Introduction to Cryptography

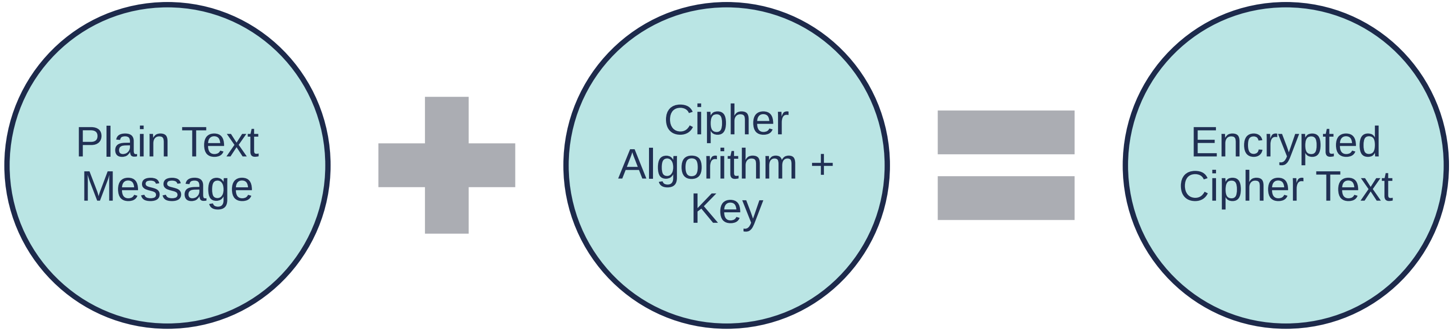
Cryptography

- **Greek Word**: “Krypto” = Hidden / Secret
- Core Features of Cryptography:
  - **Confidentiality**: Prevents unauthorized disclosure of data
  - **Integrity**: Ensure data isn’t modified
  - **Authentication**: Used to validate sender with digital signatures
  - **Non-repudiation**: Digital signatures also ensure non-repudiation

Cryptography Basics

- **Plain Text**
  - An unencrypted message
- **Cipher Text**
  - An encrypted message
- **Cipher**
  - The encryption algorithm used to encrypt & decrypt the message
- **Key**
  - Determines the output of the cipher algorithm and is needed to encrypt and decrypt a message

