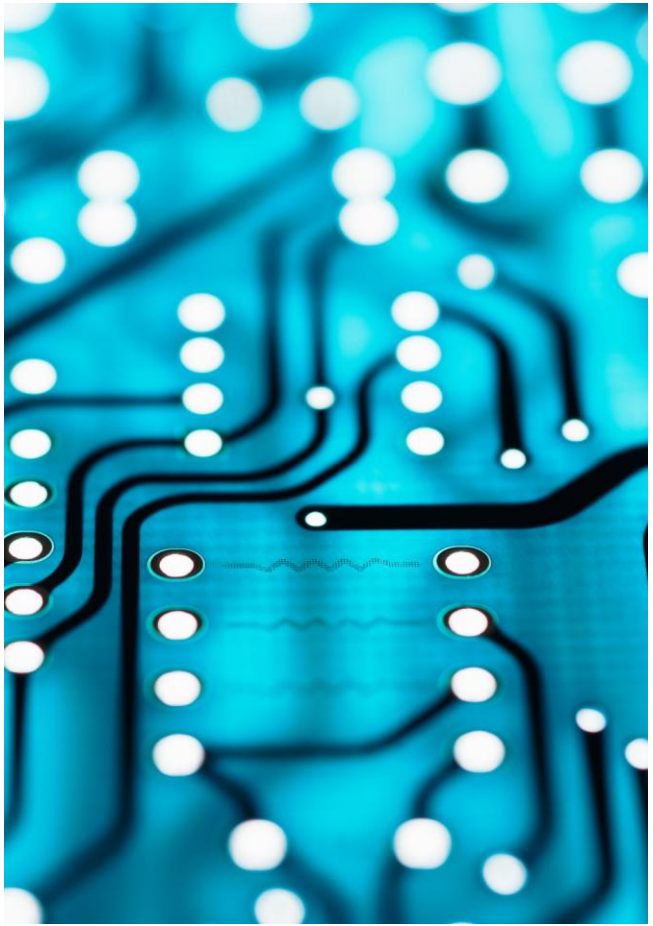
You can start an SSH session in your command prompt by executing ssh user@machine and you will be prompted to enter your password. You can create a Windows Terminal profile that does this on startup by adding the commandline setting to a profile in your settings.json file inside the list of profile objects.

You can also run these commands from PowerShell if you prefer.

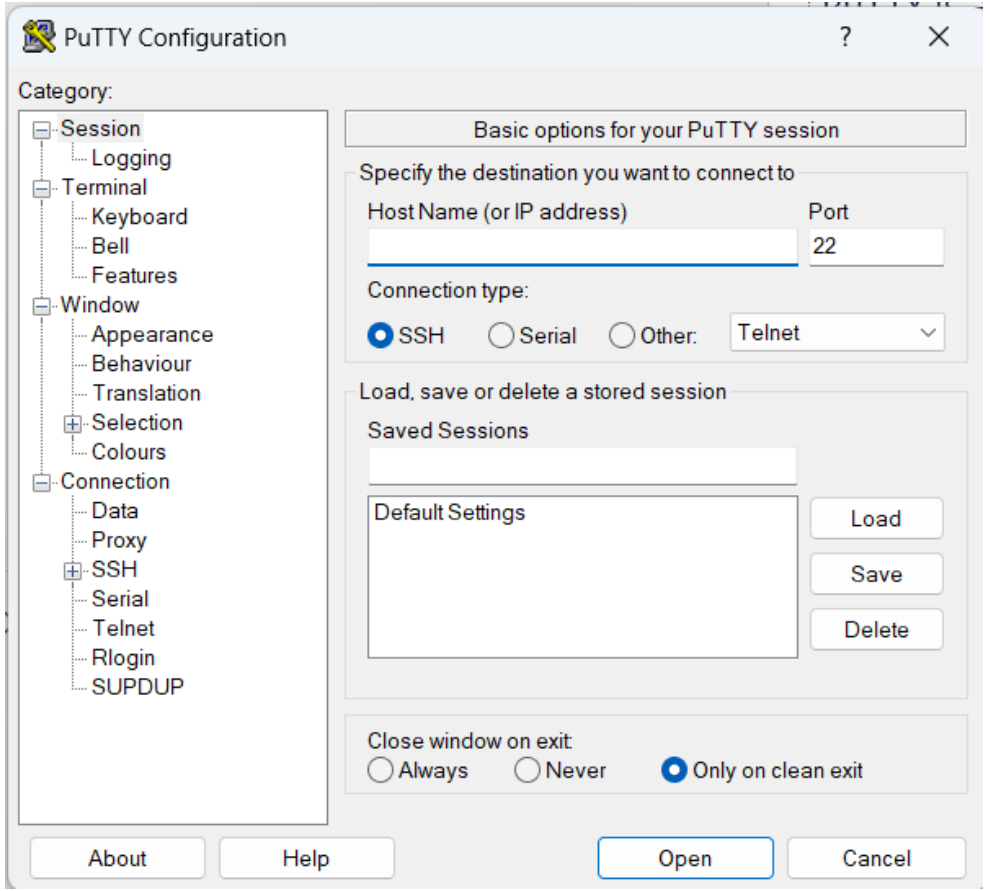
SSH in Windows using PuTTY

https://www.putty.org/

PuTTY is a free and open-source terminal emulator, serial console, and network file transfer application. It supports various network protocols, including SSH (Secure Shell), Telnet, rlogin, and raw socket connection. Developed originally by Simon Tatham for the Windows platform, PuTTY is now available for various operating systems, including Unix-like systems.



