Βήμα 1

Κάθε χρήστης πρέπει να δημιουργήσει ένα ζεύγος κλειδιών GPG (ιδιωτικά και δημόσια κλειδιά). Δείτε πώς μπορεί να το κάνει ο Χρήστης. Αυτό γίνεται με την εντολή

```
gpg –full-generate-key
```

Θα σας ζητηθούν πολλές επιλογές:

1. **Select key type: Επιλέξτε RSA**
2. **Key size: 2048**
3. **Expiration: Να ορίσετε το κλειδί ώστε να μην λήγει ποτέ ή να του δώσετε ημερομηνία λήξης.**
4. **Enter your name and email address: Δώστε ένα όνομα και μια διεύθυνση email για αναγνώριση.**
5. **Passphrase: Ορίστε μια φράση πρόσβασης για την προστασία του ιδιωτικού κλειδιού.**

Βήμα 2
Ο χρήστης πρέπει να **επιβεβαιωσει** την δημιουργία των κλειδιών με την ενοτλή

```
gpg –list-keys
```

Βήμα 3
Ο χρήστης πρέπει να κάνει **εξαγωγή** (**export**) to Public Key

```
gpg --armor --export user1@example.com > user1_public.key
```

user1@example.com ειναι το ποθ δόθηκε στο Βήμα 1

Βημα 4
Ο χρήστης πρέπει να στείλει το **public.key** στο χρήστη που πρεπει να συνομιλήσει με κρυπτογραφηση.

Βημα 5
Ο χρήστης πρέπει να κανει **εισαγωγη** (**import**) το **public key** που θα λάβει απο τον συνομιλητή του με την εντολή

```
gpg --import user2_public.key
```

Βημα 6
Παραγωγη κρυπτογρφημένου μηνύματος

```
echo "This is a secret message" | gpg --encrypt --armor
 --recipient user2@example.com > encrypted_message.asc
```

Βημα 7
Στιλτε με email attachment το κρυπτογραφημένο κείμενο

Βημα 8
Α. Αποθηκεύστε το attachment που λάβατε
Β. Αποκρυπτογραφήστε με την εντολή

```
gpg --decrypt encrypted_message.asc
```