Encrypting a Message



Plain Text Message

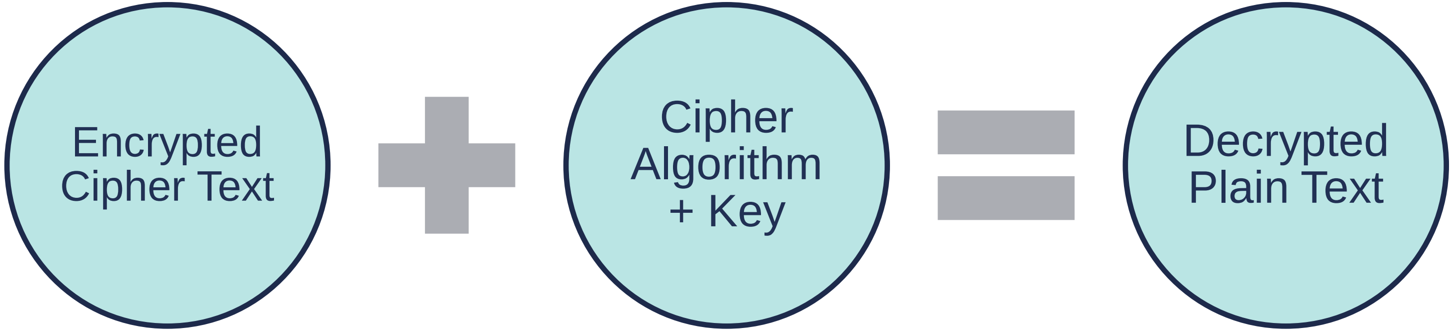
+

Cipher Algorithm + Key

=

Encrypted Cipher Text

Decrypting a Message

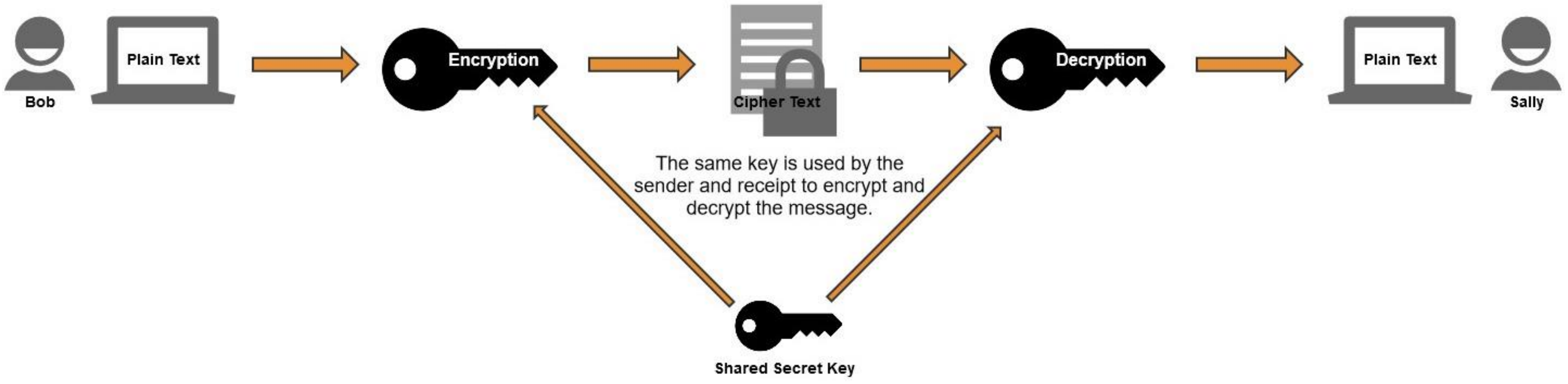


Encrypted Cipher Text + Cipher Algorithm + Key = Decrypted Plain Text

Symmetric Encryption

Symmetric (Private Key) Encryption

- Symmetric encryption uses a **single key** for **encryption** and **decryption**.
- Both the **sende**r and **receiver** have the **same key** and use it to encrypt and decrypt all messages.
- It's also known as **secret-key encryption** or **private-key** encryption.

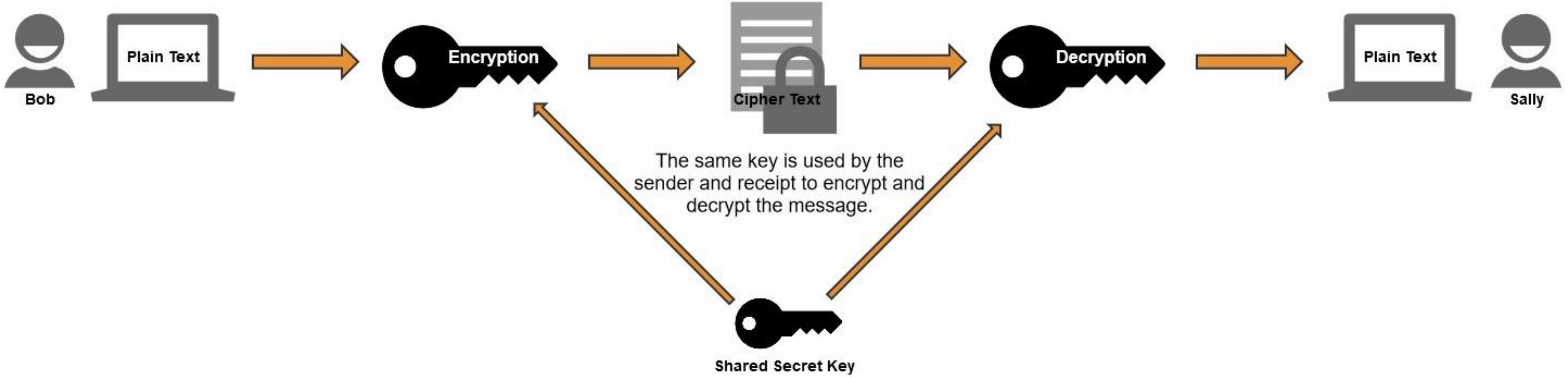


The same key is used by the sender and receipt to encrypt and decrypt the message.

INSTRUCTOR
ALTON

Symmetric (Private Key) Encryption

- **Symmetric encryption** is much more efficient at encrypting large amounts of data than its counterpart, **asymmetric encryption**.
- The downside of symmetrical encryption is that it makes it hard to initiate communication the first time.
- How do you securely transmit the private key to each user?



The same key is used by the sender and receipt to encrypt and decrypt the message.

Symmetric Encryption Algorithm: DES & 3DES

Data Encryption Standard (DES)

- DES is an older algorithm that widely used for a period of time dating back to the 1970's.
- It has been compromised and no longer secure.

Triple DES (3DES)

- 3DES was developed as an improvement over DES.
- It improved the encryption by encrypting the data with DES three times with two, or sometimes three keys.
- While 3DES is a significant improvement over DES, it consumes a lot of processer power and memory resources.
- AES is much less resource-intensive and has replaced 3DES as the current standard.

Symmetric Encryption Algorithm: AES

Advanced Encryption Standard (AES)

- AES is a very strong encryption algorithm that’s commonly used worldwide.
- It’s significantly faster than both DES and 3DES and also provides stronger encryption.
    - 128-Bit AES would take billion of years to brute force
- It’s also the “official” encryption standard for the U.S. government (since 2002).