SSH in Windows using PuTTY



SSH in Windows using PuTTY

SH Client: PuTTY is most commonly used as an SSH client, allowing secure remote login and command execution on servers. It supports SSH-1 and SSH-2 protocols.

Terminal Emulator: It provides a terminal emulator for running commands on a remote machine as if you were directly connected to it.

Telnet Client: PuTTY can connect to remote computers using the Telnet protocol, though this is less secure than SSH.

Serial Console: It can be used as a serial console, allowing you to connect to devices through serial ports, often used for managing network devices and embedded systems.

Network File Transfer: PuTTY includes tools like PSCP (PuTTY Secure Copy) and PSFTP (PuTTY Secure File Transfer Protocol) for transferring files securely between local and remote machines.

Configurable Settings: Users can configure numerous settings, including terminal behavior, keyboard mappings, window appearance, and network-related options.

SSH in Windows using PuTTY

PuTTY: The main terminal emulator application.

PSCP: A command-line tool for copying files between computers using SCP (Secure Copy Protocol).

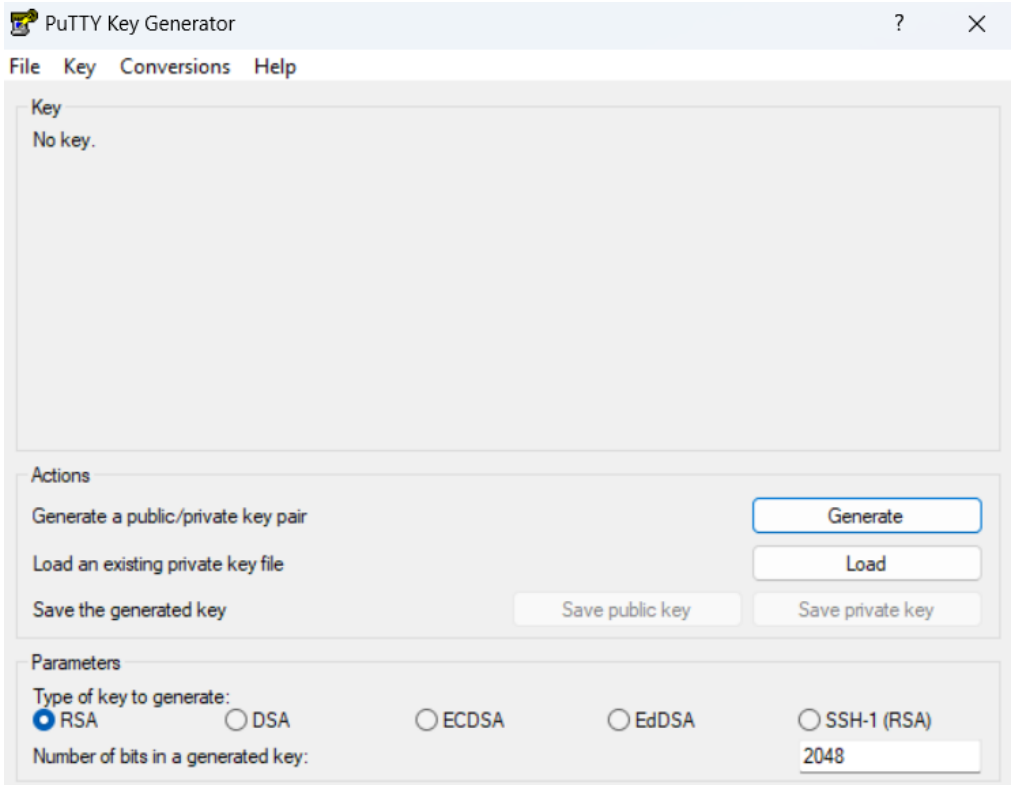
PSFTP: A command-line tool for interactive file transfer sessions using SFTP (Secure File Transfer Protocol).

PuTTYgen: A key generation tool for creating SSH key pairs for secure authentication.

Pageant: An SSH authentication agent for managing private keys.

