PGP Script

Person #1 (Bob)		Person #2 (Jane)	
pgp -kg	Bob key creation		
pgp -kxa bob bob.asc	Export Bob’s public key		
mail jane < bob.asc	Email Bob’s public key to Jane		
		pgp –kg	Jane key creation
		pgp -kxa jane jane.asc	Export Jane’s public key
		mail bob < jane.asc	Email Jane’s key to Bob
		email > bob.asc	Download Bob’s key from email
		pgp bob.asc	Import Bob’s public key to PGP
email > jane.asc	Download Jane’s public key		
pgp jane.asc	Import Jane’s public key		
vi letter	Write Jane a letter		
pgp -ea letter jane	Encrypt file named letter		
	Why does it need the recipient?		
mail jane < letter.asc	Email encrypted letter to Jane		
		email > letter.asc	Download Bob’s letter
		pgp letter.asc	Decrypt letter from Bob
		vi letter	Write Bob a reply
		pgp –sat letter	Sign file named letter
			Why need pass phrase?
			Who can read it?
			-t option makes clear text
		email bob < letter.asc	Email signed letter to Bob
email > letter.asc	Download Jane’s letter		
pgp letter.asc	Authenticate sender		
vi letter	Write Jane a letter		
pgp –esa letter	Encrypt AND sign file named letter		
email bob < letter.asc	Email letter to Jane		
		email > letter.asc	Download Bob’s letter
		pgp letter.asc	Decrypt and verify signature of letter

To learn more:

1. Read PGP Vol. I from web page
2. man pgp