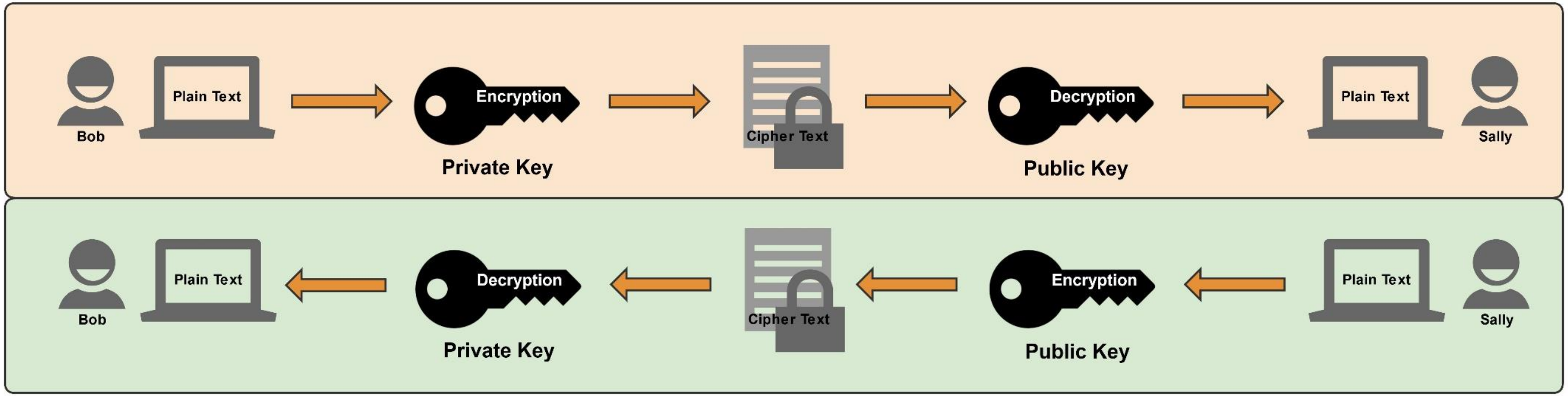
Asymmetric Encryption

Asymmetric (Public Key) Encryption

- Asymmetric encryption uses two keys, a public key and a private key created as a matched pair.
    - **Private Key**: Kept secret and never shared.
    - **Public Key**: Shared with others.
- Commonly referred to as:
    - Public Key Encryption
    - Public Key Infrastructure (PKI) Encryption

How Public Key Encryption Works

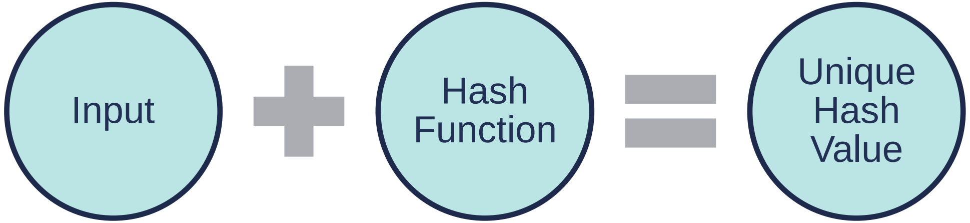
- Anything encrypted with the **private key** can only be decrypted with the matched **public key**.
- Anything encrypted with the **public key** can only be decrypted with the matched **private key**.



Hashing Algorithms

Hashing

- Hashing is the process of converting an input (data) into a fixed-size string of text.
- It’s a one-way function, meaning you can’t use a hash value to determine its input data.
- Hashing is used to provide data integrity because each unique input will have a unique output.
- We use hashing to verify that something has not been tampered with.
- MD5 and SHA are common hash algorithms.

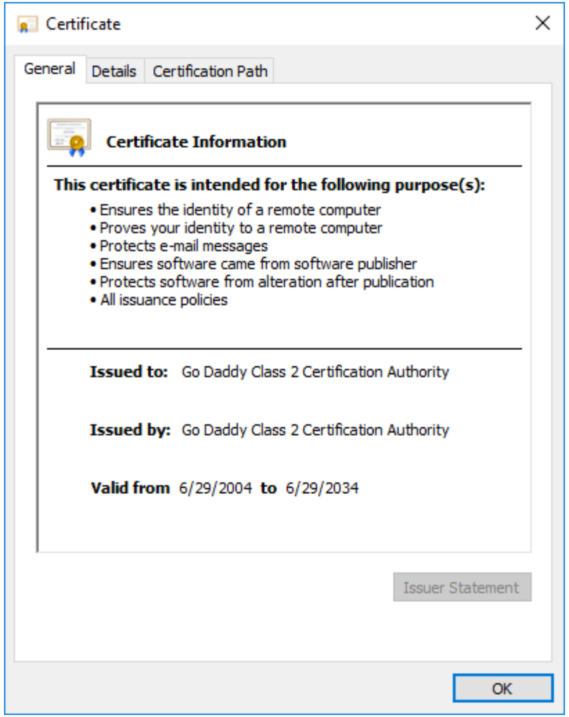


Digital Certificates and Certificate Authorities

INSTRUCTOR **ALTON**

What Is a Digital Certificate?