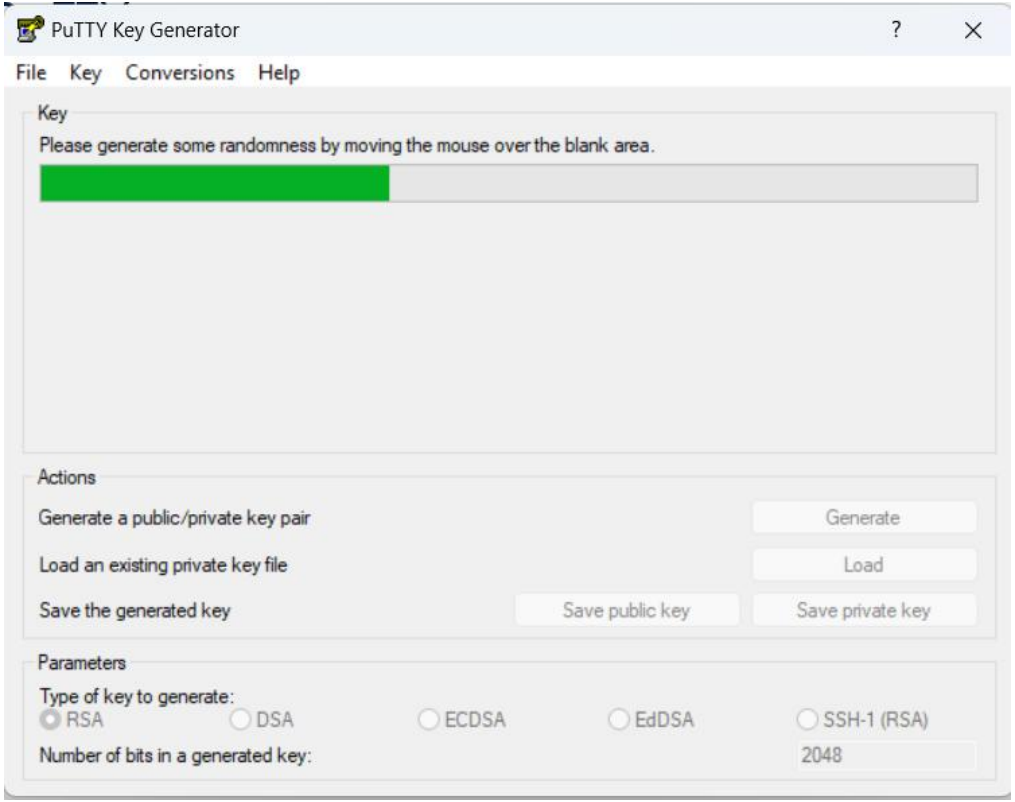
PuTTY

Also has a key generation tool for generating cryptographic keys.



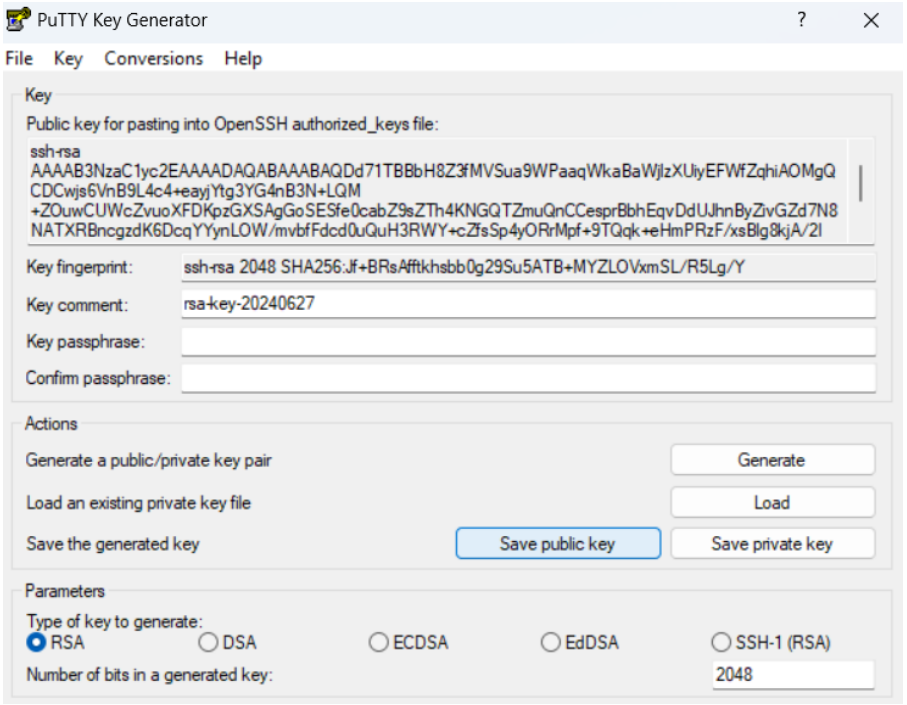
PuTTY

Also has a key generation tool for generating cryptographic keys.



PuTTY

Also has a key generation tool for generating cryptographic keys.



