GPG Command Cheat Sheet - Data Encryption

The following are a list of commonly used commands for encypting documents in Terminal (Mac, Linux) or PowerShell (Windows).

Creating A New Keypair	
gpg --gen-key	Prompts for information and then creates an appropriate keypair
Importing, Exporting, and Refreshing Keys	
Importing	
gpg --import File	Imports a key contained in File to the appropriate keyring
gpg –recv-keys KeyID1 KeyID2	Receives the key which corresponds to KeyID1, KeyID2, etc from the provided keyserver
gpg --search-keys Term1 Term2	Searches for keys which contain Term1 and Term2, etc and provides an interactive interface to choose the correct key to import to the appropriate keyring
Exporting	
gpg --export -a KEYID > publickey.asc	Output a public key to a plain text file
gpg --send-keys KeyID	Upload a public key to a keyserver
Refreshing	
gpg --refresh-keys	Check to see if your version of a key is out of date. If so update it.
Printing Key Information	
gpg --list-keys	Print a list of all of the keys in your public keyring
gpg --list-keys UniqueID	Print all keys matching UniqueID
gpg --list-sigs	Print a list of all keys in your public keyring and their associated signatures
gpg --list-sigs UniqueID	Print a list of all keys and their associated signatures matching UniqueID
gpg --fingerprint	Print a list of all keys in your public keyring and their associated fingerprints
gpg --fingerprint UniqueID	Print a list of all keys and their associated signatures matching UniqueID
Signing a Key	
gpg --fingerprint UniqueID	Check the local key fingerprint against the reported fingerprint

gpg --sign-key UniqueID	If the fingerprints match sign the key with your private key
Encrypting and Signing	
Encrypting	
gpg -er Recipient File	Produces File.gpg an encrypted version of File, which can be decrypted by Recipient
echo “Text” | gpg -ear Recipient	Produces an encrypted version of Text which can be decrypted by Recipient and prints the result to the terminal
echo “Text” | gpg -ear Recipient > OutFile	Produces an encrypted version of Text which can be decrypted by Recipient and writes the result to OutFile
cat InFile | gpg -ear Recipient	Produces an encrypted version of the text contained in InFile which can be decrypted by Recipient and prints the result to the terminal
cat InFile | gpg -ear Recipient > OutFile	Produces an encrypted version of the text contained in InFile which can be decrypted by Recipient and writes the result to OutFile
Signing	
gpg -s File	Produces File.gpg, a signed version of File, which can be verified
echo “Text” | gpg -as	Produces a signed version of Text and prints the result to the terminal
echo “Text” | gpg -s > OutFile	Produces a signed version of Text and writes the result to OutFile
cat InFile | gpg -as	Produces a signed version of the text in InFile and prints the result to the terminal
cat InFile | gpg -s > OutFile	Produces a signed version of the text in InFile and writes the result to OutFile
gpg --detach-sign File	Produces a separate signature, File.sig, which can be used to verify File
echo “Text” | gpg --clearsign	
cat InFile | gpg --clearsign	
Encrypting and Signing	
gpg -esr Recipient File	Produces File.gpg, an encrypted and signed version of File, which can be decrypted and verified by Recipient
echo “Text” | gpg -esar Recipient File	Produces an encrypted and signed version of Text which can be decrypted and verified by Recipient and prints the result to the terminal
echo “Text” | gpg -esar Recipient File > OutFile	Produces an encrypted and signed version of Text which can be decrypted and verified by Recipient and writes the result to OutFile
cat InFile | gpg -esar Recipient	Produces an encrypted and signed version of the text in InFile which can be decrypted and verified by Recipient and prints the result to the terminal
cat InFile | gpg -esar Recipient > OutFile	Produces an encrypted and signed version of the text in InFile which can be decrypted and verified by Recipient and prints the result to the terminal
Decrypting and Verifying	

gpg -d InFile > OutFile	Decrypt and/or verify File
echo “Cipher Text” | gpg -d	Decrypt and/or verify Cipher Text
echo “Cipher Text” | gpg -d > OutFile	Decrypt and/or verify Cipher Text and write the result to OutFile
cat InFile | gpg -d	Decrypt and/or verify the contents of File
cat InFile | gpg -d > OutFile	Decrypt and/or verify the contents of File and write the result to OutFile
Symmetric Encryption	
gpg -c File	Create a file symmetrically encrypted with a passphrase
gpg -ca File	Create a file symmetrically encrypted with a passphrase readable as plain text
echo “Text” | gpg -ca	Symmetrically encrypt Test with a passphrase and output the result to the terminal
echo “Text” | gpg -c > OutFile	Symmetrically encrypt Test with a passphrase and write the result to OutFile
cat InFile | gpg -ca	Symmetrically encrypt the text in InFile and output the result to the terminal
cat InFile | gpg -c > OutFile	Symmetrically encrypt the text in InFile and write the result to OutFile

Created by Brian Balsamo. Used with permission.