- A **digital certificate** is an electronic document used to identify an individual, a server, an organization, or some other entity and associate that entity with a **public key**.
- Digital certificates are used in **public key infrastructure (PKI)** encryption.
- We can think of a digital certificate as our “online” **digital credential** that verifies our identity.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

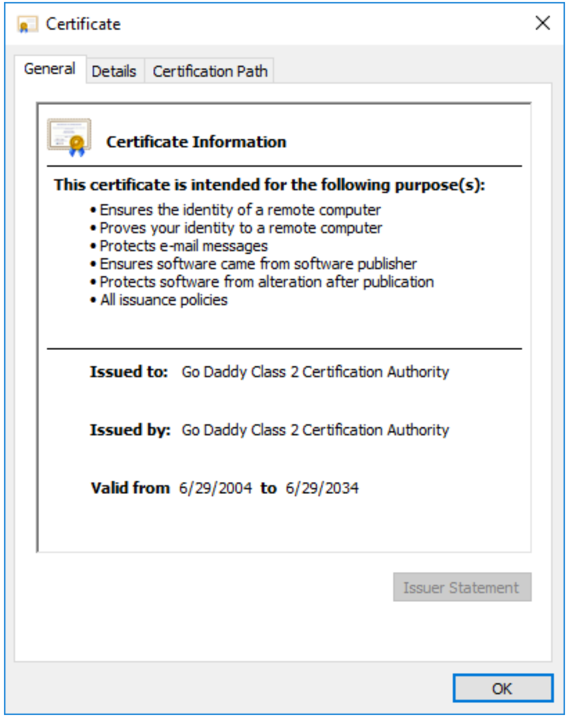
Issued to: Go Daddy Class 2 Certification Authority

Issued by: Go Daddy Class 2 Certification Authority

Valid from 6/29/2004 **to** 6/29/2034

The Role of Certificate Authorities

- Digital certificates are issued by a **Certificate Authority (CA)**.
- **Certificate Authorities** are a trusted entity, typically an organization such as VeriSign, that verifies an entity's identity, issues, manages, and signs that entity's digital certificate.
- Just like we trusted the DMV to issue driver's licenses, we trust CAs to issue digital certificates.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

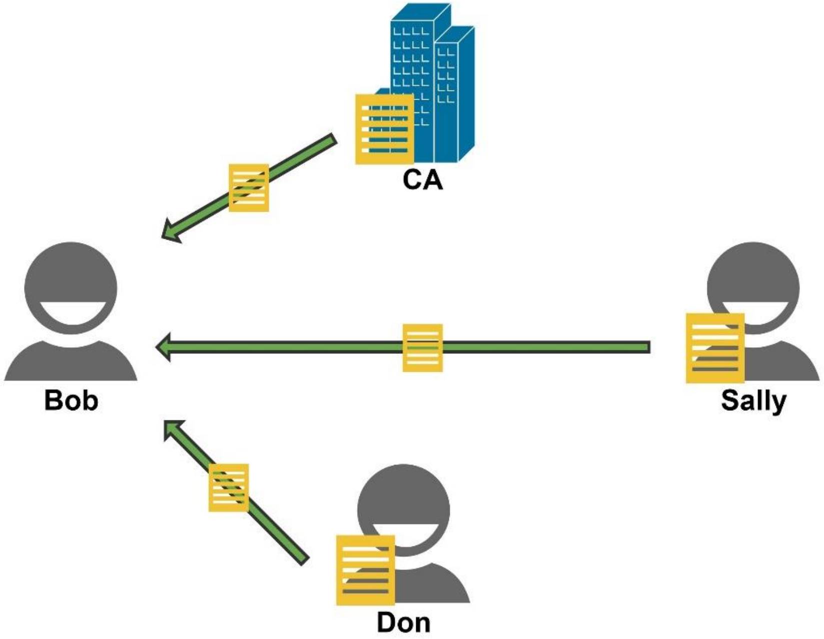
Issued to: Go Daddy Class 2 Certification Authority

Issued by: Go Daddy Class 2 Certification Authority

Valid from 6/29/2004 **to** 6/29/2034

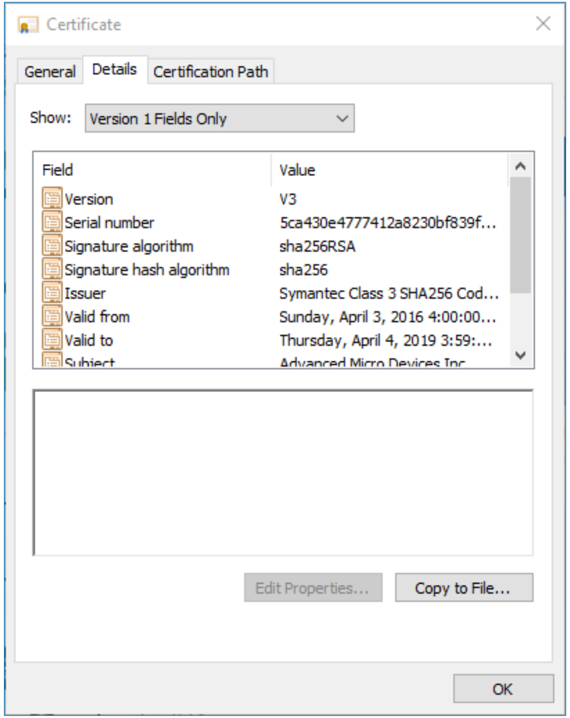
How Are Digital Certificates Shared?

- The CA has verified Sally's identity and has issued a digital certificate on her behalf.
- How does Bob obtain Sally's digital certificate?
  - The CA
  - Sally
  - Someone else who has it (Don)



What's Included in a Digital Certificate?