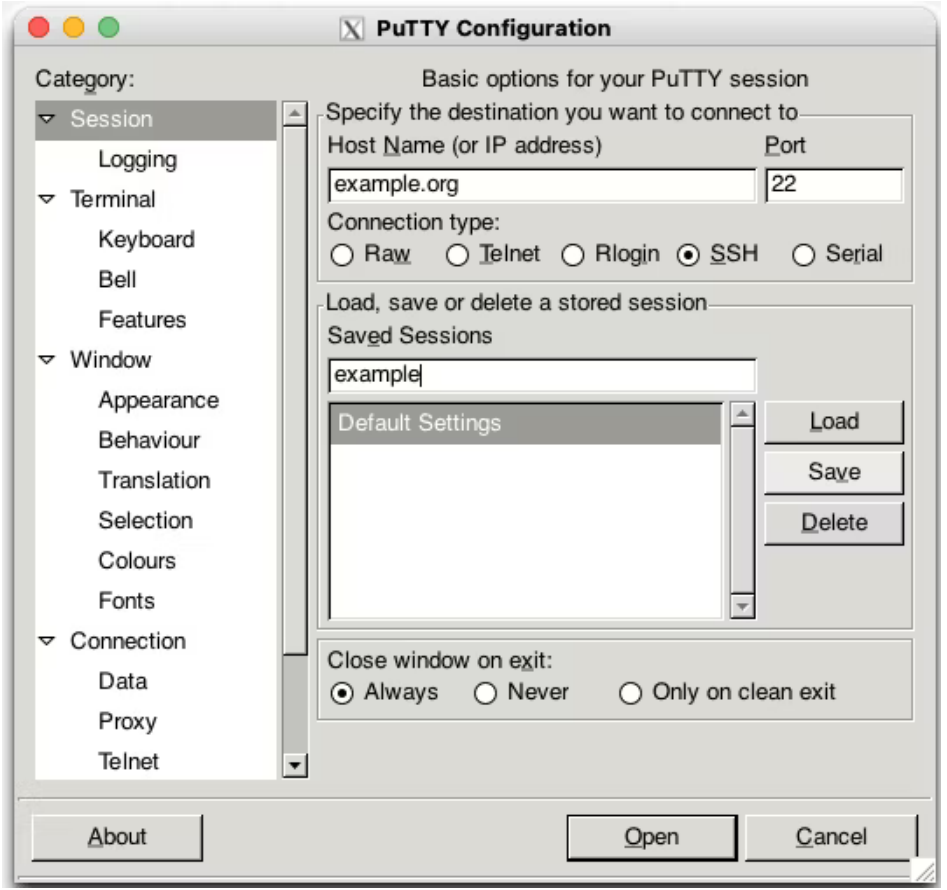
SSH For Mac

Like Windows, the macOS has both a built in SSH client, and there is a PuTTY client for it.

1. Open Terminal on your Mac.
2. Run this command: sudo port install putty
3. This should download and install three programs into /opt/local/bin: putty, puttygen, and puttytel.
4. /opt/local/bin should be in your PATH, so you should be able to run PuTTY from the command line by typing simply: putty
5. Using a symlink or Mac alias, you can create a shortcut to putty to open it more easily. For example, to add an icon to your Desktop ln -s /opt/local/bin/putty ~/Desktop/PuTTY

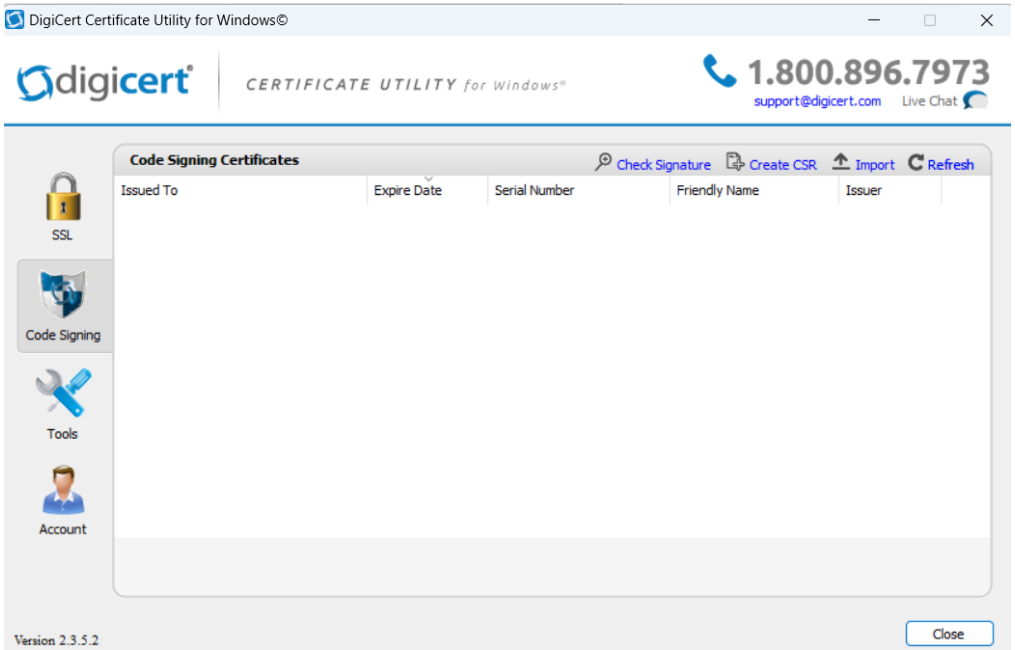
https://www.ssh.com/academy/ssh/putty/mac

