Key Encryption

Using the **PGP** encryption way to encrypt the keys.

Step1:
XOR Key1 and Key2 to get the encryption KEK.

Step2:
Using encryption KEK to encrypt the BDK and TMK to become ciphertext BDK and ciphertext TMK.

Step3:
Put Key1, ciphertext BDK, and ciphertext TMK in one file named PGP1. Using Dspread1 public key to encrypt it.

Step4:
Put Key2, ciphertext BDK, and ciphertext TMK in one file named PGP2. Using Dspread2 public key to encrypt it.

Step5:
Please make sure you send these two files to the different person. That is really important for the Security System.

Step6:
Write down the Checkvalues for cleartext Key1, KEK, cleartext BDK, and cleartext TMK on the first email to one person. And Checkvalues for cleartext Key2, KEK, cleartext BDK, and cleartext TMK to the second person.

PGP1:

Key1	32 bits cleartext key	Checkvalue	PGP1 file using Dspread1 key to encrypt
BDK	32 bits key ciphertext key (KeyKey encrypte)	Checkvalue	
TMK	32 bits key ciphertext key (KeyKey encrypte)	Checkvalue	

PGP2:

Key2	32 bits cleartext key	Checkvalue	PGP2 file using Dspread2 key to encrypt
BDK	32 bits key ciphertext key (KeyKey encrypte)	Checkvalue	
TMK	32 bits key ciphertext key (KeyKey encrypte)	Checkvalue	