- **Serial Number**: Used to uniquely identify the certificate.
- **Signature Algorithm**: The algorithm used to create the signature.
- **Issuer**: The entity that verified the information and issued the certificate.
- **Valid-From**: The date the certificate is first valid from.
- **Valid-To**: The expiration date.
- **Public Key**: The public key.
- Plus Additional Information.



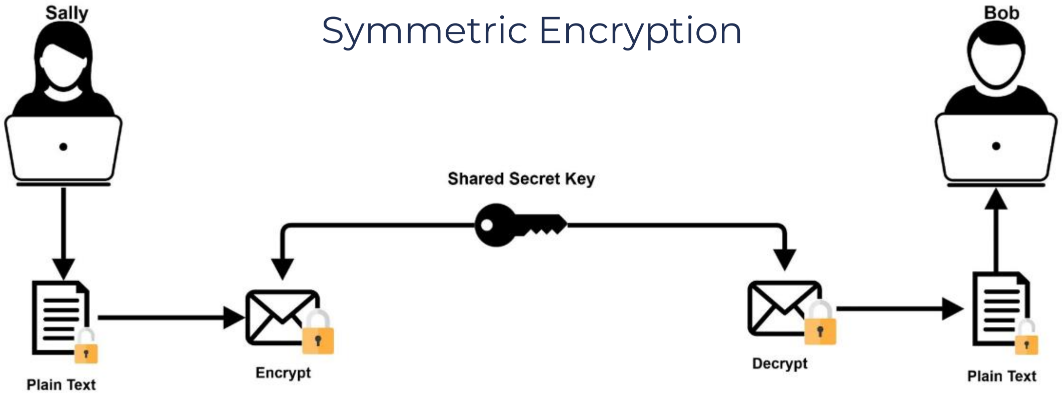
Show: Version 1 Fields Only

Field	Value
Version	V3
Serial number	5ca430e4777412a8230bf839f...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Symantec Class 3 SHA256 Cod...
Valid from	Sunday, April 3, 2016 4:00:00...
Valid to	Thursday, April 4, 2019 3:59:...
Subject	Advanced Micro Devices Inc