SSH For Mac


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Fonts
Connection
Data
Proxy
Telnet
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
example.org
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
example
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

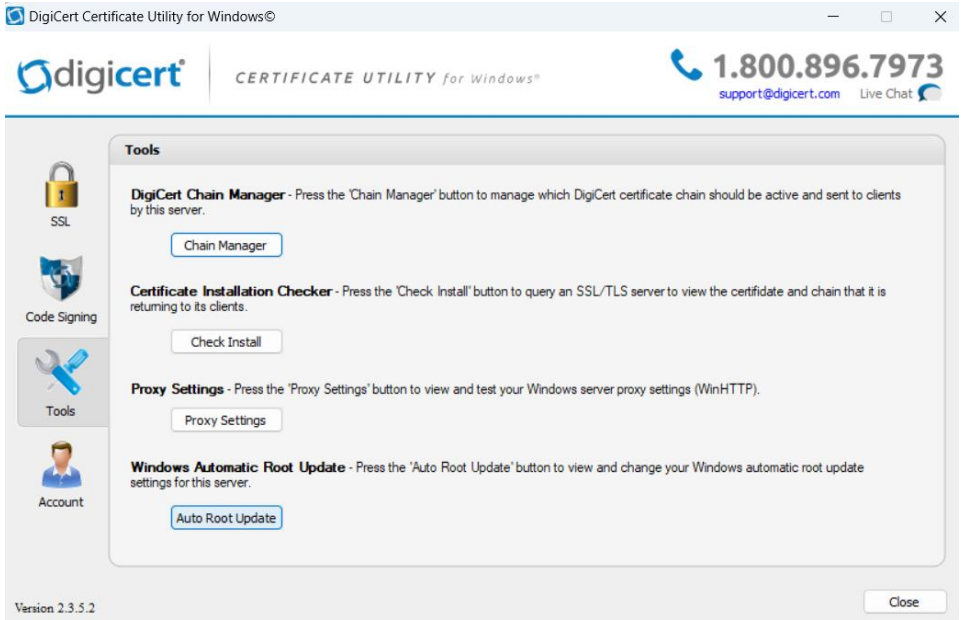
Digicert for Windows

https://www.digicert.com/support/tools/certificate-utility-for-windows



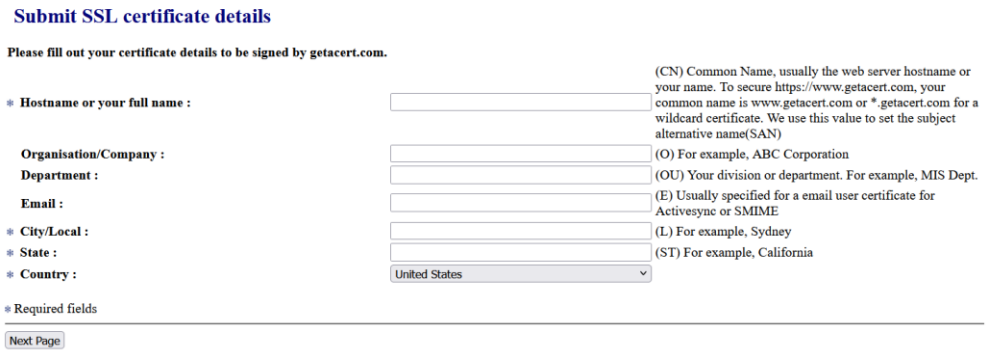
Digicert for Windows

https://www.digicert.com/support/tools/certificate-utility-for-windows



Create Digital Certificates Online

https://getacert.com/getacert.html



Submit SSL certificate details

Please fill out your certificate details to be signed by getacert.com.

* **Hostname or your full name :**		(CN) Common Name, usually the web server hostname or your name. To secure https://www.getacert.com, your common name is www.getacert.com or *.getacert.com for a wildcard certificate. We use this value to set the subject alternative name(SAN)
Organisation/Company :		(O) For example, ABC Corporation
Department :		(OU) Your division or department. For example, MIS Dept.
Email :		(E) Usually specified for a email user certificate for Activesync or SMIME
* **City/Local :**		(L) For example, Sydney
* **State :**		(ST) For example, California
* **Country :**	United States	

* Required fields

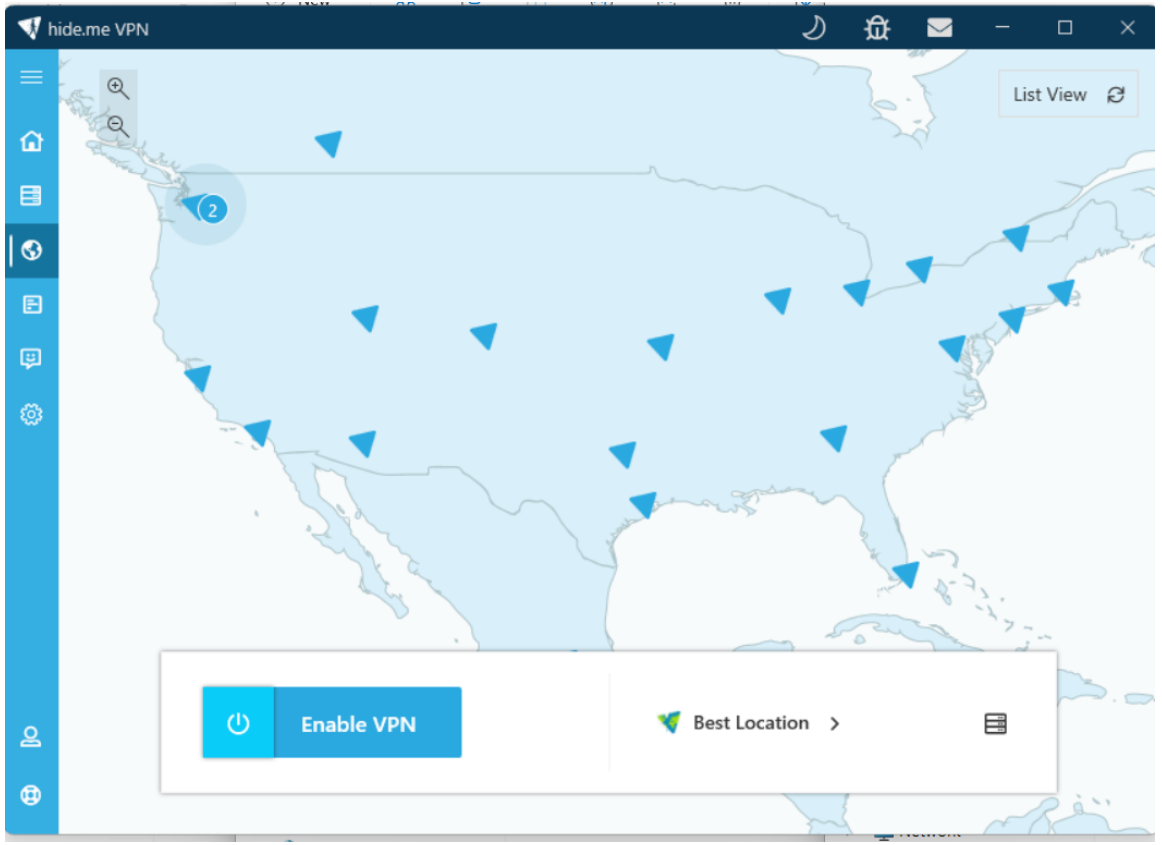
Next Page

Free VPN software for Windows

https://protonvpn.com/free-vpn/windows

Free VPN software for Windows

https://hide.me/en/software/windowsv4/download

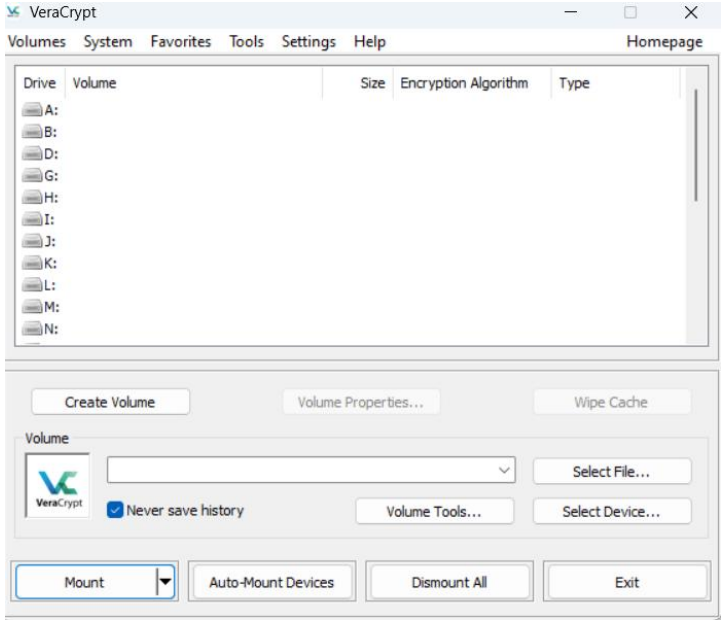


Proxy Servers

- List of proxy servers one can use https://www.proxynova.com/proxy-server-list/
- Another list of know proxy servers https://spys.one/en/

Vera Crypt

https://www.veracrypt.fr/en/Downloads.html Available for Windows, macOS, and Linux