Email Encryption Use Cases

Email Confidentiality

Symmetric Encryption



Sally

Plain Text

Encrypt

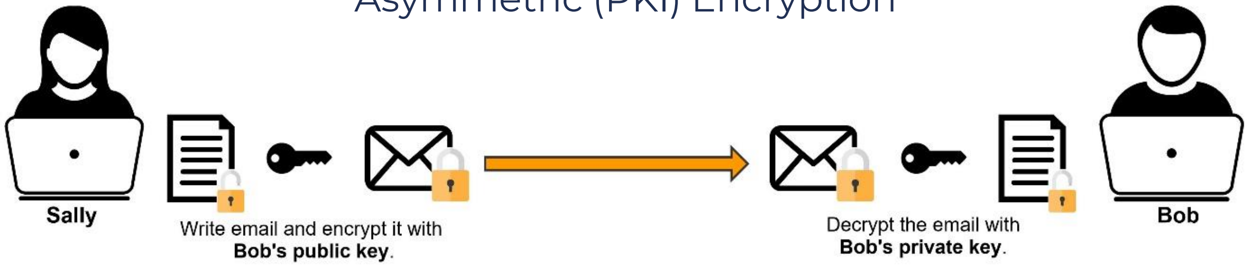
Shared Secret Key

Decrypt

Plain Text

Bob

Asymmetric (PKI) Encryption



Sally

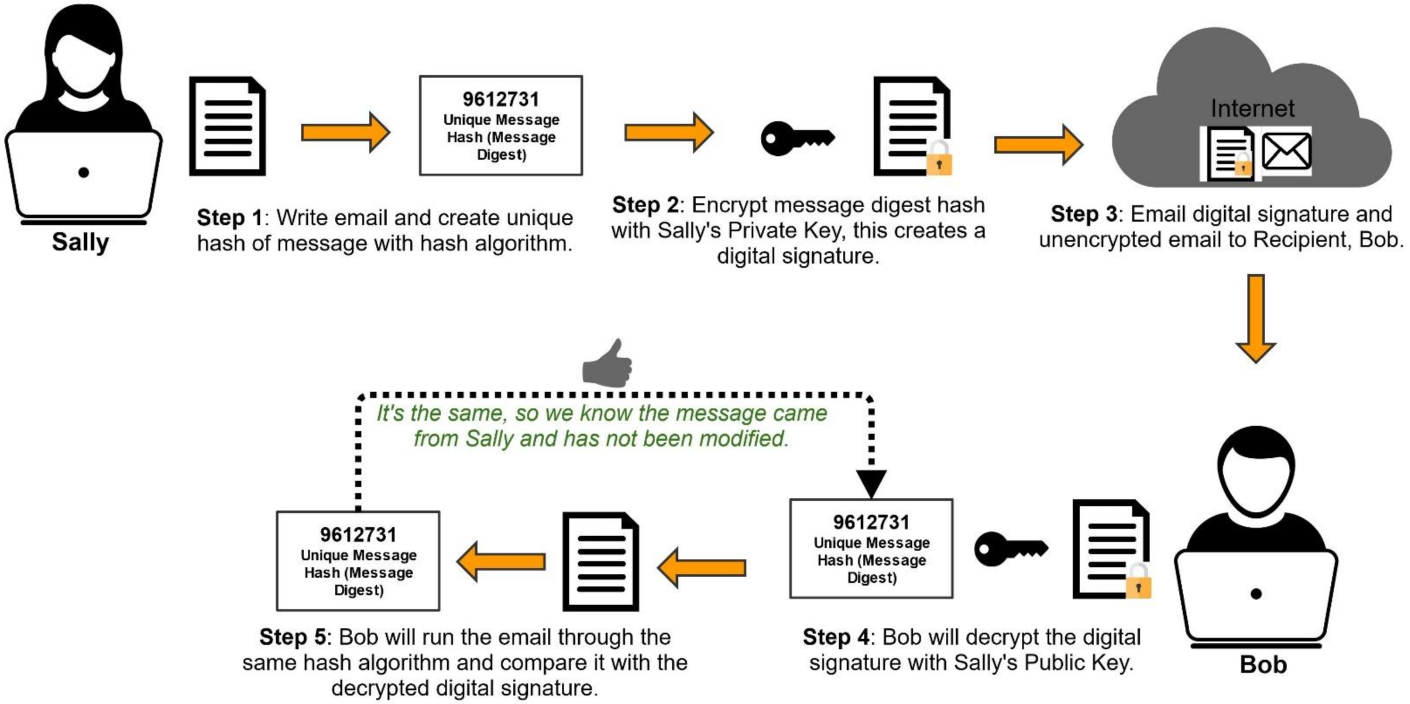
Write email and encrypt it with **Bob's public key**.

Decrypt the email with **Bob's private key**.

Bob

INSTRUCTOR
ALTON

Email Integrity, Authentication & Non-Repudiation


Sally
9612731
Unique Message Hash (Message Digest)
Internet
Bob
9612731
Unique Message Hash (Message Digest)
9612731
Unique Message Hash (Message Digest)

Step 1: Write email and create unique hash of message with hash algorithm.

Step 2: Encrypt message digest hash with Sally's Private Key, this creates a digital signature.

Step 3: Email digital signature and unencrypted email to Recipient, Bob.

Step 4: Bob will decrypt the digital signature with Sally's Public Key.

Step 5: Bob will run the email through the same hash algorithm and compare it with the decrypted digital signature.

It's the same, so we know the message came from Sally and has not been modified.

Achieving Confidentiality, Integrity, Authentication & Non-Repudiation

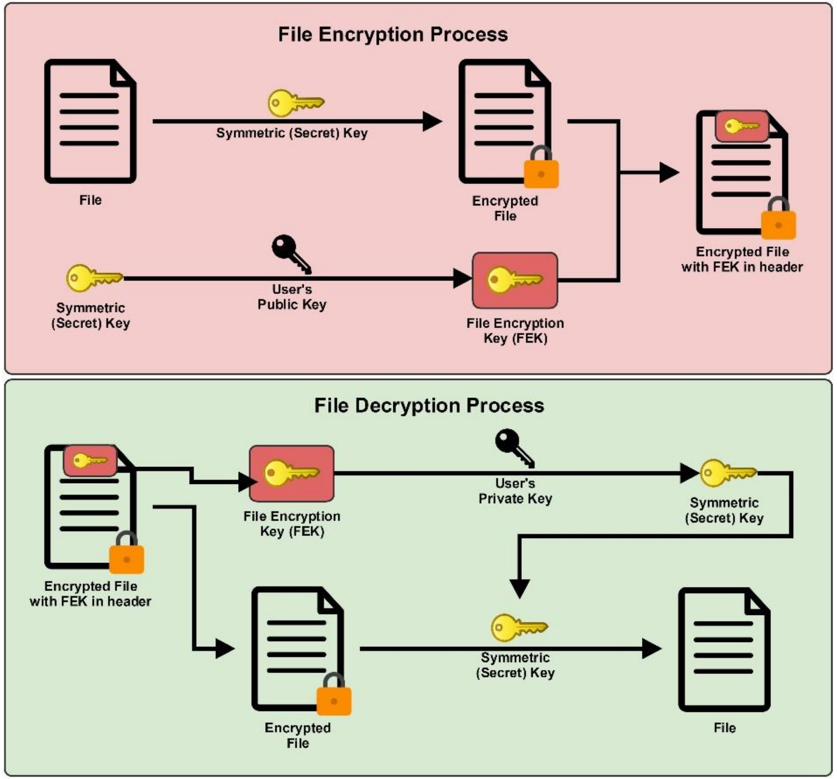
- We can achieve confidentiality, integrity, authentication, and non-repudiation by using a combination of symmetric and asymmetric encryption:
  - Use PKI to securely share symmetric encryption shared secret key.
  - Use our private key to create a digital signature and a public (or shared secret) key to encrypt an email.