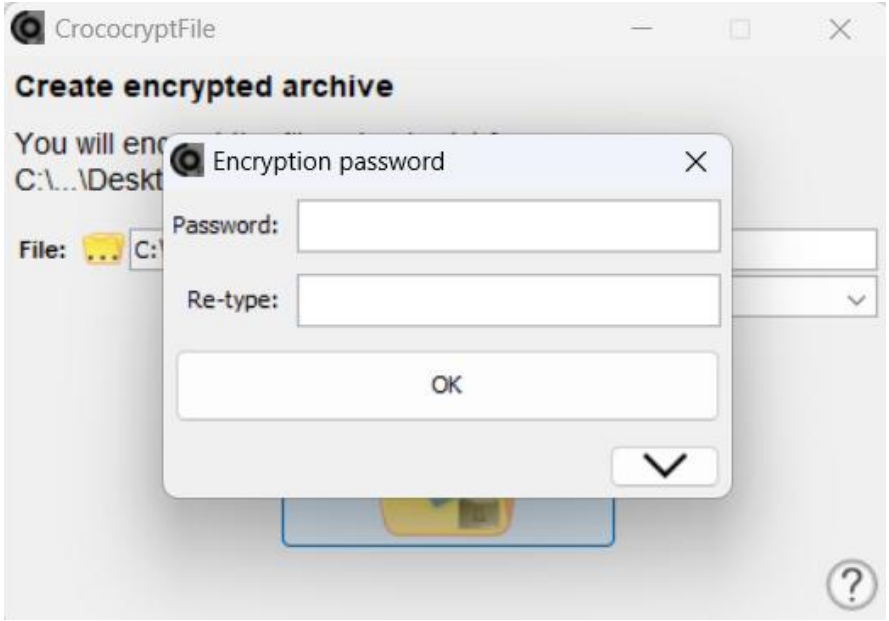


Crococrypt

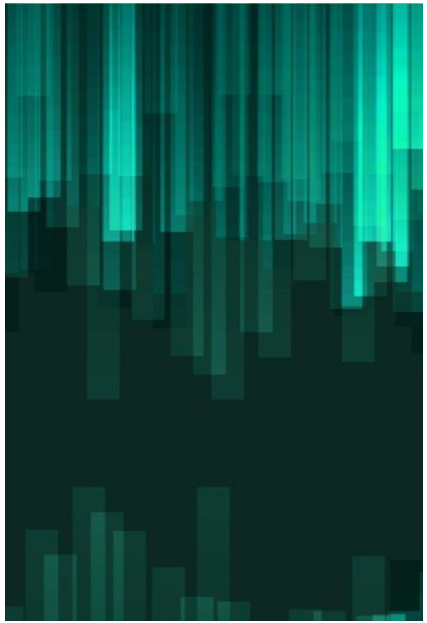
- https://www.majorgeeks.com/files/details/crococryptfile.html

Crococrypt

https://www.majorgeeks.com/files/details/crococryptfile.html



Steganography



- **Steganography** refers to any methodology used to hide a message (including text, sound, or picture) in a separate file. Most commonly text or an image is inserted into another image. However, there are permutations where video is hidden in another video, or sound in sound or even sound in video. The image/sound/video that the underlying message is hidden in is referred to as a carrier or cover file or signal.

- The most common implementation of steganography utilizes the least significant bits in a file in order to store data. By altering the least significant bit one can hide additional data without altering the original file in any noticeable way.

Historical Steganography

The ancient Chinese wrapped notes in wax and swallowed them for transport.

Histaius wanted to communicate regarding a revolt against the Persians. He shaved the hair on one of his slaves head, then tattooed the message and after the hair grew back sufficiently, sent the slave with the message.

A man named Demaratus was purported to have written messages regarding Xerxes impending invasion. The messages were on wax covering wood, Demaratus had a second message directly on the wood.

Historical Steganography

In 1518 Johannes Trithmeus wrote a book on cryptography and described a technique where a message was hidden by having each letter taken as a word from a specific column.

Morse code has been written into yarn, then the yarn sown into clothing.

Steganography details - LSB

- With least significant bit (lsb) replacement, certain bits in the carrier file are replaced.

Steganography details - LSB

Before change

Red 0

Green 33

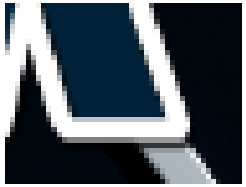
Blue 55

After change

Red 0

Green 33

Blue 54



The entire file has 469,032 bytes. If you change only 10% of them you can store 1 bit per byte, or 46,903 bits which is 46 KB

Steganography Terms

Payload

Carrier

Channel

Lossy vs lossless

Lossless algorithms that allows the original data to be perfectly reconstructed from the compressed data. Lossy (TIFF, JPEG) methods use an approximation that may lose some data.

Lossless and Lossy Compression

Lossless compression

- Reduces file size without removing data
- Can use either Huffman or Lempel-Ziv-Welch coding
- WinZip and PKZip both use lossless compression

Lossy compression

- As the name suggest you actually lose bits of information
- **Vector quantization (VQ)**
  - Determines what data to discard based on vectors in the graphics file
- LZIP uses Lossy compression

Other forms of Steganography

Echo Hiding: This method adds extra sound to an echo inside an audio file, that extra sound conceals information.

Discrete Cosine Transform is often used for Video steganography. This method alters values of certain parts of the individual frames. The usual method is to round up the values.