Windows Encrypted File System Use Case

INSTRUCTOR **ALTON**

Windows Encrypted File System

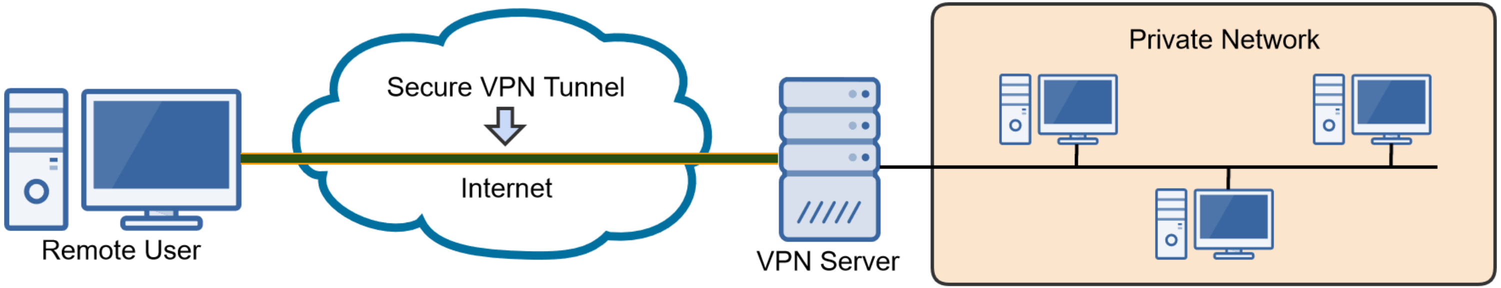
- Windows Encrypted File System (EFS) allows us to encrypt individual files and folders.
- Uses a combination of symmetric and asymmetric encryption:
  - A separate symmetric secret key is created for each file.
  - A digital certificate is created for the user, which holds the user's private and public key pair.
- If the user's digital certificate is deleted or lost, encrypted files and folders can only be decrypted with a Windows Recovery Agent.



Revisiting VPN

Virtual Private Network (VPN)

- **A virtual private network (VPN)** allows you to connect to a private network over a public network in a secure, encrypted manner.
- Once connected to the Internet with a public IP address, a tunneling protocol is used to create a protected tunnel through the Internet to the VPN server.
- Tunneling basically means encapsulating one protocol within another to ensure that a transmission is secure.



Internet Protocol Security (IPSec)

- IPSec is a protocol that authenticates and encrypts packets sent over an IP network.
- Two Primary Components:
    - **Authentication Header (AH)**
        - ✓ Provides a mechanism for authentication-only, not encryption.
    - **Encapsulating Security Payload (ESP)**
        - ✓ Provides a mechanism for both authentication and encryption.

IPSec Modes

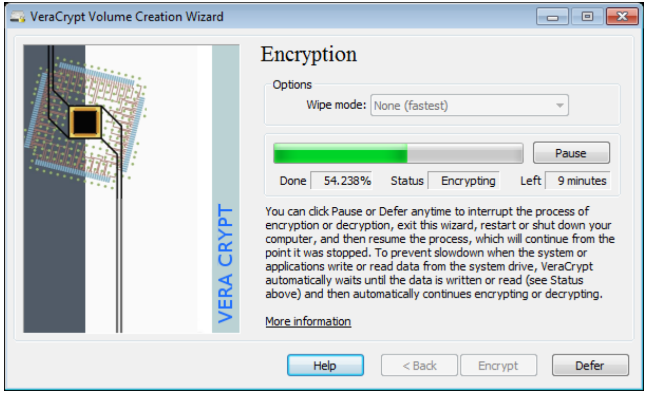
- There are 2 Different IPSec Modes:
  - **Tunnel Mode**
    - The entire IP packet is encapsulated and encrypted by IPSec. This protects the internal routing information by encrypting the IP header of the original packet.
    - Commonly used for site-to-site VPNs.
    - NAT is supported with the tunnel mode.
  - **Transport Mode**
    - Only encrypts the payload (data) and ESP trailer. The IP header of the original packet is NOT encrypted.
    - Commonly used for client-to-site VPN connections.
    - NAT is NOT supported in Transport Mode.

Software versus Hardware-Based Encryption

INSTRUCTOR
ALTON

Software-Based Encryption

- Uses software tools to encrypt your data:
  - BitLocker, Windows EFS, VeraCrypt, 7zip
- Typically as secure as the Operating System.
- A vulnerability in the Operating System can compromise the encryption software.



VeraCrypt Volume Creation Wizard

Encryption

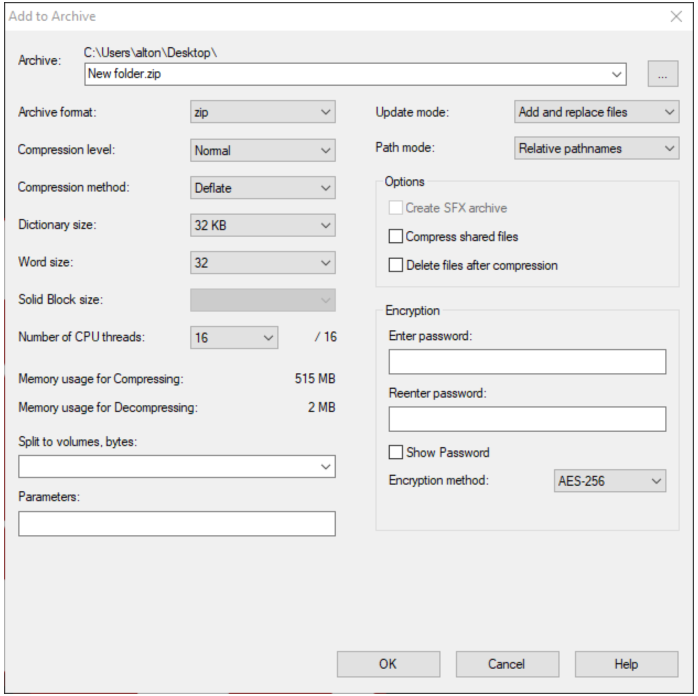
Options

Wipe mode: None (fastest)

Done 54.238% Status Encrypting Left 9 minutes

You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, VeraCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.

More information



Add to Archive

Archive: C:\Users\alton\Desktop\
New folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 16 / 16

Memory usage for Compressing: 515 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

Enter password:

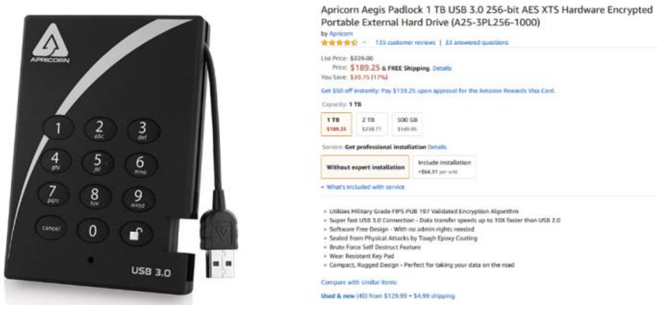
Reenter password:

□ Show Password

Encryption method: AES-256

Hardware-Based Encryption

- Uses hardware to perform encryption:
  - TPM (Crypto Processor)
  - Processors with x86 Instruction Set (AES Encryption)
- Many times, stand alone USB hard drives.



Apricorn Aegis Padlock 1 TB USB 3.0 256-bit AES XTS Hardware Encrypted Portable External Hard Drive (A25-3PL256-1000)

by Apricorn

★★★★☆ 135 customer reviews | 33 answered questions

List Price: ~~$229.00~~
Price: $189.25 & FREE Shipping. Details
You Save: $39.75 (17%)

Get $50 off instantly: Pay $139.25 upon approval for the Amazon Rewards Visa Card.

Capacity: 1 TB

1 TB $189.25	2 TB $238.71	500 GB $149.95

Service: Get professional installation Details

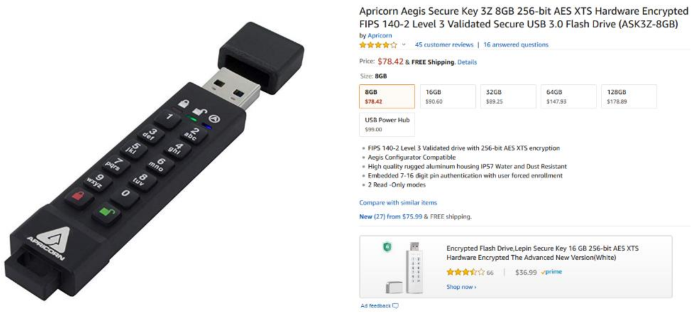
Without expert installation	Include installation +$64.31 per unit

What's included with service

- Utilizes Military Grade FIPS PUB 197 Validated Encryption Algorithm
- Super fast USB 3.0 Connection - Data transfer speeds up to 10X faster than USB 2.0
- Software Free Design - With no admin rights needed
- Sealed from Physical Attacks by Tough Epoxy Coating
- Brute Force Self Destruct Feature
- Wear Resistant Key Pad
- Compact, Rugged Design - Perfect for taking your data on the road

Compare with similar items

Used & new (40) from $129.99 + $4.99 shipping



Apricorn Aegis Secure Key 3Z 8GB 256-bit AES XTS Hardware Encrypted FIPS 140-2 Level 3 Validated Secure USB 3.0 Flash Drive (ASK3Z-8GB)

by Apricorn

★★★★☆ 45 customer reviews | 16 answered questions

Price: $78.42 & FREE Shipping. Details

Size: 8GB

8GB $78.42	16GB $90.60	32GB $89.25	64GB $147.93	128GB $178.89
USB Power Hub $99.00				

- FIPS 140-2 Level 3 Validated drive with 256-bit AES XTS encryption
- Aegis Configurator Compatible
- High quality rugged aluminum housing IP57 Water and Dust Resistant
- Embedded 7-16 digit pin authentication with user forced enrollment
- 2 Read -Only modes

Compare with similar items

New (27) from $75.99 & FREE shipping.

Encrypted Flash Drive,Lepin Secure Key 16 GB 256-bit AES XTS Hardware Encrypted The Advanced New Version(White)

★★★½☆ 66 | $36.99 ✓prime

Shop now ›

Ad feedback