How to embed

Sequential

Random

Specific

Steganograpic File Systems

- Stores data in seemingly random files

- Proposed by Ross Anderson, Roger Needham, and Adi Shamir. Their paper proposed two main methods of hiding data: in a series of fixed size files originally consisting of random bits on top of which 'vectors' could be superimposed in such a way as to allow levels of security to decrypt all lower levels but not even know of the existence of any higher levels, or an entire partition is filled with random bits and files hidden in it.

Stego Tools

- S-Tools
- Hermetic Stego (image)
- ImageHide
- JPHIDE and JPSEEK
- StagaNote
- OutGuess
- gifShuffle
- QuickStego
- MP3Stegz (audio)
- Our Secret
- Xiao Staganography
- OmniHide Pro
- Masker

Stealth Files

MP3Stego

Steghide

Audiostegano

Hide4PGP

FoxHole

Data Stash

Byte Shelter

StegParty

SpamMimic

StegoStick

Hide My Files

Steganalysis

By analyzing changes in an image's close color pairs, the steganalyst can determine if LSB substitution was used. Close color pairs consist of two colors whose binary values differ only in the LSB.

Steganalysis - RQP

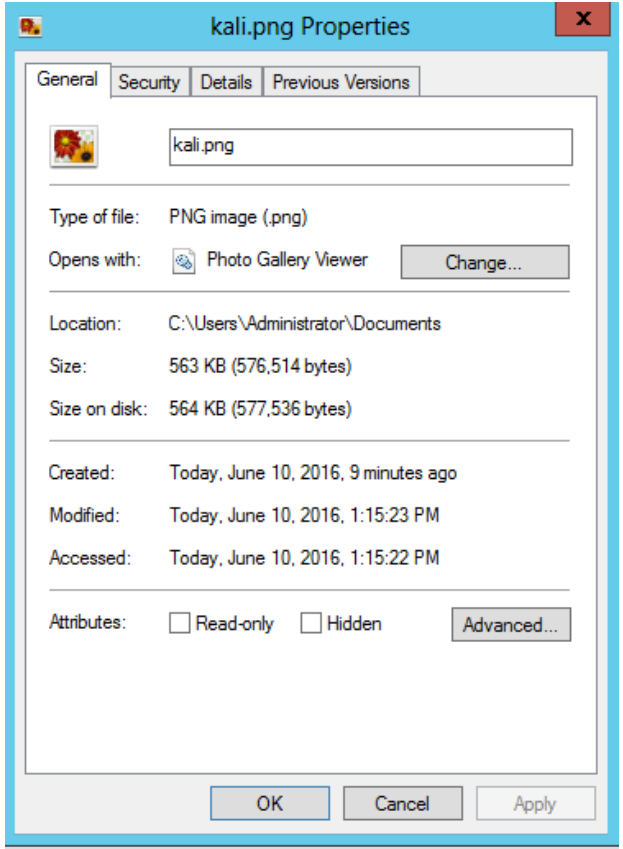
- The Raw Quick Pair method
  - Based on statistics of the numbers of unique colors and close-color pairs in a 24-bit image.
  - Analyzes the pairs of colors created by LSB embedding
  - Countermeasure - Maintaining the color palette without creating new colors

Steganalysis – Examine Edges

Many images and audio files use lossy compression (JPEGs and MP3's both do). In JPEG it is common that components like the high-contrast edges of black text on white background will distorted neighboring pixels, usually in a predictable fashion (edge ringing). Looking for unexpected values in the edge ringing can indicate steganography was used.

Steganalysis – Modification date

Most average users don’t modify images or music files. Look for recent modification dates that do not match creation dates.



What affects steganalysis

- Carrier to Payload Ratio
- Presence of tools
- Area to check

Steganography Detection Tools

- Outguess Xdetect is one tool http://www.outguess.org/detection.php
- Steg Secret is another tool http://stegsecret.sourceforge.net/
- StegSpy has fewer limitations than StegDetect http://www.spy-hunter.com/stegspydownload.htm
- AccessData's Forensic Toolkit and Guidance Software's Encase can detect steganography.

StegDetect

- stegdetect -t p sample.jpg
- Tries to detect the presence of embedded information in sample.jpg.
- **stegdetect** works only for JPEG images.

StegDetect Continued

The StegDetect utility analyses image files for steganographic content. It runs statistical tests to determine if steganographic content is present, and also tries to find the system that has been used to embed the hidden information.

The options are as follows:

—q Only reports images that are likely to have steganographic content.

—n Enables checking of JPEG header information to suppress false positives. If enabled, all JPEG images that contain comment fields will be treated as negatives.

—V Displays the version number of the software.

—s float Changes the sensitivity of the detection algorithms. Their results are multiplied by the specified number. The higher the number the more sensitive the test will become. The default is 1.

—d num Prints debug information.

—t tests

Sets the tests that are being run on the image. The following characters are understood:

j Tests if information has been embedded with jsteg.

o Tests if information has been embedded with outguess.

p Tests if information has been embedded with jphide.

i Tests if information has been hidden with invisible secret